

Quantum Key Distillation from Gaussian States by Gaussian Operations

M. Navascués,¹ J. Bae,¹ J. I. Cirac,² M. Lewenstein,^{1,3} A. Sanpera,^{1,3} and A. Acín¹

¹*ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, E-08034 Barcelona, Spain*

²*Max-Planck Institut für Quantenoptik, Hans-Kopfermann Strasse 1, D-85748 Garching, Germany*

³*Institut für Theoretische Physik, Universität Hannover, D-30167 Hannover, Germany*

(Received 24 May 2004; published 11 January 2005)

We study the secrecy properties of Gaussian states under Gaussian operations. Although such operations are useless for quantum distillation, we prove that it is possible to distill a secret key secure against any attack from sufficiently entangled Gaussian states with nonpositive partial transposition. Moreover, all such states allow for key distillation, when Eve is assumed to perform finite-size coherent attacks before the reconciliation process.

DOI: 10.1103/PhysRevLett.94.010502

PACS numbers: 03.67.Dd, 03.65.Ud

Quantum information theory (QIT) analyzes the possibilities offered by quantum states for information encoding and transmission. New processes, such as teleportation [1], more powerful algorithms [2], or completely secure data transmission [3] become possible by exploiting quantum effects. Most of the QIT applications use entanglement as a resource. It is therefore one of the most important tasks of QIT to determine if a given state is entangled, and if yes, whether its entanglement is “useful” for information processing. Distillable states [4,5] possess such useful entanglement: using several copies of them and local operations and classical communication (LOCC), one can create a smaller number of maximally entangled states, which can be used for variety of quantum information tasks. Given a state, its distillable entanglement, E_D , measures the amount of pure-state entanglement that can be extracted from it. Particularly important for cryptography is another measure of entanglement K_D : it specifies the number of secret bits that can be extracted from a quantum state using LOCC. Obviously, $K_D \geq E_D$, since a secret key can always be extracted from distilled maximally entangled states, using, for instance, the Ekert protocol [6]. Entangled states which cannot be distilled, i.e., for which $E_D = 0$, exist and are termed “bound entangled” [7]. Although it was unclear whether these states could contain useful entanglement, it has been recently shown that there exist bound entangled states for which $K_D > E_D = 0$ [8].

All of the above results were originally considered for finite-dimensional systems. More recently, many of these concepts have been translated to the infinite dimensional case [9]. In these systems, a key role is played by the set of Gaussian states and Gaussian operations. First of all, it naturally appears in experiments. In fact, non-Gaussian operations turn out to be very challenging from an experimental point of view. Moreover, the theoretical analysis of Gaussian states and operations is also simplified since all their properties can be expressed in terms of finite-dimensional matrices.

To analyze the limitations and possibilities offered by the Gaussian scenario is a relevant issue. The teleportation of coherent states of light have been experimentally dem-

onstrated [10]. Quantum cryptography has also been successfully translated into the Gaussian regime. Gottesman and Preskill proposed to use squeezed states and homodyne measurements in a “prepare and measure” scheme [11]. Actually, no squeezing is required, since coherent states are already sufficient for a secure key distribution with Gaussian operations [12,13]. The experimental implementation of a coherent-state protocol has been recently realized in [14]. From a more fundamental point of view, it is interesting to know which information tasks can be achieved in the Gaussian regime. It is known that all Gaussian states have a positive Wigner function; i.e., there is a local variable model reproducing all the (symmetrically ordered) correlations for Gaussian states. Despite the existence of this local description, these states and operations are useful for teleporting quantum states, or for secure information transmission, applications that are impossible in a classical scenario.

An important negative result in this context was obtained in Refs. [15,16]: quantum distillation by Gaussian operations is impossible. That is, although it is known that all Gaussian states with nonpositive partial transposition (NPPT) are distillable [17], any distillation protocol must include a non-Gaussian operation. This can be rephrased saying that *all entangled mixed states are bound entangled in the Gaussian scenario*. In this scenario, it is natural to define the corresponding Gaussian versions of entanglement measures that specify the entanglement properties of these states under Gaussian local operations and classical communication (GLOCC). For example, GE_D defines the Gaussian distillable entanglement. The results of [15,16] imply that $GE_D = 0$. However, these states may still be useful, since perhaps *secret bits* can be extracted from them using GLOCC.

In a similar way as for distillable entanglement, for any entangled state one can denote by GK_D the amount of secret bits that can be extracted by GLOCC. This quantity refers to the distribution of a secret key and, in principle, is independent of entanglement distillability. Thus, secret bits (GK_D) appear as a resource (measure) especially suitable for the analysis of entangled Gaussian states under

Gaussian operations: while $GE_D = 0$ for all states, there are states with positive GK_D [11,13].

In this work we analyze the secrecy properties of Gaussian states under Gaussian operations [18]. In a similar way as for entanglement distillation, it is assumed that Alice and Bob share N independent copies of a known Gaussian state. We introduce a Gaussian protocol for key distillation and study its security, under the mentioned assumption in the state preparation, in the following scenarios: (i) individual and finite coherent attacks, (ii) the coherent attack proposed in Ref. [19], and (iii) any attack. In the first case, we prove that all NPPT states are secure. Then, it is shown that our security proof ceases to work for some NPPT states under the second scenario. For the last situation, using the recent techniques of Ref. [20], we demonstrate the security of sufficiently entangled Gaussian states.

We consider quantum systems of n canonical degrees of freedom, often called modes, $\mathcal{H} = \mathcal{L}^2(\mathbb{R}^n)$. The commutation relations for the canonical coordinates $R = (X_1, P_1, \dots, X_n, P_n) = (R_1, \dots, R_{2n})$ read $[R_a, R_b] = i(J_n)_{ab}$, where $a, b = 1, \dots, 2n$ and

$$J_n = \oplus_{i=1}^n J, \quad J \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (1)$$

The characteristic function, $\chi_\rho(x)$, of a state ρ is defined as $\chi_\rho(x) \equiv \text{tr}[\rho W(x)]$, where $W(x) = \exp(-ix^T R)$ are the so-called Weyl operators. Gaussian states are those states such that χ_ρ is a Gaussian function,

$$\chi_\rho(x) = \exp\left(ix^T d - \frac{1}{4} x^T \gamma x\right), \quad (2)$$

where d is a $2n$ real vector, called a displacement vector (DV), and γ is a $2n \times 2n$ symmetric real matrix, known as a covariance matrix (CM). The positivity condition of ρ implies that $\gamma - iJ_n \geq 0$. All the information about d and γ is contained in the first and second moments $\text{tr}(\rho R_i)$ and $\text{tr}(\rho R_i R_j)$.

In what follows we consider two parties, Alice and Bob, that share a state ρ in a composite systems of $n + m$ modes. The global CM is

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix} \geq iJ_{n+m}, \quad (3)$$

where γ_A (γ_B) is the CM for the n -mode (m -mode) Gaussian state of system A (B). The entanglement properties of ρ are completely specified by its CM.

The effect of partial transposition at the level of CMs can be understood from the fact that this map is equivalent to time reversal. After partial transposition on, say, A , the sign of Alice's momenta is changed while the rest of canonical coordinates is kept unchanged. Denote by θ the matrix equal to the identity for the position coordinates and minus the identity for the momenta. Partial transposition means that $\gamma_{AB} \rightarrow \gamma'_{AB} = \theta_A \gamma_{AB} \theta_A$. Therefore, the state ρ has positive partial transposition (PPT) when γ'_{AB} defines a

positive operator; that is, $\gamma'_{AB} \geq iJ_{n+m}$. The PPT criterion provides a necessary and sufficient condition for separability for 1×1 [21] and $1 \times N$ Gaussian states [22], while it is only a necessary condition for the rest of systems [22]. As said above, the nonpositivity of the partial transposition is a necessary and sufficient condition for distillability [17].

Two known results will play an important role in what follows. First, any NPPT Gaussian state of $n + m$ modes can be mapped by GLOCC into an NPPT 1×1 Gaussian and symmetric state [17], whose CM [see Eq. (3)] is

$$\gamma_A = \gamma_B = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \quad C = \begin{pmatrix} c_x & 0 \\ 0 & -c_p \end{pmatrix}, \quad (4)$$

where $\lambda \geq 0$ and $c_x \geq c_p \geq 0$. The positivity condition reads $\lambda^2 - c_x c_p - 1 \geq \lambda(c_x - c_p)$, while the entanglement (NPPT) condition gives

$$\lambda^2 + c_x c_p - 1 < \lambda(c_x + c_p). \quad (5)$$

Second, given an n -mode Gaussian state ρ_1 with CM γ_1 , it is always possible to construct a $2n$ mode pure Gaussian state $|\Psi_{12}\rangle$ such that $\text{tr}_2(|\Psi_{12}\rangle\langle\Psi_{12}|) = \rho_1$ [23]. The global CM γ_{12} [see Eq. (3)] has $\gamma_A = \gamma_1$ and

$$\gamma_B = \theta \gamma_1 \theta, \quad C = J_n S (\oplus_{i=1}^n \sqrt{\lambda_k^2 - 1} \mathbb{1}_2) S^{-1} \theta, \quad (6)$$

where $\{\lambda_k\}$ defines the symplectic spectrum of γ_1 and S is the symplectic matrix such that $S^T \gamma_1 S$ is diagonal.

Having collected all these facts, let us describe how Alice and Bob can distill a key from a distillable $n \times m$ Gaussian state using only Gaussian operations. Since all the NPPT Gaussian states can be mapped into symmetric and entangled states of two modes by GLOCC, we restrict our analysis to this type of states. In equivalent terms, one can think that the first step in the key distillation protocol is the GLOCC transformation of [17] that transforms any NPPT state into an entangled state of this family. Then, both parties measure the X quadrature, where X_A and X_B denote the measured operator and x_A and x_B the obtained outcome. After communication, they accept only those cases where $|x_A| = |x_B| = x_0$. Each party associates the logical bit 0 (1) to a positive (negative) result with the probability $p(i, j)$, with $i, j = 0, 1$. This process transforms the quantum state into a list of correlated classical bits between Alice and Bob. Their error probability, that is, the probability that their symbols do not coincide, is

$$\epsilon_{AB} = \frac{\sum_{i \neq j} p(i, j)}{\sum_{i, j} p(i, j)} = \frac{1}{1 + \exp[4c_x x_0^2 / (\lambda^2 - c_x^2)]}. \quad (7)$$

In order to establish a key, Alice and Bob will now apply the advantage distillation protocol introduced by Maurer [24]. Alice generates the random bit b . Then, she chooses N items from her list of symbols, $\vec{b}_A = (b_{A1}, b_{A2}, \dots, b_{AN})$, and sends to Bob the vector \vec{b} such

that $b_{A_i} + b_i = b \pmod{2}$, $\forall i = 1, \dots, N$, together with the list of chosen symbols. Bob computes $b_{B_i} + b_i$ for his corresponding symbols, and if all the results are equal, $b_{B_i} + b_i = b'$, $\forall i$, the bit is accepted. If not, the symbols are discarded and the process is repeated for another vector. The new error probability is (see also [25,26])

$$\epsilon_{AB,N} = \frac{(\epsilon_{AB})^N}{(1 - \epsilon_{AB})^N + (\epsilon_{AB})^N} \leq \left(\frac{\epsilon_{AB}}{1 - \epsilon_{AB}} \right)^N, \quad (8)$$

which tends to an equality for $N \rightarrow \infty$.

What is the information that Eve can obtain? As usual, all the environment, all the degrees of freedom outside Alice and Bob's systems should be accessible to her. This means that the global state including Eve is pure, $|\Psi_{ABE}\rangle$, and such that $\text{tr}_E(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|) = \rho_{AB}$ [27]. Denote by $|e_{\pm\pm}\rangle$ Eve's states when Alice and Bob have projected onto $|\pm x_0\rangle$. For the case of individual attacks, it was shown in [25] that Eve's error in the estimation of the final bit b is bounded from below by a term proportional to $|\langle e_{++}|e_{--}\rangle|^N$. Therefore, Alice and Bob can establish a key (see [25] for more details) if

$$\frac{\epsilon_{AB}}{1 - \epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|. \quad (9)$$

More precisely, if this condition is fulfilled, there is always a finite N such that the new list of symbols can be distilled into a secret key using one-way protocols.

From Eq. (6), one can compute the global pure state including Eve. Note that taking the Gaussian purification does not imply any loss of generality on Eve's individual attack [27]. After projecting on $|\pm x_0\rangle$, Eve has a Gaussian state of two modes, with the CM and DV for the states $|e_{\pm\pm}\rangle$ given by

$$d_{++} = -\sqrt{\frac{\lambda^2 + \lambda(c_x - c_p) - c_x c_p - 1}{\lambda + c_x}}(0, 0, x_0, x_0),$$

$$\gamma_{++} = \begin{pmatrix} \gamma_x & 0 \\ 0 & \gamma_x^{-1} \end{pmatrix}, \quad \gamma_x = \begin{pmatrix} \lambda & c_x \\ c_x & \lambda \end{pmatrix}, \quad (10)$$

while $\gamma_{--} = \gamma_{++}$ and $d_{--} = -d_{++}$. Now, the overlap between these two states is given by

$$|\langle e_{++}|e_{--}\rangle|^2 = \exp\left(-\frac{4[\lambda^2 + \lambda(c_x - c_p) - c_x c_p - 1]x_0^2}{\lambda + c_x}\right). \quad (11)$$

Substituting Eqs. (8) and (11) in (9) one can check, after some algebra, that this condition is equivalent to the entanglement condition of (5). That is, all the distillable (NPPT) Gaussian states allow a secure key distribution under individual attacks using Gaussian operations. Moreover, the limits for NPPT entanglement and key distillation also coincide if Eve measures in a coherent way a finite number $N_E \ll N$ of states *before* the reconciliation process [28].

Although the presented protocol has zero efficiency, one can use continuity arguments and see that, for any NPPT state, there exist small but finite widths $dx_A = dx_B = dx$ for Alice and Bob's outcomes such that Eq. (9) still holds. Actually, this condition is independent of the Gaussian character of the state. This gives a secure protocol with finite rate. Note also that despite Eq. (9) depending on x_0 , the security of the protocol does not. When x_0 increases, Alice and Bob's error probability decreases, but also Eve's states become more distinguishable.

One may wonder what happens when Eve is no longer restricted to individual attacks. Indeed, a more powerful Eve could wait until the end of the advantage distillation protocol and measure in a coherent way all her N symbols [19]. One can see that the corresponding security condition is similar to Eq. (9), but replacing Eve's states overlap by its square. This new inequality is violated by some NPPT states (see Fig. 1). Note that this only implies that the analyzed protocol is not good for these states in this more general scenario.

Nevertheless, using the recent techniques of Ref. [20], we can find states for which the presented protocol allows one to extract common bits secure against any attack. After a successful X measurement on the state (4), Alice, Bob, and Eve share an effective state

$$|\Psi_{ABE}^{2 \times 2}\rangle = \sqrt{\frac{1 - \epsilon_{AB}}{2}}(|++\rangle|e_{++}\rangle + |--\rangle|e_{--}\rangle) + \sqrt{\frac{\epsilon_{AB}}{2}}(|+-\rangle|e_{+-}\rangle + |-+\rangle|e_{-+}\rangle). \quad (12)$$

Then, it has been shown in Ref. [20] that the amount of secret bits, R , Alice and Bob can extract from their known quantum state by means of protocols using one-way communication satisfies

$$R \geq I(x_A : x_B) - S(\rho_{AB}^{2 \times 2}), \quad (13)$$

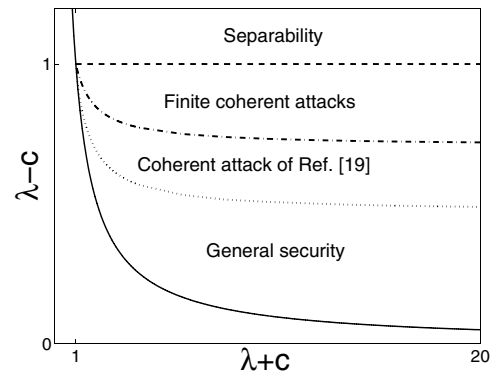


FIG. 1. Security analysis of symmetric 1×1 Gaussian states when $c_x = c_p = c$. All physical states are above the solid line. The dashed line defines the entanglement limit, which coincides with the security bound against incoherent attacks. States below the dotted line are secure against any attack.

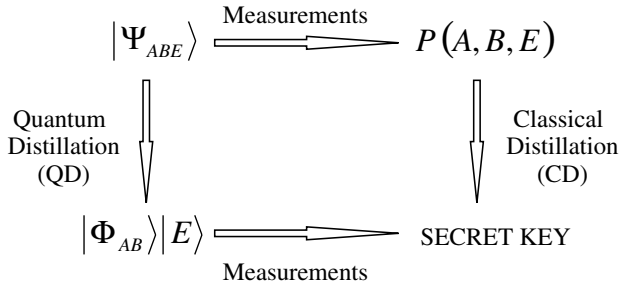


FIG. 2. Schematic representation of quantum and classical key distillation techniques from quantum states. In this work, Alice and Bob perform only Gaussian operations.

where I is the mutual information between their measurement outputs and $S(\rho_{AB}^{2 \times 2})$ the von Neumann entropy of their reduced state. Indeed, it was shown in [20] that the amount of information Eve has on Alice's symbols is bounded by the entropy of her local state, which is equal to the entropy of Alice and Bob's state. Note that this quantity also measures how strong Eve is correlated to the honest parties, since $S(\rho_{AB}^{2 \times 2})$ specifies the entanglement in the state $|\Psi_{ABE}^{2 \times 2}\rangle$ for the partition $AB - E$. In our case, this condition turns out to be dependent on x_0 . Thus, for any state, one has to look for a value of x_0 such that $R > 0$. Although we were not able to solve this problem analytically, it can be attacked using numerical methods. For example, the security curve for those states such that $c_x = c_p$ [see Eq. (3)] is shown in Fig. 1.

One can envisage different ways of improving the previous security analysis, e.g., finding better measurements for Alice and Bob or new ways of processing their measurement outcomes. A more interesting possibility consists of allowing the honest parties to manipulate in a coherent way several copies of their local states. Actually, in the study of GK_D with full generality, one should deal with joint (although local and Gaussian) operations by Alice and Bob. This defines a new type of *Gaussian quantum privacy amplification* protocols [5] different from entanglement distillability where Alice and Bob's goal is simply to factor Eve out [15,18]. A related open question that deserves further investigation is whether secret bits can be extracted from PPT Gaussian states, i.e., strict bound entangled states (cf. [8]).

Quantum and classical distillation (QD and CD) protocols are two techniques that allow one to extract secret bits from entangled states (see Fig. 2). In finite systems, there are examples of nondistillable quantum states for which the CD branch is possible [8]. Moving to continuous variables systems and the Gaussian scenario, QD techniques are useless for key agreement [15,16]. Our analysis proves that CD is still useful for (i) all NPPT states under finite coherent attacks and (ii) sufficiently entangled NPPT states under general attacks. Thus, our results close the gap between NPPT entanglement and security for the case of finite-size coherent attacks.

We acknowledge discussions with D. Bruß, M. Christandl, J. Eisert, F. Grosshans, and M. Plenio. This work has been supported by the Deutsche Forschungsgemeinschaft, the EU (projects RESQ and QUPRODIS), the Kompetenzzentrum "Quanteninformationsverarbeitung," the Spanish "Ramón y Cajal" (MCyT) and 2004FI-00068 grants, and the Generalitat de Catalunya.

- [1] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
- [2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE, Los Alamitos, CA, 1994), p. 124.
- [3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984).
- [4] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
- [5] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
- [6] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
- [8] K. Horodecki *et al.*, quant-ph/0309110.
- [9] *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht, 2003).
- [10] A. Furusawa *et al.*, Science **282**, 706 (1998).
- [11] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
- [12] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); Ch. Silberhorn *et al.*, Phys. Rev. Lett. **89**, 167901 (2002).
- [13] S. Iblisdir, G. Van Assche, and N. J. Cerf, quant-ph/0312018.
- [14] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
- [15] G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).
- [16] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002); J. Fiurasek, *ibid.* **89**, 137904 (2002).
- [17] G. Giedke *et al.*, Quantum Inf. Comput. **1**, 79 (2001).
- [18] A similar scenario has been considered by J. Eisert and M. Plenio (unpublished).
- [19] D. Kaszlikowski *et al.*, quant-ph/0312172.
- [20] M. Christandl, R. Renner, and A. Ekert, quant-ph/0402131.
- [21] L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, *ibid.* **84**, 2726 (2000).
- [22] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
- [23] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001); A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2003).
- [24] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
- [25] A. Acín, Ll. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
- [26] D. Bruß *et al.*, Phys. Rev. Lett. **91**, 097901 (2003).
- [27] The global state is specified by the local state ρ_{AB} , up to a unitary operation on Eve's system. Thus, from Eve's point of view, all the purifications are equivalent.
- [28] Similarly, as in Ref. [25], one can prove that Eq. (9) again defines the security condition for finite coherent attacks.