Continuous variable quantum cryptography using coherent states

Frédéric Grosshans, Philippe Grangier

To cite this version:

Frédéric Grosshans, Philippe Grangier. Continuous variable quantum cryptography using coherent states. Physical Review Letters, 2002, 88, pp.057902. 10.1103/PhysRevLett.88.057902 . hal-00509124

HAL Id: hal-00509124
https://hal.science/hal-00509124

Submitted on 3 Jun 2016

Continuous Variable Quantum Cryptography Using Coherent States

Frédéric Grosshans and Philippe Grangier
Laboratoire Charles Fabry de l'Institut dOptique (CNRS UMR 8501), F-91403 Orsay, France

(Received 24 September 2001; published 16 January 2002)

We propose several methods for quantum key distribution (QKD) based on the generation and transmission of random distributions of coherent or squeezed states, and we show that they are secure against individual eavesdropping attacks. These protocols require that the transmission of the optical line between Alice and Bob is larger than 50%, but they do not rely on "sub-shot-noise" features such as squeezing. Their security is a direct consequence of the no-cloning theorem, which limits the signal-to-noise ratio of possible quantum measurements on the transmission line. Our approach can also be used for evaluating various QKD protocols using light with Gaussian statistics.

DOI: 10.1103/PhysRevLett.88.057902 PACS numbers: 03.67.Dd, 42.50.Dv, 89.70.+c

Since the experimental demonstration of quantum teleportation of coherent states [1], a lot of interest has arisen in continuous variable quantum information processing. In particular, a stimulating question is whether quantum continuous variables (QCV) may provide a valid alternative to the usual "single photon" quantum key distribution schemes [2]. Most present proposals to use QCV for quantum key distribution (QKD) [3–15] are based upon the use of "nonclassical" light beams, such as squeezed light, or pairs of light beams that are correlated for two different quadrature components (the so-called "EPR" beams, by analogy with the historical paper by Einstein, Podolsky, and Rosen [16]). But recent work on this subject [17] underlined the crucial importance of the continuous variable version of the no-cloning theorem [18], as soon as security is concerned in any exchange using QCV.

In this Letter, we show that there is actually no need for squeezed light: An equivalent level of security may be obtained by simply generating and transmitting random distributions of coherent states. The security of this novel protocol is related to the no-cloning theorem, which limits possible eavesdropping even though the transmitted light has no "sub-shot-noise" feature such as squeezing. We show that our analysis can be also applied to other protocols using light with Gaussian statistics, i.e., squeezed or EPR beams, thus making the comparison easier. The basic tools for this analysis are the ones that have been extensively used for linearized quantum optics, including in particular optical quantum nondemolition (QND) measurements [19]. A brief review of the current literature on continuous variables QKD is presented in [20]. Here we consider security against individual attacks only, and we do not address the issue of unconditional security, which was demonstrated in [3] for squeezed states protocols (unconditional security of coherent states protocols remains an open question). Our results can be seen as a generalization of previous single beams protocols [4–12], based on the Gaussian reconciliation method proposed in [6,7]. "Single beam" means that the present approach does not include protocols transmitting simultaneously several quantum-correlated modes of the electromagnetic field [8,13–15], because their security analysis should take into account simultaneous attack on these modes. However, extensions of our methods to any kind of protocol using Gaussian variables should be possible.

General principle of the protocols.—The QKD protocols we study here are single Gaussian beam protocols. Alice modulates randomly a Gaussian beam and sends it to Bob through a Gaussian noisy channel. Both phase and amplitude are modulated with Gaussian random numbers, since this allows an optimal information rate [21]. Bob then measures either the phase or the amplitude of this beam and informs Alice which measurement he made. Bob and Alice have then two correlated sets of Gaussian variables, from which they can extract a common secret string of bits as explained below.

The basic tool that we will use is the Shannon formula giving the optimum information rate I of a noisy transmission channel, in units of bits/symbol [21]. If the noise is white and Gaussian and the signal-to-noise ratio (SNR) is Σ, this optimum information rate is

$$I_{AB} = 1/2 \log_2(1 + \Sigma). \tag{1}$$

Since this optimum can be closely approached only if the signal has Gaussian statistics [21], we will consider only Gaussian modulation protocols, and use (1) to calculate the amount of private information that Alice and Bob may exchange in the presence of the eavesdropper Eve. The sliced reconciliation protocol described in detail in [6,7] and briefly sketched in the Appendix allows us to get arbitrarily close to the value given by (1). For security purposes, one must assume that Eve has an arbitrarily powerful computer, and thus she is able to reach this limit. In case Alice and Bob are not, they will have to allow for an extra security margin (see *Discussion* below).

After the data exchange and reconciliation, Alice and Bob share a string of bits which may be partly known by Eve, and they also know the transmission error rate (possibly due to Eve) by comparing a subset of the exchanged data. They can then use standard privacy amplification protocol [22] to agree on a secret key. This secret key can be constructed at the rate [23]

$$\Delta I = I_{AB} - I_{AE}\,, \tag{2}$$

where I_{AB} (I_{AE}) is the information rate between Alice and Bob (Eve).

Eavesdropping.—The I_{AB} term of (2) is easy to compute for a given scheme, the SNR value Σ_B being known. We have to assume I_{AE} is being the maximum possible given the laws of physics (considering here only individual attacks). If the protocols are globally invariant under the exchange of the two quadratures X and P, the best tactic for Eve is to keep this property in her attacks. Therefore, we can restrict ourselves to attacks that treat equally both quadratures without loss of generality.

Given these hypothesis, we will use a general result, which is demonstrated in [17] (see also [5,9]): If the added noise on Bob's side is χN_0, where N_0 is the vacuum noise variance, then the minimum added noise on Eve's side is $\chi^{-1}N_0$. This applies to both quadratures, and the added noise may be due to line losses, eavesdropping, or any other reason [17]. Since the demonstration of Ref. [17] is just another form of the no-cloning theorem, it also addresses any individual attack by Eve using a cloning machine [18]. When the line has a transmission η with no Eve present, one has $\chi = (1 - \eta)/\eta$. The best attack for Eve is then to take a fraction $1 - \eta$ of the beam at Alice's site, and to send the fraction η to Bob through her own lossless line (that may be a perfect teleporter). Eve is then totally undetected, and she gets the maximum possible information according to the no-cloning theorem. More generally, Eq. (2) shows that the exchange is secure as long as Bob has more information on Alice's key than Eve, i.e., as long as $I_{AB} > I_{AE}$. Since the Shannon formula (1) is valid for both Bob and Eve, the security condition is just a condition on the SNR, which turns to be a condition on the added noises:

$$\Delta I > 0 \Leftrightarrow \Sigma_B > \Sigma_E \Leftrightarrow \chi < 1\,. \tag{3}$$

Since $\chi = (1 - \eta)/\eta$ for a line with transmission η, the condition $\chi < 1$ requires that $\eta > 1/2$. Therefore, a usable key can be obtained in principle as soon as the transmission losses are less 3 dB. Taking into account the standard loss of 0.2 dB/km in optical fibers at 1550 nm, the typical range would be around 10 km.

In this security evaluation, the noise added in Alice's side cancels out because it disturbs equally Eve and Bob. This "canceled" noise includes the quantum noise of the beam. As a consequence, the security of these protocols relies on the quantum aspects of measuring or copying quantum states, but not on the use of squeezing or entanglement. We can do quantum cryptography with coherent beams, as mentioned in [3,8,9], or even with highly noisy beams (in that case Alice should measure the amplitude of the beam, split off a small part, and send it to Bob). Quantum features of the beams might influence some characteristics of the protocol such as the secret key rate or the amount of classical communication needed to agree on the secret key, but not its security.

Coherent beam protocol.—Let us now explicitly describe the coherent beam protocols of this family: (i) Alice draws two random numbers x_A and p_A from a Gaussian law with variance $V_A N_0$. (ii) She sends to Bob the coherent state $|x_A + ip_A\rangle$. (iii) Bob randomly chooses to measure either X or P. This measurement can be done perfectly. (iv) Using a classical public channel, he informs Alice about the observable that he measured (as in the BB84 protocol, half of the key generated by Alice is unused). (v) Alice and Bob share two correlated Gaussian variables. Then they may use the "sliced reconciliation" protocol [6,7] to transform it into errorless bit strings. Finally, they have to use a standard protocol for privacy amplification [22] in order to distill the private key.

According to Eq. (1), the channel rate ΔI for the private key will be

$$\Delta I = \tfrac{1}{2}\log_2(1 + \Sigma_B) - \tfrac{1}{2}\log_2(1 + \Sigma_E)\,. \tag{4}$$

The total variance of any quadrature of the beam when it leaves Alice's realm is $VN_0 = V_A N_0 + N_0$. Using the expressions $1 + \Sigma_B = \frac{V+\chi}{1+\chi}$, and $1 + \Sigma_E = \frac{V+1/\chi}{1+1/\chi}$, the useful secret information rate is

$$\Delta I = \frac{1}{2}\log_2 \frac{V + \chi}{1 + V\chi}\,. \tag{5}$$

If $\chi < 1$, ΔI will increase as a function of the signal modulation V_A. For large modulation ($\chi V_A \gg 1$), the asymptotic value of ΔI is

$$\Delta I_{\mathrm{asymp}} = -\frac{1}{2}\log_2\chi = \frac{1}{2}\log_2\frac{\eta}{1 - \eta}\,, \tag{6}$$

while the raw channel rate between Alice and Bob is $I_{AB} = \frac{1}{2}\log_2[V/(1 + \chi)]$.

Squeezed state protocol.—This protocol can straightforwardly be generalized to the modulated squeezed beam, with a squeezing factor $s < 1$. The protocol becomes as follows: (i) Alice chooses randomly if the beam is squeezed in X or P (for instance we will later assume the beam being X squeezed). Let $|\psi\rangle$ denote this squeezed state. (ii) Alice draws two random numbers x_A and p_A from two Gaussian laws with variances $V_{x_A}N_0$ and $V_{p_A}N_0$. The two squeezed directions are indistinguishable for Eve iff

$$V_{x_A}N_0 + sN_0 = V_{p_A}N_0 + \frac{1}{s}N_0 \equiv VN_0\,. \tag{7}$$

(iii) Alice sends to Bob the displaced squeezed state $D(x_A + ip_A)|\psi\rangle$. (iv) Bob randomly chooses to measure either X or P. (v) Using a public channel, Alice and Bob inform each other about the squeezing direction and the measured observable. (vi) Such as with coherent states, Alice and Bob share correlated Gaussian variables, from which they can extract a private binary key.

This protocol obviously reduces to the protocol described above if $s = 1$. Another limit, where $V_{p_A} = 0$ or $V = 1/s$, is the protocol described by Cerf *et al.* in [5,6]. In this case, information is gathered for the key only when Bob makes the right guess.

To compute the private rate ΔI, we will average between the right guesses and the wrong guesses:

$$\Delta I = \frac{1}{2}[(I_{ABX} - I_{AEX}) + (I_{ABP} - I_{AEP})], \quad (8)$$

$$= \frac{1}{4}\log_2 \frac{(1 + \Sigma_{BX})(1 + \Sigma_{BP})}{(1 + \Sigma_{EX})(1 + \Sigma_{EP})}. \quad (9)$$

We have $\Sigma_{BX} = V_{x_A}/(s + \chi) = \frac{V-s}{s+\chi}$ and $1 + \Sigma_{BX} = \frac{V+\chi}{s+\chi}$. The three other SNR are obtained by replacing χ and/or s by χ^{-1} or s^{-1}. Therefore,

$$I_{AB} = \frac{1}{4}\log_2 \frac{(V + \chi)^2}{\chi} - \frac{1}{4}\log_2\left(\chi + \frac{1}{\chi} + s + \frac{1}{s}\right), \quad (10)$$

$$I_{AE} = \frac{1}{4}\log_2 \frac{(V + 1/\chi)^2}{1/\chi} - \frac{1}{4}\log_2\left(\chi + \frac{1}{\chi} + s + \frac{1}{s}\right). \quad (11)$$

Since the s-dependent term of these information rates are the same, they cancel each other in ΔI. The secret information rate is thus again given by Eq. (5), and does not depend on the degree of squeezing.

Extension to EPR case.—The previous description does not apply directly on EPR protocols. However, an EPR QKD protocol where Alice keeps one of the beams and sends the other to Bob is logically equivalent to a randomly modulated beam with a sub-shot-noise quantum variance. Let X_A denote the quadrature Alice measures and X_{out} the same quadrature of the beam sent to Bob when it leaves Alice's lab. For a standard nonmodulated EPR scheme [11], we have the following relations:

$$\langle X_A^2\rangle = \langle X_{\text{out}}^2\rangle \equiv V = (s + 1/s)/2, \quad (12)$$

$$\langle (X_A - X_{\text{out}})^2\rangle = 2s, \quad (13)$$

$$\langle X_A X_{\text{out}}\rangle = V - s. \quad (14)$$

We can separate Bob's beams into two parts, which are, respectively, correlated and uncorrelated with Alice's measurement, by writing $X_{\text{out}} = gX_A + N$, where $\langle X_A N\rangle = 0$. Bob's beam is then equivalent to a beam with quantum noise $\langle N^2\rangle$ on quadrature X, which is randomly modulated with the variable gX_A. Using Eqs. (12) and (14), one gets

$$g = 1 - s/V = (1 - s^2)/(1 + s^2), \quad (15)$$

$$\langle N^2\rangle = s(2 - s/V) = 2s/(1 + s^2). \quad (16)$$

These equations describe the case where Alice and Bob measure the same quadrature. When Alice changes her quadrature, while Bob keeps the same measurement, the initial wave packet is reduced onto a noisy quadrature, and no useful correlation is generated. On the average, the information rate is therefore half of the "equivalent" modulation scheme. Using (12), we then have

$$1 + \Sigma_B = 1 + \frac{g^2 V}{\langle N^2\rangle + \chi} = \frac{V(V + \chi)}{1 + \chi V}, \quad (17)$$

$$\Delta I = \frac{1}{4}\log_2\left(\frac{V + \chi}{1 + \chi V}\frac{1 + V/\chi}{V + 1/\chi}\right)$$

$$= \frac{1}{2}\log_2\left(\frac{V + \chi}{1 + \chi V}\right). \quad (18)$$

This value of ΔI is again just the same as the coherent state result (5) for given χ and V, so that s is defined by (12). Adding excess noise or a modulation on the outgoing beam brings no further improvement.

Discussion.—Various comments are in order. First, it appears that nonclassical features such as squeezing or EPR correlations have no influence on the achievable secret key rate for the family of protocols that were described here. This result may not apply to all possible protocols; e.g., we did not consider using a continuous quantum memory. On the other hand, since the raw information rate is different for the same secret key rate, squeezed beams can be used to save classical communications during the privacy amplification procedure. The EPR beams have also the advantage of directly providing quantum-generated Gaussian noise, rather than having it externally generated by Alice. More importantly, entanglement, which is not directly used in the present protocols, can be useful to beat the 3 dB limit by using more than one beam. Though the 3 dB loss limit of our cryptography protocols makes their security demonstration quite intuitive, there exist multiple ways for Alice and Bob to go beyond this limit. The most radical way is to send many EPR beams through the noisy channel, then to use entanglement purification [24] to build stored entanglement between Alice and Bob, and finally to implement a high fidelity teleporter. For any finite value of the losses and EPR entanglement, an arbitrarily high fidelity can be achieved [24]. The no-cloning theorem ensures the security of these schemes as soon as the fidelity of the teleporter is above 2/3 [17], which is equivalent to the 3 dB loss limit discussed above. In some sense, a "lossless" line is recreated by using entanglement purification. There may exist more realistic ways to cross the 3 dB barrier, but their security analysis is beyond the scope of this Letter.

On the practical side, one should note that Bob's detectors are not ideal, but have a nonzero electronic noise B_0 that should be much smaller than N_0, and a maximum (saturation) input power $\sigma B_0 \gg N_0$, where $\sigma \gg 1$ is the detector's dynamics. Taking into account these characteristics in the simplest coherent state protocol gives an optimum value of the signal variance, $V_A \sim \sqrt{\sigma}$. Another point is that Alice and Bob may not be able to

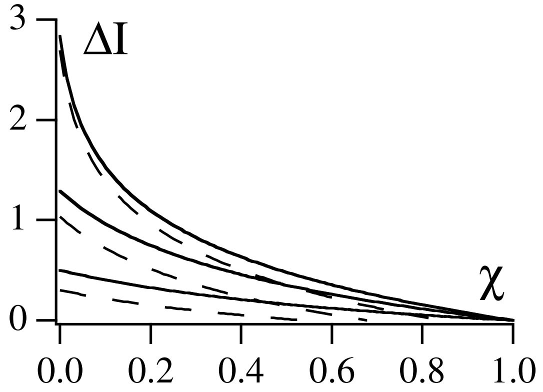

FIG. 1. Private channel information rate ΔI as a function of the channel noise χ. The three curves in solid lines correspond to $V_A = 1$, 5, and 50 from the bottom to the top, assuming that the reconciliation protocol between Alice and Bob reaches the Shannon limit. The three curves in dashed lines correspond to the effective ΔI with the same values of V_A, with (arbitrarily chosen) reconciliation efficiencies α that are, respectively, 0.6, 0.8, and 0.95 of the Shannon limit.

achieve the Shannon limit (1), due to limited computing power (no such limitation is relevant for Eve). Assuming that the effective information rate between Alice and Bob is reduced by a factor $\alpha < 1$, the net secret rate becomes $\Delta I_{\text{eff}} = \alpha I_{AB} - I_{AE}$, and remains positive if $\alpha > I_{AE}/I_{AB}$. The quantity ΔI_{eff} is plotted in Fig. 1 for $\alpha = 1$ (solid lines), and for various values of α that are arbitrarily associated with various values of the SNR (dashed lines). It is clear that low values of α reduce the secure transmission range of the protocol. We note that, according to [6,7], the sliced reconciliation protocol should yield $\alpha \sim 1$, but this may be costly in terms of calculation time and public channel transmissions. All these constraints should eventually be taken into account to choose the most appropriate value of V_A.

In conclusion, it is possible to design a QKD scheme with coherent states, secure against any individual attack, by using optimized reconciliation protocols and privacy amplification. Since the protocol does not require squeezing, it can be implemented by sending light pulses in a low-loss optical fiber, such as in a coherent optical telecommunication scheme. In that case, all pulses will be useful, but half of the information sent by Alice will be lost. We demonstrated that the protocol is asymptotically secure [7] for losses smaller than 3 dB (or a teleportation fidelity larger than 2/3 [17]), and the net information rate for the private key with a large signal modulation is $1/2\log_2(1/\chi) = 1/2\log_2[\eta/(1-\eta)]$.

This work was carried out in the framework of the European IST/FET/QIPC project "QuICoV." We are grateful to N. J. Cerf and G. Van Assche for helpful discussions.

Appendix: Sliced reconciliation protocol.—In the n-slice version of the reconciliation protocol proposed in Ref. [7], the real axis representing the amplitude of the signal is split in 2^n intervals $s_1 =]-\infty, -t_1], s_2 =]-t_1, -t_2], \ldots, s_{2^n} =]t_{2^n-1}, +\infty[$, where $t_p = -t_{2^n-p}$, and $t_{2^{n-1}} = 0$. Alice assigns an amount of n bits to an amplitude that lies in the interval s_p, by using the parity of p for bit 1, the parity of the integer part of $p/2$ for bit 2, and of $p/2^{n-1}$ for bit n. After receiving the data, Bob makes an optimized guess of the first bit value using appropriate weighting functions, which are computed by optimizing the choice of the $\{t_p\}$ (this optimization is made only once, before exchanging the data). After a first correction round by exchanging public data between Alice and Bob, Bob knows the correct value of the first bit. Then he tries to guess the second bit, with a much higher probability of success, because he already knows the first one. By increasing both the SNR Σ and the number of slices, the process gets more and more efficient, keeping the same main idea: After each correction round, Bob can guess the next bit with a higher probability. For the five-slice protocol with $\Sigma = 15$ presented in [7], the probabilities of guessing right for slices four and five are, respectively, 0.976 and 0.999 994, and the efficiency is more than 90% of the Shannon limit $\frac{1}{2}\log_2(16) = 2$.

[1] A. Furusawa *et al.,* Science **282**, 706 (1998).
[2] For a review see, e.g., W. Tittel, G. Ribordy, and N. Gisin, Phys. World **11**, 41 (1998).
[3] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[4] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[5] N. J. Cerf *et al.,* Phys. Rev. A **63**, 052311 (2000).
[6] N. J. Cerf, S. Iblisdir, and G. Van Assche, quant-ph/0107077, 2001 [Eur. Phys. J. D (to be published)].
[7] G. Van Assche *et al.,* cs.CR/0107030 (to be published).
[8] T. C. Ralph, Phys. Rev. A **61**, 010303 (2000).
[9] T. C. Ralph, Phys. Rev. A **62**, 062306 (2000).
[10] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[11] Ch. Silberhorn *et al.,* quant-ph/0109009, 2001.
[12] P. Navez *et al.,* quant-ph/010113, 2001.
[13] S. Lorenz *et al.,* quant-ph/0109018, 2001.
[14] K. Bencheikh *et al.,* J. Mod. Opt. (to be published).
[15] S. F. Pereira *et al.,* Phys. Rev. A **62**, 042311 (2000).
[16] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[17] F. Grosshans and Ph. Grangier, Phys. Rev. A **64**, 010301 (2001).
[18] N. J. Cerf *et al.,* Phys. Rev. Lett. **85**, 1754 (2000); N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301 (2000).
[19] J.-Ph. Poizat *et al.,* Ann. Phys. (Paris) **19**, 265 (1994); Ph. Grangier *et al.,* Nature (London) **396**, 537 (1998).
[20] F. Grosshans and Ph. Grangier, quant-ph/0109084.
[21] C. E. Shannon, Bell Syst. Tech. J. **27**, 623–656 (1948).
[22] G. Brassard and L. Salvail, *Advances in Cryptology–EUROCRYPT93,* Lecture Notes in Computer Science Vol. 765 (Springer-Verlag, Berlin, 1994), pp. 411–423.
[23] U. Maurer, IEEE Trans. Inf. Theory **39**, 733–742 (1993).
[24] L.-M. Duan *et al.,* Phys. Rev. Lett. **84**, 4002 (2000).