Quantum distribution of Gaussian keys using squeezed states

N. J. Cerf,[1,2] M. Lévy,[1] and G. Van Assche[1]
[1]*Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[2]*Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91109*
(Received 26 October 2000; published 18 April 2001)

A continuous key-distribution scheme is proposed that relies on a pair of conjugate quantum variables. It allows two remote parties to share a secret Gaussian key by encoding it into one of the two quadrature components of a single-mode electromagnetic field. The resulting quantum cryptographic information versus disturbance trade-off is investigated for an individual attack based on the optimal continuous cloning machine. It is shown that the information gained by the eavesdropper then simply equals the information lost by the receiver.

DOI: 10.1103/PhysRevA.63.052311 PACS number(s): 03.67.Dd, 03.65.Ta, 42.50.−p, 89.70.+c

Quantum cryptography—or, more precisely, quantum key distribution—is a technique that allows two remote parties to share a secret string of random bits (a secret key) that can be used for exchanging encrypted information [1–3]. The security of this process fundamentally relies on the fact that the measurement of incompatible variables inevitably affects the state of a quantum system. Any leak of information to an eavesdropper necessarily induces a disturbance of the system, which is, in principle, detectable by the authorized receiver.

In most quantum cryptosystems proposed so far, a single photon (or, in practice, a weak coherent state with an average photon number lower than one) is used to carry each bit of the key. Mathematically, the security results from the use of a pair of noncommuting observables such as the x and z projections of a spin 1/2, σ_x and σ_z, whose eigenstates are used to encode the key. The sender (Alice) randomly chooses to encode the key using either σ_z (0 is encoded as $|\uparrow\rangle$ and 1 as $|\downarrow\rangle$) or σ_x [0 is encoded as $2^{-1/2}(|\uparrow\rangle+|\downarrow\rangle)$ and 1 as $2^{-1/2}(|\uparrow\rangle-|\downarrow\rangle)$], the choice of the basis being disclosed only *after* the receiver (Bob) has measured the photon. This guarantees that an eavesdropper (Eve) cannot read the key without corrupting the transmission. Such a procedure, known as BB84 [1], is at the heart of most of the quantum cryptographic schemes that have been experimentally demonstrated in the past few years, which are based either on the polarization (e.g., [4]) or the optical phase (e.g., [5]) of single photons. An alternative scheme, realized experimentally only a year ago [6], can also be devised relying on a pair of polarization-entangled photons instead of single photons [7]. It is, however, fundamentally equivalent to BB84 (see [8]) as it again relies on the algebra of spin-1/2 particles.

Recently, it has been shown that other quantum key distribution protocols can be devised based on continuous variables, where squeezed coherent light modes are used to carry the key [9–11]. In these techniques, one exploits a pair of canonically conjugate (continuous) variables such as the two quadratures X_1 and X_2 of the amplitude of a mode of the electromagnetic field, which behave just like position and momentum. The uncertainty relation $\Delta X_1 \Delta X_2 \geqslant 1/4$ then implies that Eve cannot read both quadrature components without degrading the state. Even though the experimental preparation of squeezed states is a difficult task, these schemes circumvent a main weakness of the above-mentioned cryptosystems that is the critical dependence of their security on the ability of preparing single-photon states.

In this paper, we propose an alternative squeezed-state quantum cryptographic scheme, which provides a means to distribute a *continuous* secret key. Here, Alice and Bob aim at sharing a continuous key that consists of a random list of Gaussian-distributed variables that cannot be known to Eve. The key is simply a Gaussian noise that is imposed on the squeezed quadrature of a squeezed light mode. Thus, in our protocol, *both* the key and the quantum variable that carries it are continuous. This is in contrast with the schemes proposed in Refs. [9–11], which appear hybrid as a continuous quantum carrier encodes a discrete key element (the shared key is made of bits or, in general, discrete variables). Instead, our approach can be viewed as an *all-continuous* quantum cryptographic scheme, which is the proper continuous extension of BB84. From a theoretical perspective, this provides a more satisfying continuous treatment of quantum key distribution. The trade-off between Eve's information gain and Bob's disturbance can be expressed in an unexpectedly simple way (restricting ourselves to individual attacks based on the optimal continuous cloning machine [12,13]): the information gained by Eve on one quadrature is at most equal to the information lost by Bob on the other quadrature. This provides a simple information-theoretic disturbance measure, namely, the defect of information at Bob's station. Moreover, our all-continuous scheme avoids a potential attack against the continuous cryptosystems proposed so far by filling in the gaps between the discrete values used to encode the key.

Let us detail our protocol. The uncertainty relation implies that it is impossible to measure with full accuracy *both* quadratures of a single mode, X_1 and X_2. Alice exploits this property by encoding the key elements (random Gaussian samples) as a quadrature squeezed state either in X_1 or in X_2 in such a way that an eavesdropper ignoring which of these two ''bases'' is used cannot acquire information without disturbing the state. In basis 1, Alice prepares a squeezed vacuum state such that the fluctuations of X_1 are squeezed ($\Delta X_1^2 = \sigma_1^2 < 1/4$), and applies a displacement of X_1 by an amount equal to the key value ($\langle X_1 \rangle = x$, where x is the encoded key element). The quantity σ_1^2 refers here to the in-

trinsic variance of X_1; the corresponding squeeze parameter is $r_1=-\ln(2\sigma_1)$. We denote by Σ_1^2 the variance of the key, that is, the mean value $\langle X_1\rangle$ is itself distributed as a Gaussian variable of zero mean and variance Σ_1^2. Conversely, in basis 2, Alice sends a squeezed state in X_2 ($\Delta X_2^2=\sigma_2^2<1/4$), whose displacement encodes the Gaussian key $\langle X_2\rangle=x$. Again, $\langle X_2\rangle$ has a zero mean and a variance Σ_2^2, while the squeeze parameter is $r_2=-\ln(2\sigma_2)$. Thus, in summary, Alice encodes the Gaussian key into a displaced vacuum squeezed state, the squeezing (by r) and displacement (by x) being applied at random on quadrature X_1 or X_2. The actual quadrature that carries the key is disclosed by Alice only *after* Bob announces that he has received the signal, thereby imposing a penalty on Eve.

Now, for our cryptographic setup to be maximally secure, we require the distribution of X_1 measurement outcomes to be indistinguishable whether basis 1 or 2 is used by Alice. If this condition is fulfilled, Eve cannot obtain any indication on whether she is measuring a type 1 or type 2 squeezed state, whatever the statistics she accumulates. If basis 1 is used, the outcomes of X_1 measurements (that can be obtained by homodyne detection) are distributed as a Gaussian of variance $\Sigma_1^2+\sigma_1^2$ since each squeezed state gives an extra contribution of σ_1^2 to the key variance. If, on the contrary, a type 2 squeezed state is measured, then the outcomes of X_1 measurements exhibit a Gaussian distribution of variance $1/(16\sigma_2^2)$ as a result of the uncertainty principle. Thus, we impose the condition

$$\Sigma_1^2+\sigma_1^2=1/(16\sigma_2^2). \tag{1}$$

Similarly, the requirement that type 1 and 2 squeezed states are indistinguishable when performing X_2 measurements implies that $\Sigma_2^2+\sigma_2^2=1/(16\sigma_1^2)$. These two relations can be summarized as

$$1+\Sigma_1^2/\sigma_1^2=1+\Sigma_2^2/\sigma_2^2=1/\alpha^2, \tag{2}$$

where $\alpha=4\,\sigma_1\sigma_2=e^{-(r_1+r_2)}$ is a dimensionless constant that satisfies $\alpha\leqslant 1$ (or $\sigma_1\sigma_2\leqslant 1/4$). More generally, Eq. (2) guarantees that the density matrices of the encoded key elements are the same in bases 1 and 2, making them indistinguishable. Equation (2) also implies that the squeeze parameters r_1 and r_2 completely characterize the protocol.

Let us first analyze this Gaussian key distribution in the case where there is no eavesdropping and the transmission is perfect. For that, we need to recall some standard notions of Shannon theory concerning continuous transmission channels [14]. Consider a discrete-time continuous channel that adds a Gaussian noise of variance σ^2 on the signal. If the input x of the channel is a Gaussian signal of variance Σ^2, the uncertainty on x is measured by the differential Shannon entropy $h(x)=2^{-1}\log_2(2\pi e\Sigma^2)$ bits [15]. Conditionally on x, the output y is distributed as a Gaussian of variance σ^2 so that the entropy of y conditionally on x becomes $h(y|x)=2^{-1}\log_2(2\pi e\sigma^2)$ bits. Now, the distribution of y is given by the convolution of these two Gaussians, i.e., a Gaussian of variance $\Sigma^2+\sigma^2$. Hence, the output entropy is $h(y)=2^{-1}\log_2[2\pi e(\Sigma^2+\sigma^2)]$ bits. According to Shannon theory, the information processed through this noisy channel can be expressed as the mutual entropy between x and y (the amount by which the uncertainty on y is reduced by knowing x) [15],

$$I\,(\text{bits})=h(y)-h(y|x)=\frac{1}{2}\log_2(1+\gamma), \tag{3}$$

where $\gamma=\Sigma^2/\sigma^2$ is the signal-to-noise ratio (SNR). This is Shannon's famous formula for the capacity of a Gaussian additive noise channel where the signal variance (or power) is Σ^2 while the noise variance is σ^2.

Equation (3) immediately applies to our cryptographic setup in the absence of eavesdropping. Assume Bob performs a measurement in the good basis after the latter is announced by Alice on an authenticated public channel. (This is equivalent to the more realistic procedure where Bob actually measures the key in a random basis, but then discards the bad outcomes after the basis is disclosed by Alice.) The SNR in basis 1 is simply $\gamma_1=\Sigma_1^2/\sigma_1^2$, while it is $\gamma_2=\Sigma_2^2/\sigma_2^2$ in basis 2. Then, Eq. (2) becomes $1+\gamma_1=1+\gamma_2=1/\alpha^2$ so that the SNR is the same in both the bases, $\gamma=e^{2(r_1+r_2)}-1$. This means that the processed information from Alice to Bob in both the bases can be expressed, using Eq. (3), as

$$I\,(\text{bits})=-\log_2(\alpha)=(r_1+r_2)/\ln 2. \tag{4}$$

This information I measures the number of bits that can be transmitted asymptotically (using block coding) per use of the channel with an arbitrary high fidelity for a given SNR. This transmission rate can be shown to be attainable if the signal is Gaussian distributed (which is the case under consideration here). Note that I (when expressed in natural units—nats—rather than bits) simply equals the sum of the squeeze parameters in bases 1 and 2, which reflects that the protocol cannot work in the absence of squeezing. As an example, if $\sigma_1^2=\sigma_2^2=1/8$, i.e., if we have a 3-dB squeezing ($e^r=\sqrt{2}$) in each basis, then $\gamma=3$, so we can process one bit on average per key state.

Let us now estimate the average photon number $\langle N\rangle$ contained in each encoded key state. It clearly increases with the widening (Σ^2) of the displacement used to represent Alice's key values. It also increases with squeezing but then the displacement distribution can be narrowed to achieve a same SNR. Let us determine the relative contribution of these two effects assuming, for simplicity, that $\sigma_1=\sigma_2=\sigma$ so that the same squeezing is applied on both quadratures. Then, Eq. (2) implies that $\sigma^2=\frac{1}{4}e^{-2r}$, $\Sigma^2=\frac{1}{2}\sinh(2r)$, and $1+\gamma=e^{4r}$. The mean photon number in a given encoded key state (with a given displacement x) is $N=x^2+\sinh^2 r$, where the first term reflects the displacement effect while the second characterizes vacuum squeezing [16]. Then, for a given SNR (or a given r), the average number of photons over all values of x sent by Alice is $\langle N\rangle=\Sigma^2+\sinh^2 r$. This yields for the average number of photons per key state,

$$\langle N\rangle=\frac{1-\alpha}{2\alpha}=\frac{e^{2r}-1}{2}=\frac{(1+\gamma)^{1/2}-1}{2}. \tag{5}$$

Equivalently, the processed information can be expressed as $I\,(\text{bits})=\log_2(2\langle N\rangle+1)$, implying that the photon number increases exponentially with the processed information. Note that $\langle N\rangle=1/2$ in the above example of a 1-bit channel (3-dB squeezing).

Let us now analyze the signature that is left by an eavesdropper Eve in this continuous cryptographic protocol. First, we must emphasize that in contrast with BB84, the key values received by Bob are not exactly equal to those sent by Alice even in the absence of eavesdropping. This simply results from the fact that the noise due to the intrinsic fluctuations of the squeezed quadrature adds to the signal, giving rise to a finite SNR. This already holds at Alice's station regardless of the (possibly tapped) channel. So, an eavesdropper will be detectable in this scheme by an enhanced noise variance (or reduced SNR) at Bob's station. Thus, a protocol that Alice can follow to detect eavesdropping is to disclose on an authenticated public channel the exact values x of a random subset of key elements. Then, Bob compares them to the received values y and computes the distribution of the differences $y-x$. For a perfect and untapped channel, it should be a Gaussian of variance σ^2, so the SNR is unchanged. Otherwise, the SNR decreases by an amount that can be viewed as a measure of the disturbance of the Alice-to-Bob channel. Assume, for example, that Eve uses an individual ''intercept-and-resend'' attack, measuring each key element in basis 1 or 2 at random, and resending a squeezed state centered on the value of the measured quadrature. The variance at Bob's station will be $2\sigma^2$ (twice the intrinsic variance) if Eve used the good basis, or $1/(16\sigma^2)$ in the opposite case, so the resulting noise variance is $\sigma^2[1+1/(2\alpha^2)]$. Thus Bob's computed SNR is reduced by a factor $2/(3+\gamma)$.

As we shall see, the trade-off between the information acquired by Bob and Eve in this protocol can be analyzed exactly using Eq. (3). For that, we will assume that the optimal individual eavesdropping strategy for Eve consists in using the optimal (Gaussian) cloning machine for continuous quantum variables [12,13]. More precisely, we consider an attack where Eve makes two imperfect copies (or clones) of the key state, then sends one to Bob while she keeps the other one. Once Alice has revealed the basis she used for encoding the key, Bob and Eve then measure their received states in the appropriate basis (again, this is equivalent to Bob measuring in a random basis and then discarding the bad measurements after the basis disclosure). In practice, Eve must keep her clones in a quantum memory until completion of the protocol, i.e., until after Bob informed Alice that he has received the data and Alice revealed the bases in return. The optimality of this eavesdropping strategy is a very reasonable assumption in view of the fact that the phase-covariant qubit cloner is known to be the best individual eavesdropping strategy for BB84 [17] (actually, the universal qubit cloner is optimal for the related six-state quantum cryptographic protocol [18]). It is also corroborated by an independent study of the optimum eavesdropping strategy in a continuous-variable cryptographic scheme that was brought to our attention after completion of the present paper [19].

In order to analyze the information-theoretic balance between Bob and Eve, we use a class of *asymmetric* Gaussian cloners defined in Ref. [12], which produce a different amount of noise on both quadratures and for Bob and Eve. It has been proved in Ref. [12] that the no-cloning inequality

$$\sigma_{1,B}^2\sigma_{2,E}^2\geqslant 1/16 \tag{6}$$

must hold (and is saturated for this class of cloners), where $\sigma_{1,B}^2$ and $\sigma_{2,E}^2$ are the variances of the cloning-induced errors that affect Bob's X_1 measurements and Eve's X_2 measurements, respectively. For example, in basis 1, the outcomes of X_1 measurements by Bob will be distributed as a Gaussian of variance $\sigma_1^2+\sigma_{1,B}^2$, since these cloning-induced errors are superimposed on the intrinsic fluctuations of the squeezed states. Similarly, a dual no-cloning uncertainty relation holds, connecting Bob's errors on X_2 and Eve's errors on X_1: $\sigma_{2,B}^2\sigma_{1,E}^2\geqslant 1/16$. Note that Eq. (6) and its dual were also shown in [19] to put a bound on Bob and Eve's measurements in a continuous-variable setup, implying that our cloning-based eavesdropping strategy is indeed optimal.

In order to calculate the information acquired by Bob and Eve, we characterize the cloners that saturate these inequalities by two parameters χ and λ: we rewrite the cloning-induced error variances on Bob's side as $\sigma_{1,B}^2=\chi\lambda(\sigma_1^2/\alpha)$ and $\sigma_{2,B}^2=\chi\lambda^{-1}(\sigma_2^2/\alpha)$, while the errors on Eve's side are written as $\sigma_{1,E}^2=\chi^{-1}\lambda(\sigma_1^2/\alpha)$ and $\sigma_{2,E}^2=\chi^{-1}\lambda^{-1}(\sigma_2^2/\alpha)$. Thus, χ characterizes the balance between Bob's and Eve's errors as $\sigma_{1,B}/\sigma_{1,E}=\sigma_{2,B}/\sigma_{2,E}=\chi$. (The limit $\chi\to 0$ corresponds to the case of vanishing eavesdropping where Bob gets the entire information I while Eve does not get any information. The case $\chi=1$ represents a symmetric cloner where the error variances are the same for Bob and Eve.) Similarly, λ describes the quadrature 1 vs 2 balance, that is, $\sigma_{1,B}/\sigma_{2,B}=\sigma_{1,E}/\sigma_{2,E}=\lambda(\sigma_1/\sigma_2)$. Let us now express the information processed from Alice to Bob (or from Alice to Eve) in basis 1 (or basis 2). In basis 1, the variance of Bob's measurement outcomes is $\sigma_1^2+\sigma_{1,B}^2=(1+\chi\lambda/\alpha)\sigma_1^2$, while the distribution of the key elements has a variance Σ_1^2. Using Shannon's formula, Eq. (3), and the identity $1+\Sigma_1^2/\sigma_1^2=1/\alpha^2$, we obtain for Bob's information in basis 1,

$$I_{1,B}=\frac{1}{2}\log_2\left(\frac{1+\alpha\chi\lambda}{\alpha^2+\alpha\chi\lambda}\right). \tag{7}$$

Similarly, using the variance of Eve's outcomes in basis 2, $\sigma_2^2+\sigma_{2,E}^2=[1+1/(\chi\lambda\alpha)]\sigma_2^2$, we obtain for Eve's information in basis 2

$$I_{2,E}=\frac{1}{2}\log_2\left(\frac{1+\alpha/(\chi\lambda)}{\alpha^2+\alpha/(\chi\lambda)}\right). \tag{8}$$

Then, the balance between Bob and Eve's information can be expressed by calculating the *sum* of Eqs. (7) and (8),

$$I_{1,B}+I_{2,E}=\frac{1}{2}\log_2(1/\alpha^2)=I. \tag{9}$$

Remarkably, the information $I_{2,E}$ acquired by Eve on the second quadrature is *exactly* counterbalanced by the defect of information at Bob's side on the first quadrature, $I-I_{1,B}$. Of course, the counterpart of Eq. (9) also holds when interchanging the bases, that is, $I_{2,B}+I_{1,E}=I$.

Thus, assuming that the continuous cloner is the best possible individual attack against our continuous cryptographic protocol, Bob's information loss $I-I_B$ can be viewed as a proper disturbance measure as it simply is an upper bound on the information that might be gained by a potential eavesdropper. Consequently, the net amount of key bits that can be generated by this method is bounded from below by $I_B-I_E \geqslant 2I_B-I$. This follows from [20] where it is proven that the secret key rate of A and B with respect to E is lower bounded by the difference of mutual information $I(A;B)-I(A;E)$. Even though A, B, and E here denote continuous variables, we can use this result provided that the generated key and the exchanged reconciliation messages are discrete as required in [20]. Our continuous variables A, B, and E only appear at the right of the conditional bar in entropy formulas, so they can be approximated by discrete numbers (that is, they can be replaced by an integer such as $\lfloor nA \rfloor$, approximating the real variable A). As n grows, this will approximate the real variable with a precision far beyond what is needed given the noise level. Thus, our protocol is guaranteed to generate a nonzero net key rate provided that $I_B > I_2$, that is, in terms of signal-to-noise ratios $\gamma' > \sqrt{1+\gamma}-1$, where γ' is the actual SNR measured by Bob. This means that a 1-bit channel ($\gamma=3$) may still be used if the noise power is almost tripled ($\gamma'>1$).

In practice, a cryptosystem—even continuous—is of course expected to yield key bits, not continuous keys. So, the procedure proposed here consists in performing the quantum distribution of a (real) Gaussian key followed by a discretization procedure so as to apply some (discrete) reconciliation and privacy amplification protocols. The detail of the extraction of a binary key from a Gaussian key will be investigated in a further paper [21]. Such a strategy has the advantage of circumventing a weakness of the squeezed-state cryptosystems as presented in Refs. [9–11]. There, the key is binary (or belongs to a larger finite alphabet), so there are gaps between the discrete key values. This allows Eve to gain knowledge about the occurrences where she measured the wrong quadrature (without getting the key value). For example, if Alice sends $\pm V$ to encode a bit 0 or 1 and Eve gets a real value around zero, then Eve can deduce with a high probability that she measured the wrong quadrature. This knowledge alone is sufficient for her to attack the key distribution scheme simply by omitting to resend the corresponding key element to Bob, thereby faking an attenuation in the transmission. This limitation does not apply to our scheme since the key values continuously fill in an entire region in the (X_1,X_2) phase space, the marginal distributions of X_1 or X_2 being independent of the encoding basis.

In conclusion, an all-continuous quantum cryptographic protocol was proposed that is based on single-mode squeezed states of the electromagnetic field. It exploits the uncertainty relation between the conjugate pair of quadrature components X_1 and X_2 by encoding a continuous Gaussian-distributed key into either X_1- or X_2-squeezed states, thereby allowing a continuous key distribution between two remote parties. It is shown that the information acquired by an eavesdropper on the key elements encoded in X_1 is compensated by a reduction (by the same amount) of the key information available on the X_2 amplitude at the receiver's station. This information-theoretic trade-off characterizes the worst-case individual attack based on the cloning machine, so we conclude that the loss of information at the receiver's end is a good upper bound on the tapped information. A realization of this continuous protocol based on squeezed states would be very challenging as the generation of squeezed light has been a difficult experimental task for years. Also, it would require synchronized local oscillators at Alice's and Bob's stations in order for them to have a common phase for homodyne detecting the amplitudes X_1 and X_2. In addition, probably the main limitation in the implementation of this protocol is related to the loss of squeezing effected by attenuation in the transmission medium. This would dramatically decrease the SNR and make the protocol less efficient (or insecure). In analogy with what is known for BB84, there probably is a threshold on the squeeze parameter that Alice should reach below which the protocol would fail. Nevertheless, it should be stressed that the cryptographic protocol proposed here was analyzed using the conjugate pair (X_1,X_2), but other complementary variables might be exploited as well. In particular, one could imagine a continuous cryptographic scheme based on the time-frequency complementarity where ultrashort single-photon pulses or, alternatively, single-photon pulses that are highly peaked in frequency would be used in order to encode the Gaussian key. Such a scheme might possibly avoid some of the weaknesses of the squeezed state protocol and be more appropriate for an experimental realization.

We are grateful to Jonathan Dowling, Nicolas Gisin, Sofyan Iblisdir, Serge Massar, and Hugo Zbinden for helpful discussions. G.V.A. acknowledges the support from the Banque Nationale de Belgique.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[4] H. Zbinden *et al.*, Appl. Phys. B: Lasers Opt. **B67**, 743 (1998).
[5] P. D. Townsend, Opt. Fiber Technol.: Mater., Devices Syst. **4**, 345 (1998).
[6] T. Jennewein *et al.*, Phys. Rev. Lett. **84**, 4729 (2000); D.S. Naik *et al.*, *ibid.* **84**, 4733 (2000); W. Tittel *et al.*, *ibid.* **84**, 4737 (2000).
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[9] T. C. Ralph, Phys. Rev. A **61**, 010303 (2000).
[10] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[11] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[12] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[13] N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301 (2000).
[14] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley New York, 1991).
[16] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, England, 1997).
[17] C. A. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997).
[18] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999); D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[19] T. C. Ralph, Phys. Rev. A **62**, 062306 (2000).
[20] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[21] G. Van Assche, J. Cardinal, and N. J. Cerf (unpublished).