Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography

Miguel Navascués,[1] Frédéric Grosshans,[2] and Antonio Acín[1]

[1]ICFO—Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
[2]Laboratoire de Photonique Quantique et Moléculaire, UMR CNRS 8537, ENS Cachan, 61 Avenue du Président Wilson, 94235 Cachan Cedex, France

(Received 4 August 2006; published 10 November 2006)

We analyze the asymptotic security of the family of Gaussian modulated quantum key distribution protocols for continuous-variables systems. We prove that the Gaussian unitary attack is optimal for all the considered bounds on the key rate when the first and second momenta of the canonical variables involved are known by the honest parties.

DOI: 10.1103/PhysRevLett.97.190502 PACS numbers: 03.67.Dd, 03.67.Hk

In 1984, Bennett and Brassard introduced the concept of quantum cryptography and presented the first quantum key distribution (QKD) protocol: BB84 [1]. The original idea was that in quantum mechanics, contrary to classical physics, the observation of a system invariably perturbs the system under observation. Therefore, if two honest parties, Alice and Bob, establish a quantum channel and use it to send information, an eavesdropper's presence could be detected by analyzing how the noise-free channel has changed. It was then shown that QKD protocols are completely secure against any eavesdropping attacks as long as the bit error rates do not exceed a certain value (see, for instance, [2] and references therein). In the meantime, new applications of quantum mechanics to certain information tasks started to develop: coin tossing, dense coding, teleportation, etc.

All these results first appeared in the context of discrete systems, but many of them were later translated into the language of continuous-variables (CV) systems. This is *per se* an interesting theoretical problem. However, the main motivation for dealing with these systems comes from a practical point of view: although the set of feasible operations is reduced, the so-called Gaussian operations are easy to implement and amazingly precise. Quantum cryptography with continuous-variables systems [3–8] was the most immediate result: the transmission of coherent or squeezed pulses of light, together with homodyne measurements, allows one to perform QKD with very high key rates [9].

The security analysis of these new protocols is not straightforward. First, the commonly used reconciliation and privacy amplification protocols are designed to correct and distill secret bits from binary random variables, although some have been adapted to continuous variables [10,11]. Second, the dimension of the Hilbert space on which the CV systems are defined is infinite in theory, which makes a complete tomography impossible in principle, thus preventing Alice and Bob to know precisely the state they are actually sharing. Therefore, security proofs for CV protocols have to consider the optimal attack by Eve when Alice and Bob know their state is in some set, usually defined by the momenta of the quadratures up to second order [12]. In her search for information, Eve's possible attacks can be classified in three different types [13]: individual attacks, where Eve interacts individually with the sent states and measures them individually before public reconciliation; collective attacks, where Eve applies the same unitary individual attack over the sent states but performs her (possibly collective) measurements at any time during Alice and Bob's reconciliation protocol; coherent attacks, where Eve is allowed to perform any unitary collective interaction over the sent states and any measurement strategy at any time she wants. The latter is the most general attack Eve can use. Most of the present security proofs give necessary and sufficient conditions for key distillation when Eve is restricted to perform an individual [4,5] or finite-size coherent attack [12]. General proofs of security are given in [3] for a squeezed-state protocol and in [14,15] for coherent states.

Recently, bounds on extractable key rates have been derived for the case of collective [16,17] and general attacks [18]. These bounds are easy to adapt to a wide class of protocols since they correspond to the difference of smooth entropies, which tend to von Neumann or Shannon entropies in the asymptotic case. In this work we analyze a family of CV protocols based on Gaussian modulation. This family includes most of the protocols in the field of CV systems, such as those of Ref. [5] using squeezed light, or those of Refs. [6,8] that employ coherent states. We prove that for all of them, the Gaussian attack is the unitary attack by Eve that minimizes the bounds on the key rate of [16,17], when Alice and Bob know the quadrature momenta of their state up to the second order. Therefore, Gaussian attacks turns out to be optimal for these protocols. We consider quantum systems of n canonical degrees of freedom, called modes, belonging to $B(\mathcal{H}(\mathbb{R}^n))$. These are characterized by the set of operators $\vec{\Xi} = (\Xi_1, \ldots, \Xi_{2n}) = (Q_1, P_1, \ldots, Q_n, P_n)$ satisfying the canonical commutation relations $[\Xi_j, \Xi_k] = i(\sigma_n)_{jk}$, where σ_n is the n-mode symplectic matrix,

$$\sigma_n = \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1}$$

A state is said to be Gaussian iff its density matrix, $\tilde{\rho}$, is the exponential of a quadratic function f on the canonical operators of the system, i.e.,

$$\tilde{\rho} = \exp[-f(\vec{\Xi})]. \tag{2}$$

Because of their simple structure, any Gaussian state can be completely described in terms of its displacement vector, d, and its covariance matrix, γ, both defined as

$$\begin{aligned} d_k &= \langle \Xi_k \rangle = \mathrm{tr}(\rho \Xi_k), \\ \gamma_{kl} &= \mathrm{tr}(\rho\{\Xi_k - d_k, \Xi_l - d_l\}_+), \end{aligned} \tag{3}$$

where $\{\cdots\}_+$ denotes the anticommutator. Therefore, Gaussian states are characterized just by the first and second order momenta of the canonical variables $\vec{\Xi}$. Gaussian operations are completely positive maps that map Gaussian states into Gaussian states.

The considered CV QKD protocols are based on random Gaussian modulation of squeezed or coherent states of light [5,6,8]. They are prepare and measure (PM) protocols, suitable to realistic implementation with today's technology. However, for any PM protocol there exists a completely equivalent entanglement-based scheme [19]. This description simplifies the theoretical analysis, even if it would be more difficult to implement experimentally. The entanglement-based scheme consists of the following five steps (see also [20]): (1) Alice prepares a two-mode squeezed state. (2) She performs a measurement over the first mode. This measurement projects the second mode into a randomly displaced (possibly squeezed) state. If Alice performs a heterodyne measurement, she effectively prepares a coherent state on the second mode. If she randomly chooses to perform a homodyne measurement on Q or P, she is effectively preparing a randomly displaced squeezed state. (3) She sends the second mode to Bob via a noisy quantum channel. (4) Bob receives the state sent by Alice. He performs either a homodyne measurement in Q or P, or a heterodyne measurement, his result being y. (5) Alice and Bob apply one-way error correction and privacy amplification codes to distill a perfect secret key. If the classical communication flows from Alice to Bob, we speak about direct reconciliation. On the contrary, if it is Bob who sends the classical information to Alice during the reconciliation process, we say they are using a reverse reconciliation protocol [21].

Recently, general bounds on the extractable key rate under collective attacks have been published [16,17]. All of them exploit the entanglement-based picture, but of course they also apply to the corresponding PM scheme. They are expressed in terms of entropy quantities. Throughout this work, the same notation H is used for the (classical) Shannon entropy and the (quantum) von Neumann entropy. Let $X(Y)$ be the random variable associated with Alice's (Bob's) measured quantity and by $x(y)$ its value. According to [16,17], the key rate K obtained using direct reconciliation is bounded by

$$K \geq I(X{:}Y) - \chi(X{:}E) \equiv K_{\mathrm{coll}}. \tag{4}$$

Here $I(X{:}Y)$ denotes the classical mutual information, $I(X{:}Y) = H(Y) - H(Y|X)$, while χ refers to the Holevo bound [22],

$$\chi(X{:}B) = H(B) - H(B|X), \tag{5}$$

where $H(B|X) = \sum_x p(x) H(B|X = x)$. Formally, I and χ look identical, but they refer to different types of variables. While the mutual information deals only with classical random variables, the Holevo bound quantifies the accessible classical information on quantum states. This justifies the different notation.

Suppose now that Bob is allowed to use a collective arbitrary measurement on many copies of the received states. Of course, this is a rather unrealistic scenario, but it provides an upper bound to the maximum one-way secret-key rate when Bob is free to perform any individual measurement. If, again, Eve is restricted to apply collective attacks, the key rate, upon Bob optimizing his measurement, is given by [16]

$$K \geq \chi(X{:}B) - \chi(X{:}E) \equiv K'_{\mathrm{coll}}. \tag{6}$$

In these two bounds, namely, Eqs. (4) and (6), the first term specifies the correlation between the honest parties. It quantifies the amount of classical information Alice and Bob should exchange to correct their errors. The second term estimates Eve's knowledge on Alice's (or Bob's) variable. It is thus related to the amount of privacy amplification required to make Eve's information vanishing.

Eve's attack has to be defined in order to compute the secret-key rate and therefore needs to be optimized. Indeed, after the estimation strategy, Alice and Bob have some knowledge about their state, this information being denoted by g. In the calculation of key rates, as for any other interesting function, Alice and Bob should minimize (4) or (6) over the set G, consisting of all states ρ compatible with g (see also [23]).

In the CV scenario, it is natural to take g, i.e., Alice and Bob's information on their state, as the first and second moments on the measured quadratures. The first order correlations do not play any role in the discussion, as they can be changed arbitrarily by the use of local unitaries. As shown in the next lines, for fixed second (and first) moments, the corresponding Gaussian state optimizes the bounds on the key rates given above. Interestingly, the Gaussian attack turns out to maximize Eve's information as well, $\chi(X{:}E)$. Before proceeding with the proof of these results, we spend some lines clarifying the notation used from now on.

Let $\rho \in B(\mathcal{H}^2)$ be a density matrix in any Hilbert space $\mathcal{H}$. Then $\tilde{\rho}$ denotes the corresponding density matrix of a

Gaussian state characterized by the same covariance matrix and displacement vector as ρ. Analogously, if $p(\vec{x})$ is a probability distribution, then $\tilde{p}(\vec{x})$ (or $\tilde{p}$ for short) denotes the Gaussian probability distribution with the same first and second momenta as $p(\vec{x})$. Moreover, if $F(\vec{x})$ represents any quantity concerning a variable $\vec{x}$, described by a certain distribution $p(\vec{x})$, then $\tilde{F}$ has to be understood as the same functional F calculated from the distribution $\tilde{p}$. $\tilde{\Delta}F$ will be a shorthand notation for the difference of these two quantities, $\tilde{\Delta}F = \tilde{F} - F$.

Three results are used in what follows. First, let $\rho \in B(\mathcal{H}^2)$ be any physical state of a system A and $\bar{\rho}$ the one into which ρ is transformed after the measurement of the classical variable X. The measurement is defined by a set of positive operators $\{M_x\}_x$ obeying $\sum_x dx M_x M_x^\dagger = \mathbb{I}$. Note that X can refer just to one real variable, as in the case of a homodyne measurement, or to a pair of real variables, as in the case of a heterodyne measurement, with $x = (q, p)$, $dx = dqdp$. One has

$$\bar{\rho} = \sum_x |x\rangle\langle x| dx M_x \rho M_x^\dagger = \sum_x p(x) dx |x\rangle\langle x| dx \otimes \rho_{|x}, \quad (7)$$

where $\rho|x$ is the normalized state of ρ knowing $X = x$,

$$\rho_{|x} = \frac{M_x \rho M_x^\dagger}{p(x)}, \quad (8)$$

and $p(x) = \mathrm{tr}(M_x \rho M_x^\dagger)$. It is straightforward to check that

$$H(A|X) = H(\bar{A}) - H(X), \quad (9)$$

where H denotes the Shannon entropy for the measurement outcomes, i.e., $H(X) = -\sum_x p(x) dx \log(p(x)dx)$, $H(\bar{A}) = -\mathrm{tr}\bar{\rho}\log\bar{\rho}$ is the von Neumann entropy of the measured quantum state $\bar{\rho}$ and the conditional entropy $H(A|X)$ is $\sum_x p(x) dx S(\rho_{|x})$. In the case of continuous variables, this expression is not bounded in the limit $dx \rightarrow 0$. Therefore, we will only take such limit (if necessary) for the computation of the final mutual (or Holevo) information quantities, which stay finite.

Second, for any state ρ, one has [24]

$$\tilde{\Delta}H(A) = H(\rho \parallel \tilde{\rho}) \geq 0, \quad (10)$$

where $H(\rho \parallel \tilde{\rho})$ denotes the relative entropy

$$H(\rho \parallel \tilde{\rho}) = \mathrm{tr}(\rho \log\rho) - \mathrm{tr}(\rho \log\tilde{\rho}). \quad (11)$$

Note that since the relative entropy is never negative, the state of maximal entropy for fixed first and second moments is Gaussian [24]. In particular, if Alice and Bob share a state ρ_{AB}, they can bound its entropy from its covariance matrix, that is, $H(\rho_{AB}) \leq H(\tilde{\rho}_{AB})$. Using similar arguments, it can be seen that the same property is fulfilled by probability distributions, i.e.,

$$\tilde{\Delta}H(X) = H(X \parallel \tilde{X}), \quad (12)$$

where

$$H(X \parallel \tilde{X}) = \sum_x p(x) dx \log\left(\frac{p(x)}{\tilde{p}(x)}\right). \quad (13)$$

Third, the relative entropy (11) never increases after the application of a trace-preserving map (or a stochastic map in the classical case). That is, for any of those maps, denoted by $\mathcal{T}$, and any two states, ρ_1 and ρ_2,

$$H(\rho_1 \parallel \rho_2) \geq H(\mathcal{T}(\rho_1) \parallel \mathcal{T}(\rho_2)). \quad (14)$$

This obviously implies

$$\tilde{\Delta}H(A) \geq \tilde{\Delta}H(\mathcal{T}(A)), \quad (15)$$

for any Gaussian trace-preserving channel $\mathcal{T}$, and for any quantum state or classical random variable A.

To prove the optimality of Gaussian attacks, we first show that for fixed first and second moments, the Gaussian attack maximizes Eve's information, $\chi(X{:}E)$. In order to give the maximal allowed information to Eve, one has to consider that the global state shared by Alice, Bob, and Eve is pure. However, it must be noted that Alice and Bob's state refers to any canonical degree of freedom belonging to their local Hilbert spaces, including those not subject to measurement (if any). This observation allows, for example, one to treat the problem of errors in the measuring process. Indeed, suppose the errors on Bob's measurement can be modeled by an n-mode system where only a fraction of the modes are measured. For the calculation of $\chi(X{:}E)$, all the n modes should be considered. Otherwise, we would be giving Eve more power than what she actually has. Then,

$$\begin{aligned} \tilde{\Delta}\chi(X{:}E) &= \tilde{\Delta}H(E) - \tilde{\Delta}H(E|X) \\ &= \tilde{\Delta}H(AB) - \tilde{\Delta}H(AB|X) \\ &= \tilde{\Delta}H(AB) - \tilde{\Delta}H(\overline{AB}) + \tilde{\Delta}H(X), \end{aligned} \quad (16)$$

where we first use the fact that the global state is pure and then (9). Now, since the channel $AB \rightarrow \overline{AB}$ defined by the X measurement is Gaussian, $\tilde{\Delta}H(AB) - \tilde{\Delta}H(\overline{AB})$ is not negative. This, together with (10), implies that

$$\tilde{\Delta}\chi(X{:}E) = \tilde{\chi}(X{:}E) - \chi(X{:}E) \geq 0, \quad (17)$$

so the Gaussian attack maximizes Eve's information for fixed first and second moments.

Furthermore, the mutual information between Alice and Bob is minimized if Eve's attack is Gaussian: one has

$$\tilde{\Delta}I(X{:}Y) = \tilde{\Delta}H(X) + \tilde{\Delta}H(Y) - \tilde{\Delta}H(XY) \leq 0. \quad (18)$$

The first term is null since Alice's modulation is Gaussian, and the difference of the last two terms is negative, following from (15), for the map $XY \rightarrow Y$. The optimality of Gaussian attacks is therefore proved. A very similar argument can be used to prove the optimality of these attacks with respect to Eq. (6).

It is important to stress here that most of the known bounds on the secret-key rate, including Eqs. (4) and (6), were introduced for finite-dimensional systems, so in principle they should be carefully applied to the continuous case. However, in Ref. [15], it is shown that the sliced-reconciliation CV protocol of [10] achieves the rate (4) for the case of collective attacks. This result has to be combined with the fact that, for discrete variable systems as well as for continuous-variable systems, collective attacks are the most powerful general attacks [18]. This means that the bounds considered in this Letter actually provide general security bounds for CV systems. The explicit computation of these bounds for the Gaussian case, now proven to be optimal, can be found in [25].

Before concluding, we would like to comment on the recent related results of [23]. There, it was shown that, for a given covariance matrix, the state with minimal distillable secret-key rate is Gaussian, assuming the distillable secret-key rate is a continuous functional. This implies that, up to the continuity assumption, Alice and Bob, for fixed first and second moments, can safely assume their state to be Gaussian, whenever they are able to apply any protocol. This result is very interesting and satisfactory from a theoretical point of view. However, one should be careful when applying it to a practical scenario. Indeed, the distillable secret-key rate is defined with respect to the optimal protocol. However, the optimal protocol can be very challenging from a practical point of view. For instance, it may include local coherent and non-Gaussian operations among several copies of the state. In particular, it may be quite different from the realistic protocol considered here, where the techniques (measurements) used for the correlation distribution are fixed and experimentally feasible. Thus, one cannot directly apply the results of [23] to the considered protocols and conclude that the optimal collective attack is Gaussian.

We have studied the security limits for the CV QKD protocols proposed in [6,8], using the recently obtained lower bounds on the secret-key rate under collective and general attacks, and we have proven the optimality of Gaussian attacks for these bounds.

In order to improve the derived security conditions, note that we have always studied the situation in which Alice and Bob use one-way reconciliation protocols. Two-way communication protocols should be analyzed as well, to completely solve the problem of secret-key extraction. Such protocols (e.g., CASCADE [26]) have already been used in key distribution experiments [9] or in the scheme proposed in [7], even if the security analysis for these cases is only preliminary yet.

The research of F. G. was supported by a Marie Curie Intra-European Fellowship within the 6th European Community Framework Programme (Contract No. MEIF-CT-2003-502045). M. N. and A. A. acknowledge financial support from the Spanish MEC, under a ''Ramón y Cajal'' grant and the FIS2204-05639-C02-02 project, and the Fundación Ramón Areces.

Note added.—The optimality of Gaussian attacks has been also proven using different techniques in [27].

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), Vol. 175.
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[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, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[7] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[8] C. Weedbrook *et al.*, Phys. Rev. Lett. **93**, 170504 (2004).
[9] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[10] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[11] K.-C. Nguyen, G. Van Assche, and N. J. Cerf, cs.IT/0406001; M. Bloch, A. Thangaraj, and S. W. McLaughlin, cs.IT/0509041.
[12] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[13] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[14] S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
[15] G. Van Assche, S. Iblisdir, and N. J. Cerf, Phys. Rev. A **71**, 052304 (2005).
[16] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); Proc. R. Soc. A **461**, 207 (2005).
[17] R. König, U. Maurer, and R. Renner, IEEE Trans. Inf. Theory **51**, 2391 (2005).
[18] R. Renner, Ph.D. thesis, ETH Zürich [quant-ph/0512258].
[19] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[20] F. Grosshans *et al.*, Quantum Inf. Comput. **3**, 535 (2003).
[21] F. Grosshans and Ph. Grangier, in *Proceedings of the Sixth International Conference on Quantum Communications, Measurement, and Computing*, edited by J. H. Shapiro and J. O. Hirota (Rinton Press, Princeton, NJ, 2002), p. 351.
[22] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[23] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[24] E. T. Jaynes, Phys. Rev. **106**, 620 (1957).
[25] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005); M. Navascués and A. Acín, *ibid.* **94**, 020505 (2005).
[26] G. Brassard and L. Salvail, in *Proceedings of Advances in Cryptology Eurocrypt'93*, edited by T. Helleseth, Lecture Notes in Computer Science Vol. 765 (Springer-Verlag, New York, 1994), p. 410.
[27] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).