Gaussian operations and privacy

Miguel Navascués and Antonio Acín
ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, E-08034 Barcelona, Spain

(Received 21 March 2005; published 5 July 2005)

We consider the possibilities offered by Gaussian states and operations for two honest parties, Alice and Bob, to obtain privacy against a third eavesdropping party, Eve. We first extend the security analysis of the protocol proposed in [Navascués *et al.* Phys. Rev. Lett. **94**, 010502 (2005)]. Then, we prove that a generalized version of this protocol does not allow one to distill a secret key out of bound entangled Gaussian states.

DOI: 10.1103/PhysRevA.72.012303 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

The study of those tasks that can be achieved by processing information encoded on quantum states is the main scope of quantum information theory (QIT). The basic unit for quantum information is the so-called quantum bit, or *qubit*—namely, a two-dimensional quantum system. Moreover, quantum correlations, or entanglement, constitute a key resource in QIT, their unit being the entangled bit or *ebit*. In general, any (quantum) information task can be seen as an interconversion of resources. For instance, quantum teleportation [1] can be summarized as the process transforming 1 ebit+2 bits → 1 qubit, while dense coding [2] corresponds to the transformation 1 ebit+1 qubit → 2 bits. Moving to cryptography, secret bits are a fundamental resource. These are perfectly correlated and random bits shared by two honest parties, Alice and Bob, about which a third dishonest party, Eve, has no information. Any quantum key distribution protocol can be seen as the process of distributing secret bits through an insecure channel by means of quantum states. Therefore, relevant questions in this context are to identify those quantum states containing secret correlations and show how to distill these correlations into a perfect secret key. Indeed, it has recently been shown that a quantum state contains secret correlations if and only if it is entangled [3].

In these last years, quantum information theory for continuous variable systems has proved to be a very fruitful area, as it allows theory to connect easily with experiments (for a review, see [4]). In this case, the information encoding is done on continuous quantum variables, such as the quadratures of the electromagnetic field. Recent works have been developed in the aim of reproducing well-known quantum information protocols for finite-dimensional systems in this new setup. Examples of these are quantum cryptography [5] or quantum teleportation [6]. Interestingly, most of these protocols work using only Gaussian operations—i.e., operations that transform Gaussian states into Gaussian states. This is important because Gaussian operations are easy to implement experimentally with a high accuracy level. A beam splitter and a squeezer are examples of Gaussian operations, while photon counting constitutes a non-Gaussian operation. Up to now, non-Gaussian operations are challenging from an experimental point of view (see, however, [7]).

A significant effort has been devoted to study the possibilities and limitations Gaussian operations provide to quantum Information protocols. We know, for example, that entanglement distillation of Gaussian states with Gaussian operations is impossible [8–10]. More precisely: although there exist entangled Gaussian states that are distillable to singlets, the distillation process requires a non-Gaussian operation. Or, in other words, the process of converting Gaussian quantum states into perfect ebits by means of Gaussian local operations and classical communication (GLOCC) is impossible. However, ebits are not the only information resource two collaborating parties may want to establish through quantum states. Actually, distillation of perfect secret bits by GLOCC is known to be possible from some Gaussian states [5]. Thus, the set of Gaussian states and operations can sometimes be sufficient for cryptographic applications. At first sight, this result may seem surprising taking into account that Gaussian states have a positive Wigner function; i.e., there is a local variable model that reproduces the correlations given by Gaussian measurements.

In this article, we analyze the process of extracting secret bits from several copies of a given Gaussian state when the honest parties are allowed to perform local Gaussian operations and communicate classically. In the derivation of all the results, it is assumed that Alice and Bob share N independent copies of a known Gaussian state. That is, we do not consider the important problem of the distribution and estimation of these states. They simply constitute an initially given resource that the honest parties will to convert into secret bits. We start reviewing the results of [11], where it was shown that, provided Eve is restricted to individual attacks, a secret key can be extracted from any entanglement distillable state. We extend the security analysis of this protocol for the case of collective attacks, giving a necessary and sufficient condition for secret key distillation. We also show that there is no way in which the honest parties can attain privacy with our protocol if the initial state is bound entangled. This is true even if Eve is assumed to measure her state before any reconciliation process has taken place. This suggests that Gaussian operations may be useless to extract a secret key out of bound entangled Gaussian states, in opposition to the astounding results in [12] for finite-dimensional systems.

The article is organized as follows: Section II is a brief introduction to the Gaussian states and Gaussian operations formalism. The reader familiar with both topics can skip this part. In Sec. III, we analyze the limits of the protocol introduced in [11]. In particular, we show that it allows one to prove the security of sufficiently entangled states, while it fails for any bound entangled state. Section IV is devoted to our conclusions.

II. GAUSSIAN STATES AND OPERATIONS

In this article we consider quantum systems of n canonical degrees of freedom, called modes, belonging to $B(\mathcal{H}(\mathbb{R}^n))$. These are characterized by operators $(X_1,P_1,\ldots,X_n,P_n)=(R_1,\ldots,R_{2n})$ satisfying the commutation relations $[R_j,R_j]=i(\sigma_n)_{jk}$, where

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

is called the *symplectic matrix*. In this context, it can be proved that any operator A transforming n-mode states to n-mode states can be expressed as

$$A=(2\pi)^{-n}\int \chi_A(\xi)W_{-\xi}d^{2n}\xi, \tag{2}$$

where $\chi_A(\xi)$ is the so-called characteristic function and W_ξ are the Weyl operators, defined as

$$W_\xi=e^{i\xi^T\sigma R}, \tag{3}$$

and $R=(R_1,\ldots,R_{2n})$. Weyl operators satisfy the well-known *Weyl relations*

$$W_\xi W_\eta=e^{-i\xi^T\sigma\eta}W_{\xi+\eta}. \tag{4}$$

When A corresponds to the density operator associated with a certain state, $\chi_A(\xi)$ is called the *characteristic function of the state A*. One can also define the *Wigner function* $\mathcal{W}_A(\xi)$ of A as

$$\mathcal{W}_A(\xi)=(2\pi)^{-2n}\int e^{i\xi^T\sigma\eta}\chi_A(\eta)d^{2n}\eta. \tag{5}$$

The Wigner function behaves as a quasiprobability distribution in phase space. It is normalized, and integrating over X_i or P_i for each mode gives the corresponding probability distribution of the remaining canonical variables.

For every state ρ, one can define its *displacement vector d* as $d_k=tr\{\rho R_k\}$ and its *covariance matrix* γ as $\gamma_{kl}=tr\{\rho\{R_k-d_k,R_l-d_l\}_+\}$, where $\{\}_+$ denotes the anticommutator. Because of the Heisenberg uncertainty relations, any state has to satisfy

$$\gamma\geqslant i\sigma. \tag{6}$$

Gaussian states are those n-mode quantum states whose characteristic function is of the form

$$\chi(\xi)=e^{i\xi\sigma d-\xi\sigma^T\gamma\sigma\xi/4}. \tag{7}$$

Thus, any Gaussian state is completely described by its displacement vector d and covariance matrix γ.

Gaussian operations are completely positive maps transforming Gaussian states into Gaussian states. Gaussian operations were fully characterized in [8,10]. There, the authors show that a Gaussian state G with covariance matrix Γ and displacement Δ can be associated to each Gaussian operation $\mathcal{G}$. In particular, if Γ and Δ are given by

$$\Gamma=\begin{pmatrix}\Gamma_1 & \Gamma_{12}\\ \Gamma_{12}^T & \Gamma_2\end{pmatrix}\quad \Delta=\begin{pmatrix}\Delta_1\\ \Delta_2\end{pmatrix}, \tag{8}$$

then the application of $\mathcal{G}$ on a Gaussian state (γ,d) produces a Gaussian state (γ',d') such that

$$\gamma'=\tilde{\Gamma}_1-\tilde{\Gamma}_{12}\frac{1}{\tilde{\Gamma}_2+\gamma}\tilde{\Gamma}_{12}^T,$$

$$d'=\Delta_1+\tilde{\Gamma}_{12}\frac{1}{\tilde{\Gamma}_2+\gamma}(\Delta_2+d), \tag{9}$$

where $\tilde{\Gamma}=(\mathbb{1}\oplus\theta)\Gamma(\mathbb{1}\oplus\theta)$ and $\theta=D(1,-1,1,-1,\ldots)$ is the transformation that changes the sign of the momenta. Throughout this article, $D(a,b,\ldots)$ will denote a diagonal matrix with nonzero entries a,b and so on.

A fundamental Gaussian operation is homodyne detection—that is, the physical measurement of one of the canonical coordinates. Let γ define a Gaussian state with zero displacement vector. Suppose γ can be divided into modes as

$$\gamma=\begin{pmatrix}A & C\\ C^T & B\end{pmatrix}. \tag{10}$$

If we measure the X component of each of the modes corresponding to A, obtaining the result $(X_1,X_2,\ldots)$, system B will turn into a Gaussian state with covariance matrix (CM) [9]

$$B'=B-C^T(XAX)^{MP}C \tag{11}$$

and displacement vector

$$d_B=C^T(XAX)^{MP}d_A, \tag{12}$$

where $d_A=(X_1,0,X_2,0,\ldots)$, MP denotes the pseudoinverse (inverse on the range), and X is the projector $X=D(1,0,1,0,1,0,\ldots)$.

Another important subset of Gaussian operations is constituted by the so-called *symplectic transformations*. It can be proved that unitary Gaussian operations are the ones that transform the canonical coordinates in the following way:

$$R'=SR+T, \tag{13}$$

where T is a vector and S is a matrix belonging to the symplectic group $Sp(2n,\mathcal{R})$. The symplectic group is given by those matrices leaving invariant the symplectic matrix—i.e., satisfying $S\sigma S^T=\sigma$. When $T=0$, the transformation is called symplectic. Under symplectic transformations, the displacement vector and the covariance matrix change into $d'=Sd$ and $\gamma'=S\gamma S^T$. Symplectic transformations are very relevant because of the following.

Theorem (Williamson) [13]. For any real and positive definite $2n\times 2n$ matrix, C, one can find a symplectic matrix S such that

$$SCS^T=\oplus_{i=1}^{n}\lambda_i\mathbb{1}_2, \tag{14}$$

where $\lambda_i>0$ are called the *symplectic eigenvalues* of C.

Because of Eq. (6), if we apply this theorem to the covariance matrix of a certain state, we will get that all its symplectic eigenvalues λ_i have to be greater or equal than 1. Moreover, for a Gaussian state with covariance matrix γ, the identity $\mathrm{tr}(\rho^2)=\det(\gamma)^{-1/2}$ holds [recall that $\mathrm{tr}(\rho^2)$ gives a measure of the purity of ρ]. So a Gaussian state is pure if and only if all its symplectic eigenvalues are equal to one.

Finally, let us give some known results about entanglement and Gaussian states that will next be used. In this case, one considers Gaussian states in bipartite systems of $n+m$ modes, where Alice and Bob's systems are of n and m modes, respectively.

Theorem [14]. Let γ_{AB} be the covariance matrix of a Gaussian state in a bipartite system. This state is separable if and only if

$$\gamma_{AB} \geqslant \gamma_a \oplus \gamma_b \tag{15}$$

for certain *physical* covariance matrices γ_a and γ_b in systems A and B, respectively.

Partial transposition is a positive, but not completely positive, map that plays a key role in entanglement theory. In the case of continuous variable systems, after partial transposition on, say, system B, the sign of Bob's momenta is changed while the rest of canonical coordinates is kept unchanged. At the level of covariance matrices, this means that $\gamma_{AB} \rightarrow \gamma'_{AB} = \theta_B \gamma_{AB} \theta_B$. Therefore, a state ρ has nonpositive partial transposition (NPPT) when γ'_{AB} does not define a positive operator—that is,

$$\gamma_{AB} \ngeq i\tilde{\sigma}, \tag{16}$$

where $\tilde{\sigma}=(\mathbb{1}_A \oplus \theta_B)\sigma(\mathbb{1}_A \oplus \theta_B)$. It can be shown that this condition is equivalent to

$$\gamma_{AB} \ngeq \tilde{\sigma}\gamma_{AB}^{-1}\tilde{\sigma}^T. \tag{17}$$

The positivity of partial transposition, also known as the PPT criterion, represents a necessary and sufficient condition for separability for 1×1 [15] and $1\times N$ Gaussian states [14], while it is only a necessary condition for the rest of systems [14]. It also gives a necessary and sufficient condition for entanglement distillability: a Gaussian state is distillable if and only if it is NPPT [16].

III. SECRET BITS FROM GAUSSIAN STATES

In our quantum cryptographic scenario, there are two parties, Alice and Bob, who share several copies of a certain Gaussian state ρ_{AB}. As said, it is assumed that the honest parties know to have N independent copies of ρ_{AB}. There is also an eavesdropper, Eve, who keeps the purification of that state. In a prepare and measure scheme, the assumption in the state preparation means that Eve interacts identically, individually and in a Gaussian way, with the states sent to Bob by Alice. Alice and Bob perform some individual measurements over their copies and afterwards apply advantage distillation, error correction, and privacy amplification techniques to extract a perfect secret key. These three processes constitute the reconciliation part of the protocol. We consider two types of attacks: (i) *individual*, where Eve performs individual measurements, possibly non-Gaussian, over her set of states before Alice and Bob's public reconciliation, or (ii) *collective*, where Eve waits until the reconciliation is finished and then decides what (possibly collective) measurement gives her more information on the final key. Note that this second type of attacks is the most general under the mentioned assumption in the state preparation. On the other hand, to assume that Eve measures her state before the reconciliation process, as for individual attacks, appears quite reasonable from an experimental point of view.

In this section, we first review the protocol described in [11]. There, it was proved that (i) a secret key can be distilled from any NPPT Gaussian state, provided that Eve is restricted to individual attacks, (ii) there exist slightly entangled states that become insecure, with our protocol, when Eve's attack is collective and (iii) key distillation secure against collective attacks is still possible for sufficiently entangled states. Here, we will first improve the security analysis against collective attacks, giving a necessary and sufficient condition for secret key distillation from Gaussian states with our protocol. Later, we will show that our scheme does not allow to extract a secret key out of bound entangled Gaussian states.

A. Key distillation protocol

The key distillation protocol presented in [11] consists of the following steps

(i) Starting from ρ_{AB}, Alice and Bob apply the GLOCC protocol of [16] mapping any NPPT Gaussian state of $n+m$ modes into an NPPT 1×1 Gaussian and symmetric state, whose CM [see Eq. (10)] is

$$A = B = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad C = \begin{pmatrix} c_x & 0 \\ 0 & -c_p \end{pmatrix}, \tag{18}$$

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

$$\lambda^2 + c_x c_p - 1 < \lambda(c_x + c_p). \tag{19}$$

(ii) Each of them measure the X quadratures of their modes, X_A, X_B. As soon as all measurements are done, Alice randomly chooses a real number $X_0 > 0$ and sends it to Bob via a classical channel. If their measured quadratures satisfy $|X_A| = |X_B| = X_0$, they accept the results. Otherwise, they discard them. They then make binary these results according to the prescription $X_i = X_0 \rightarrow 0$, $X_i = -X_0 \rightarrow 1$, $i=A,B$, thus obtaining a list of correlated bits.

(iii) Alice and Bob apply classical advantage distillation [17] over their lists of symbols: they randomly choose a set of N indices and build binary N-vectors with the corresponding symbols appearing in their lists: $(A_1, A_2, \ldots, A_N)$ for Alice and $(B_1, \ldots, B_N)$ for Bob. Then, Alice generates a random bit, $c \in \{0,1\}$, and sends Bob a vector $(c_1, \ldots, c_N)$ such that $A_1 \oplus c_1 = A_2 \oplus c_2 = \cdots = A_N \oplus c_N = c$. Next, Bob computes the quantities $c'_i = B_i \oplus c_i$, $i=1,\ldots,N$. In case $c'_1 = c'_2 = \cdots = c'_N = c'$, Bob accepts the symbol c'. Otherwise, he discards it. Anyhow, after this step Alice and Bob will have to throw away all the symbols used and repeat the process with the remaining symbols. At the end, they will have a reduced list of more correlated symbols.

(iv) Alice and Bob apply error correction and privacy amplification protocols to the new list in order to obtain a secret key.

Let us denote by ω_{AB} Alice and Bob's 1×1 state after step (i) and by ϵ_B the probability that Alice and Bob obtain different results [namely, $(X_0,-X_0)$ or $(-X_0,X_0)$] after the homodyne measurements and post-selection. Let us also denote by $|e_{\pm\pm}\rangle$ Eve's resulting states when Alice and Bob measure $(\pm X_0,\pm X_0)$. If Eve is restricted to individual attacks—i.e., she measures before step (iii)—the honest parties can distill a key when [18]

$$\frac{\epsilon_B}{1-\epsilon_B} < |\langle e_{++}|e_{--}\rangle|. \tag{20}$$

Actually, this security condition also holds for the case in which Eve applies a measurement on a finite number of copies of her states before the reconciliation process has started. As shown in [11], Eq. (20) is equivalent to demand that the initial state ρ_{AB} was NPPT.

Now, one would naturally wonder how this security condition has to be modified when Eve is allowed to perform a collective attack; i.e., she can measure after the public reconciliation. In this case, Eve's information during the whole protocol is quantum. Note that, once the honest parties accept a symbol after advantage distillation, they can agree to both change its sign or not. This is so because the symplectic transformation $(X_A,P_A,X_B,P_B)\rightarrow(-X_A,-P_A,-X_B,-P_B)$ leaves the Gaussian state ω_{AB} invariant. Therefore, we can consider that Alice's N symbols employed in a successful performance of step (iii), are equal and so Bob's. That is, the global state resulting from step (iii) is (see also [19])

$$\rho_{ABE}=\frac{1-\epsilon_{BN}}{2}([00]\otimes[e_{++}]^{\otimes N}+[11]\otimes[e_{--}]^{\otimes N}) + \frac{\epsilon_{BN}}{2}([01]\otimes[e_{+-}]^{\otimes N}+[10]\otimes[e_{-+}]^{\otimes N}), \tag{21}$$

where $[\psi]$ denotes the projector onto $|\psi\rangle$ and ϵ_{BN} is Bob's error probability after advantage distillation. For large N, this error has the form [18]

$$\epsilon_{BN}\propto\left(\frac{\epsilon_B}{1-\epsilon_B}\right)^N. \tag{22}$$

In step (iv), Alice and Bob apply the one-way key distillation protocol given in [20]. This protocol deals with the case where Alice has a classical random variable A correlated to a quantum state on Bob and Eve's hands, $\rho_{B|A}$ and $\rho_{E|A}$. The achievable key rate satisfies [20]

$$K_{\rightarrow}\geqslant\chi(A{:}B)-\chi(A{:}E), \tag{23}$$

where $\chi(X{:}Y)$ denotes the Holevo bound [21]—i.e., $\chi(X{:}Y)=S(\rho_Y)-\Sigma_X p(X)S(\rho_{Y|X})$ and $\rho_Y=\Sigma_X p(X)\rho_{Y|X}$. In our case, Alice and Bob have classical variables, so $\chi(A{:}B)$ is actually equal to the mutual information $I(A{:}B)$, which is a function of ϵ_{BN}. Let us compute in what follows $\chi(A{:}E)$.

Notice that in the limit of large N, the error terms in Eq. (21) can be neglected, since $\epsilon_{BN}\rightarrow 0$. This means that the states $\rho_{E|A}$ are actually pure, so $\chi(A{:}E)\approx S(\rho_E)$ for large N. If the covariance matrix associated to the state ω_{AB} is given by

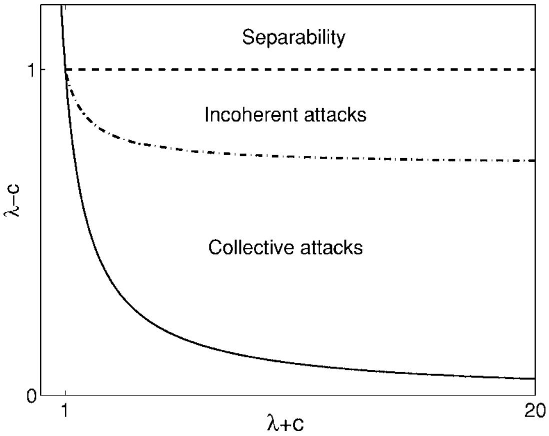

FIG. 1. Security analysis of isometric 1×1 Gaussian states, with covariance matrix satisfying [see Eq. (18)] $c_x=c_p=c$. All physical states are above the solid line. The dashed line defines the entanglement limit, which coincides with the security bound against incoherent attacks. States below the dash-dotted line are secure against any attack. It is implicitly assumed that Alice and Bob measure the X quadratures.

$$\gamma_{AB}=\begin{pmatrix}\gamma_x & R\\ R^T & S\end{pmatrix}, \tag{24}$$

where γ_x, R, T, and S are 2×2 matrices, one can see that for large N, $S(\rho_E)\propto k_E^N$, where

$$\log k_E=-(X_0,X_0)(S-R^T\gamma_x^{-1}R-\gamma_x^{-1})\begin{pmatrix}X_0\\ X_0\end{pmatrix}. \tag{25}$$

Actually, one has that $S-R^T\gamma_x^{-1}R-\gamma_x^{-1}=\{(\sigma\gamma_{AB}^{-1}\sigma^T)_x\}^{-1}-\gamma_x^{-1}$. Throughout this article, $(M)_x$ denotes the projection of a generic operator M onto the x space. It follows from this expression that $k_E=|\langle e_{++}|e_{--}\rangle|^2$. Comparing now the two quantities, it is clear that a positive key rate is possible when

$$\frac{\epsilon_B}{1-\epsilon_B} < |\langle e_{++}|e_{--}\rangle|^2. \tag{26}$$

This gives a sufficient condition for distilling a secret key. On the other hand, if Eve applies the particular attack proposed in [22], our protocol turns out to be insecure if Eq. (26) does not hold [11]. That is, Eq. (26) is indeed the necessary and sufficient condition for positive key extraction using our GLOCC protocol from Gaussian states. Therefore, this closes the security gap left open in the analysis of [11] (see also Fig. 1).

This result could somehow be expected: the application of the projectors $[\pm X_0]$ transforms the original Gaussian state into an effective two-qubit state that tends to a Bell diagonal state in the limit N going to infinite. The necessary and sufficient for positive key extraction from a two-qubit state has recently been derived in [19]. The bound given there looks identical to Eq. (26).

B. Bound entangled states

Our next result concerns the distillation of secret bits from PPT Gaussian states using the previous GLOCC protocol. Recall that in the Gaussian scenario, a state is entanglement distillable if and only if it is NPPT. This means that there do not exist NPPT bound entangled states. It is quite clear that the considered protocol, in the form previously presented, does not allow to extract a secret key from any PPT state. Indeed, in step (i) any PPT state is mapped into a 1×1 PPT state, which is separable [15], and no secret key can be extracted from separable states [23]. This is why we consider a generalized version of the protocol above, where step (i) is replaced by (i'). Alice and Bob perform any GLOCC pre processing, possibly non deterministic, over their states. Then, they measure the X quadrature of one of their modes as in step (ii) and the protocol proceeds as explained above. It is next shown that even in this more general scenario and restricting Eve to an individual attack, no secret key distillation is possible from PPT states.

As above, ϵ_B defines Bob's error probability after homodyne measurement and postselection. Let ρ_+ and ρ_- be Eve's resulting states when Alice and Bob measure (X_0,X_0) or $(-X_0,-X_0)$, respectively. Contrary to the previous situation, these states can now be mixed. Then, if Eve is restricted to individual attacks, a secret key can be distilled using our scheme if and only if

$$\frac{\epsilon_B}{1-\epsilon_B} < \mathrm{tr}(\sqrt{\sqrt{\rho_-}\rho_+\sqrt{\rho_-}}). \tag{27}$$

It is possible to derive this formula from [18]. There, it is shown that Eve's error probability behaves as $\epsilon_{EN} \propto [\Sigma_{i=1}^{M}\sqrt{\mathrm{tr}(\rho_+ M_i)\mathrm{tr}(\rho_- M_i)}]^N$, where M_i is the i_{th} operator corresponding to the i_{th} outcome of Eve's measurement, $\Sigma_i M_i = \mathbb{1}$. Now, one has to take into account that the minimum of $\Sigma_i\sqrt{\mathrm{tr}(\rho_+ M_i)\mathrm{tr}(\rho_- M_i)}$ over all possible measurements is equal to the Uhlmann's fidelity [24] of ρ_+ and ρ_-—namely, $\mathrm{tr}(\sqrt{\sqrt{\rho_-}\rho_+\sqrt{\rho_-}})$. A derivation of this result can be found in [25]. Recall that Bob's error probability after step (iii) goes as Eg. (22). Thus, for Alice and Bob to extract a secret key it is enough that ϵ_{BN} decreases exponentially faster than ϵ_{EN}. Then, condition (27) immediately applies.

Our goal is now to express (27) in terms of γ_{AB}. In fact, it will be seen that (27) is equivalent to the NPPT condition for Gaussian states.

As usual, it is supposed that Eve's state is entangled with Alice and Bob's one, so that the whole state is pure. Let us assume that Alice and Bob have just finished the GLOCC pre processing of step (i), and let us call $\gamma_{AB}^{(r)}$ the resulting reduced covariance matrix that contains only their first modes. We introduce the following notation:

$$\gamma_{ABE} = \begin{pmatrix} \gamma_{AB}^{(r)} & L & E \\ L^T & \gamma_{AB}^{(m)} & G \\ E^T & G^T & \gamma_E \end{pmatrix}, \quad F = \begin{pmatrix} E \\ G \end{pmatrix}$$

$$\gamma_{AB}^{(r)} = \begin{pmatrix} \gamma_x & R \\ R^T & S \end{pmatrix}, \quad (\gamma_{AB}^{(r)})^{-1} = \begin{pmatrix} X & Y \\ Y^T & Z \end{pmatrix}, \tag{28}$$

where γ_x and X correspond to the X_A, X_B space. The following formula will next be useful [26]:

$$\begin{pmatrix} A & C \\ C^T & B \end{pmatrix}^{-1} = \begin{pmatrix} \left(A - C\frac{1}{B}C^T\right)^{-1} & A^{-1}C\left(C^T\frac{1}{A}C - B\right)^{-1} \\ \left(C^T\frac{1}{A}C - B\right)^{-1}C^TA^{-1} & \left(B - C^T\frac{1}{A}C\right)^{-1} \end{pmatrix}. \tag{29}$$

Using Eqs. (11) and (12) it is straightforward to check that ρ_+ is described by

$$\gamma_E' = \gamma_E - E^T\beta E,$$

$$d_E' = E^T\beta\begin{pmatrix} X_0 \\ X_0 \\ 0 \\ 0 \end{pmatrix}, \tag{30}$$

where

$$\beta = \begin{pmatrix} \gamma_x^{-1} & 0 \\ 0 & 0 \end{pmatrix}. \tag{31}$$

Similarly, if Alice and Bob measure $-X_0$, Eve's corresponding state ρ_- will have the same covariance matrix and opposite displacement vector.

Let us first calculate the right-hand side of (27). It can be shown (see the Appendix) that

$$\mathrm{tr}(\sqrt{\sqrt{\rho_-}\rho_+\sqrt{\rho_-}}) = e^{-d_E'^T\gamma_E'^{-1}d_E'}. \tag{32}$$

Now we want to write this in terms of γ_{AB}. If we define

$$E=\begin{pmatrix} E_x \\ E_p \end{pmatrix}, \tag{33}$$

where E_x is the part of E corresponding to the X quadratures, we only have to substitute to get that $d_E'^T \gamma_E'^{-1} d_E'$ can be written as

$$\begin{pmatrix} X_0 & X_0 \end{pmatrix} \gamma_x^{-1} E_x (\gamma_E - E_x^T \gamma_x^{-1} E_x)^{-1} E_x^T \gamma_x^{-1} \begin{pmatrix} X_0 \\ X_0 \end{pmatrix}. \tag{34}$$

Using formula (29) applied to the matrix

$$K=\begin{pmatrix} \gamma_x & E_x \\ E_x^T & \gamma_E \end{pmatrix}^{-1} \tag{35}$$

(29) and the condition $KK^{-1}=\mathbb{1}$, we have that $E_x(\gamma_E - E_x\gamma_x^{-1}E_x)^{-1}E_x^T\gamma_x^{-1} = \gamma_x(\gamma_x - E_x\gamma_E^{-1}E_x^T)^{-1} - \mathbb{1}$. Substituting, we arrive at

$$d_E'^T \gamma_E'^{-1} d_E' = \begin{pmatrix} X_0 & X_0 \end{pmatrix} [(\gamma_x - E_x \gamma_E^{-1} E_x^T)^{-1} - \gamma_x^{-1}] \begin{pmatrix} X_0 \\ X_0 \end{pmatrix}. \tag{36}$$

Note that $(\gamma_x - E_x\gamma_E^{-1}E_x^T)$ is just the projection of $(\gamma_{AB} - F\gamma_E^{-1}F^T)$ onto the x space. Therefore, one can replace in the previous expression $(\gamma_x - E_x\gamma_E^{-1}E_x^T)$ and γ_x^{-1} by $(\gamma_{AB} - F\gamma_E^{-1}F^T)_x$ and $(\gamma_{AB}^{-1})_x$.

On the other hand, we have assumed that Eve purifies the state shared by Alice and Bob. Since all purifications are equivalent up to a unitary transformation on Eve's space, one can consider a particular purification without losing generality. One possible purification [see (28)] is given by [27]

$$F = \sigma_{AB}[-(\sigma_{AB}\gamma_{AB})^2 - \mathbb{1}]^{1/2}\theta \quad \gamma_E = \theta\gamma_{AB}\theta. \tag{37}$$

If S is the symplectic matrix such that $S^T\gamma_{AB}S$ is diagonal, one can verify that

$$\begin{aligned} F\gamma_E^{-1}F^T &= -\sigma_{AB}S(\oplus_k\sqrt{\lambda_k^2 - 1}\mathbb{1}_2)S^{-1}S\left(\oplus_k\frac{1}{\lambda_k}\mathbb{1}_2\right) \\ &\quad \times S^T(S^{-1})^T(\oplus_k\sqrt{\lambda_k^2 - 1}\mathbb{1}_2)S^T\sigma_{AB} \\ &= -\sigma_{AB}S\left(\oplus_k\frac{\lambda_k^2 - 1}{\lambda_k}\mathbb{1}_2\right)S^T\sigma_{AB} \\ &= \gamma_{AB} - \sigma_{AB}\gamma_{AB}^{-1}\sigma_{AB}^T. \end{aligned} \tag{38}$$

So $\gamma_{AB} - F\gamma_E F^T = \sigma\gamma_{AB}^{-1}\sigma^T$ and $\mathrm{tr}(\sqrt{\sqrt{\rho_-}\rho_+\sqrt{\rho_-}})$ is equal to

$$\exp\left[-X_0^2\begin{pmatrix} 1 & 1 \end{pmatrix}[(\sigma_{AB}\gamma_{AB}^{-1}\sigma_{AB}^T)_x^{-1} - (\gamma_{AB})_x^{-1}]\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right]. \tag{39}$$

The next step is to calculate the left-hand side of (27).

Let $\rho(X_A, X_B)$ be the probability density of (X_A, X_B), the X quadratures of the reduced state $\gamma^{(r)}$. The corresponding Wigner function satisfies

$$w(\xi) \propto e^{-\xi^T(\gamma_{AB}^{(r)})^{-1}\xi}. \tag{40}$$

If $\xi = (x_1^A, x_1^B, \vec{p})$, then, according to Eqs. (28),

$$\rho(x_1^A, x_1^B) \propto \int e^{-(\xi^T(\gamma_{AB}^{(r)})^{-1}\xi)} d\vec{p} = \int e^{-(\vec{x}^T X\vec{x} + 2\vec{x}^T Y\vec{p} + \vec{p}^T Z\vec{p})} d\vec{p}. \tag{41}$$

Finally, we get

$$\rho(x_1^A, x_1^B) \propto e^{-\vec{x}^T(X - YZ^{-1}Y^T)\vec{x}}. \tag{42}$$

But, looking at Eq. (29), we see that this is just $\exp(-\vec{x}^T\gamma_x^{-1}\vec{x})$. Writing

$$\gamma_x = \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \tag{43}$$

it is easy to see that, in our protocol,

$$\frac{\epsilon_B}{1 - \epsilon_B} = \exp\left(-\frac{4bX_0^2}{ac - b^2}\right). \tag{44}$$

In a similar way, one can define

$$(\sigma\gamma_{AB}^{-1}\sigma^T)_x = \begin{pmatrix} d & e \\ e & f \end{pmatrix}, \tag{45}$$

and then, the term in the exponent of Eq. (39) can be expressed as

$$-X_0^2\left(\frac{d - 2e + f}{de - f^2} - \frac{a - 2b + c}{ac - b^2}\right). \tag{46}$$

Collecting all these results, the condition (27) for distilling a key with this protocol is equivalent to

$$\frac{d + f - 2e}{df - e^2} - \frac{a + c + 2b}{ac - b^2} < 0. \tag{47}$$

We are now in a position to prove the next

Theorem. A secret key secure against individual attacks can be distilled with our GLOCC protocol from a Gaussian state if and only if the state is NPPT.

Proof. The idea of the proof is to show that condition (27) is equivalent to the PPT criterion. First, note that Eq. (47) can be rewritten as

$$\begin{pmatrix} 1 & -1 \end{pmatrix}[(\tilde{\sigma}\gamma_{AB}^{-1}\tilde{\sigma}^T)_x^{-1} - \gamma_x^{-1}]\begin{pmatrix} 1 \\ -1 \end{pmatrix} < 0. \tag{48}$$

Since $(\tilde{\sigma}\gamma_{AB}^{-1}\tilde{\sigma}^T)_x$ and γ_x are positive operators, the previous equation implies that $\gamma_{AB} - \tilde{\sigma}\gamma_{AB}^{-1}\tilde{\sigma}^T \ngeq 0$. But this is the condition for a Gaussian state to be NPPT, as stated in (17). Therefore, if a key can be distilled out of a Gaussian state with the previous protocol, this state has to be NPPT. For the opposite implication one simply has to apply the protocol of [11], which has previously been described.

IV. CONCLUSIONS

In this article, we have analyzed the extraction of secret bits from quantum states in the every-day-growing field of quantum information theory with continuous variables. We have first reviewed the protocol and results of [11]: a secret key can be distilled from any NPPT state when Eve is restricted to individual attacks. In the more general scenario of collective attacks, we extend the analysis of [11], providing a necessary and sufficient condition for key distillability, with the considered protocol. This protocol turns out to be completely useless for bound entangled states, even in the case of individual attacks. Before concluding, we would like to discuss several open questions and implications that follow from our results.

First, note that all the presented results aim at answering whether secret bits can be extracted from Gaussian states by GLOCC. In terms of resources, we study the conversion of Gaussian states into secret bits. However, very little is said about the rate governing this conversion. This problem appears as a natural follow-up of the present work. Notice that, strictly speaking, the considered key-distillation protocol has zero rate. Indeed, the probability that Alice and Bob obtain the outcomes $\pm X_0$ is zero. Of course, the analysis can easily be adapted to a protocol with finite rate: Alice and Bob only have to accept outcomes in the range $|X_0 \pm \delta|$, where $\delta > 0$. By choosing a properly small δ, the security conditions still hold because of continuity, while the protocol automatically acquires a finite rate. It is intriguing the fact that both security conditions, Eqs. (20) and (26), are independent of X_0. This suggests that key distillation should still be possible when Alice and Bob directly assign a bit to the sign of their measurements, without discarding any value. This would represent a significant improvement of the final key rate. Unfortunately, this result remains unproven. It would also be desirable to adapt the reconciliation process to the continuous character of the measured quantity, in a similar way as the sliced-reconciliation protocols for error correction introduced in [28].

Another related question is the distribution of quantum states. All our results were based on the hypothesis that Alice and Bob share N independent realization of the same known Gaussian state. However, in any practical cryptographic protocol, Alice and Bob will send and measure quantum states through an insecure channel. From the observed probabilities, they have to infer what their correlations with the environment are. This is indeed a very delicate process that has not been considered here. For instance, the honest parties cannot in principle exclude the existence of correlations between the different quantum systems they measure. While in our case, we simply assume that N copies of the same Gaussian state were given as an initial resource.

At a more fundamental level, our analysis represents one of the first steps in the identification of the set of Gaussian states that can be converted into secret bits by GLOCC. As discussed in [11], for any Gaussian state one can define GK_D and GE_D, quantities that specify the amount of secret and entangled bits extractable from it by GLOCC protocols. The results of Refs. [8–10] imply that $GE_D=0$. On the other hand, it follows from [11] and this work that GK_D is non zero for sufficiently entangled NPPT states. It would be relevant to extend the present results, proving that $GK_D > 0$ for some states violating our security conditions. An almost unexplored possibility in this direction is the use of global, but still Gaussian, operations by Alice and Bob. In particular, note that in the analyzed protocol, all the quantum operations were at the single-copy level. Therefore, it is unknown whether the use of coherent quantum operations gives any improvement for key extraction. A related open question is the existence of the so-called "entanglement purification" protocols [8], where Alice and Bob map many copies of a noisy entangled state into a pure entangled state (not necessarily maximally entangled). The goal would then be to decouple the honest parties' correlation from the eavesdropper, something that it is sufficient in a cryptographic scenario.

The case of bound entangled states is also of particular interest. Indeed, our result suggest that $GK_D=0$ for all these states (cf. [12]). In the same spirit as in Ref. [12], one could look for *Gaussian secret states*. These would be states for which there exist Gaussian measurements by Alice and Bob almost perfectly correlated about which Eve has an arbitrarily small amount of information. The results of Sec. III B rule out this possibility for PPT states. Indeed, if this were the case, there would be PPT secret states. This would imply that our protocol would work for a PPT state, which has been shown here to be impossible. Unfortunately, this does not allow to conclude that $GK_D=0$ for PPT states. More in general, it would also be interesting to prove that $K_D > 0$ for a Gaussian PPT state—i.e., that key extraction is possible—even if the distillation protocol employs a non-Gaussian operation.

ACKNOWLEDGMENTS

We acknowledge discussion with Ignacio Cirac, Jens Eisert, and Géza Giedke. This work has been supported by the Ministerio de Ciencia y Tecnología, under a "Ramón y Cajal" grant, and the Generalitat de Catalunya.

APPENDIX: PROOF OF RELATION (32)

From the definition of the characteristic function and relation (3) it can be derived that

$$\rho_1^2 \rightarrow \chi_1^{(2)}(\xi) = e^{-i\xi^T \sigma d_E' - \xi^T \sigma D(\gamma_E')\sigma^T \xi/4} S(\gamma_E'). \tag{A1}$$

Therefore,

$$\sqrt{\rho_1} \rightarrow \chi_1^{(1/2)}(\xi) = e^{-i\xi^T \sigma d_E' - \xi^T \sigma V(\gamma_E')\sigma^T \xi/4} H(\gamma_E'), \tag{A2}$$

and then

$$\sqrt{\rho_1}\rho_0\sqrt{\rho_1} \rightarrow A(\gamma_E', d_E') e^{-\xi^T B(\gamma_E')\xi + i\xi^T \sigma r(\gamma_E', d)}. \tag{A3}$$

Using the cyclic property of the trace, we get $\mathrm{tr}(\sqrt{\rho_1}\rho_0\sqrt{\rho_1}) = \mathrm{tr}(\rho_1\rho_0) = e^{-2d_E'^T \gamma_E'^{-1} d_E'} |\gamma_E'|^{-1/2} = A(\gamma_E', d_E')$. One then has

$$\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}} \rightarrow C(\gamma_E')\sqrt{A(\gamma_E', d_E')} e^{-\xi^T U(\gamma_E')\xi + i\xi^T \sigma s(\gamma_E', d_E')}, \tag{A4}$$

which, after substitution, gives

$$\mathrm{tr}(\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}) = e^{-d_E'{}'^T \gamma_E'^{-1} d_E'} M(\gamma_E'). \tag{A5}$$

However, note that if $d_E'=0$, $\rho_0=\rho_1$, and $\mathrm{tr}(\sqrt{\sqrt{\rho_0}\rho_0\sqrt{\rho_0}})=1$. This implies that $M(\gamma_E')=1$, and so

$$\mathrm{tr}(\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}) = e^{-d_E'^T \gamma_E'^{-1} d_E'}. \tag{A6}$$

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[3] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).

[4] S. L. Braunstein and P. van Loock, e-print quant-ph/0410100.

[5] M. Hillery, Phys. Rev. A **61**, 022309 (2000);N. J. Cerf, M. Lévy, and G. Van Assche, *ibid.* **63**, 052311 (2001); D. Gottesman and J. Preskill, *ibid.* **63**, 022309 (2001); F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *ibid.* **89**, 167901 (2002).

[6] S. L. Braunstein and H. J. Kimble Phys. Rev. Lett. **80**, 869 (1998); A. Furusawa, J. L. Sørensen, S. L. Braustein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik , Science **282**, 706 (1998).

[7] J. Wenger, R. Tualle-Brouri, and P. Grangier Phys. Rev. Lett. **92**, 153601 (2004).

[8] G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).

[9] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).

[10] J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).

[11] M. Navascués, J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acín, Phys. Rev. Lett. **94**, 010502 (2005).

[12] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, e-print quant-ph/0309110.

[13] J. Williamson, Am. J. Math. **58**, 141 (1936).

[14] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).

[15] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, *ibid.* **84**, 2726 (2000).

[16] G. Giedke L.-M. Duan, J. I. Cirac, and P. Zoller, Quantum Inf. Comput. **1**, 79 (2001).

[17] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[18] A. Acín, Ll. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).

[19] A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, e-print quant-ph/0411092.

[20] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).

[21] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

[22] D. Kaszlikowski, J. Y. Lim, D. K. L. Oi, F. H. Willeboordse, A. Gopinathan, and L. C. Kwek, e-print quant-ph/0408088.

[23] N. Gisin and S. Wolf, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Berlin, 2000), p. 482; M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[24] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[25] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[26] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, England, 1987).

[27] G. Giedke, J. Eisert, J. I. Cirac, and M. B. Plenio, Quantum Inf. Comput. **3**, 211 (2003).

[28] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).