Fundamental limitations to key distillation from Gaussian states with Gaussian operations

Lami, L.; Mišta, L.; Adesso, G.

DOI
10.1103/PhysRevResearch.5.033153

Publication date
2023

Document Version
Final published version

Published in
Physical Review Research

Fundamental limitations to key distillation from Gaussian states with Gaussian operations

Ludovico Lami [1,2,3,*] Ladislav Mišta, Jr. [4,†] and Gerardo Adesso [1,‡]

[1] *School of Mathematical Sciences and Centre for the Mathematics and Theoretical Physics of Quantum Non-Equilibrium Systems (CQNE), University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*

[2] *Institut für Theoretische Physik und IQST, Universität Ulm, Albert-Einstein-Allee 11, D-89069 Ulm, Germany*

[3] *QuSoft, Korteweg-de Vries Institute for Mathematics, and Institute for Theoretical Physics, University of Amsterdam, Science Park, 1098 XG Amsterdam, Netherlands*

[4] *Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*

(Received 3 November 2020; revised 23 June 2023; accepted 1 July 2023; published 5 September 2023)

We establish fundamental upper bounds on the amount of secret key that can be extracted from quantum Gaussian states by using local Gaussian operations, local classical processing, and public communication. For one-way public communication or when two-way public communication is allowed but Alice and Bob first perform destructive local Gaussian measurements, we prove that the key is bounded by the Rényi-2 Gaussian entanglement of formation $E_{F,2}^{G}$. The saturation of this inequality for pure Gaussian states provides an operational interpretation of the Rényi-2 entropy of entanglement as the secret key rate of pure Gaussian states accessible with Gaussian operations and one-way communication. In the general setting of two-way communication and arbitrary interactive protocols, we argue that $2E_{F,2}^{G}$ still serves as an upper bound on the extractable key. We conjecture that the factor of 2 is spurious, suggesting that $E_{F,2}^{G}$ coincides with the secret key rate of Gaussian states under Gaussian measurements and two-way public communication. We use these results to prove a gap between the secret key rates obtainable with arbitrary versus Gaussian operations. This gap is observed for states produced by sending one half of a two-mode squeezed vacuum through a pure loss channel, in the regime of sufficiently low squeezing or sufficiently high transmissivity. Finally, for a wide class of Gaussian states, including all two-mode states, we prove a recently proposed conjecture on the equality between $E_{F,2}^{G}$ and the Gaussian intrinsic entanglement. The unified entanglement quantifier emerging from such an equality is then endowed with a direct operational interpretation as the value of a quantum teleportation game.

DOI: 10.1103/PhysRevResearch.5.033153

I. INTRODUCTION

Quantum entanglement enables distant parties to generate a shared secret key by employing public discussion only [1–3], a feat impossible in the classical setting [4,5] without additional assumptions on the information available to the eavesdropper [5–9]. In the last decades, quantum key distribution (QKD) has established itself as a fundamental primitive in quantum cryptography, thus gaining a central role in the flourishing quantum information science and technology [10]. Accordingly, the amount of secret key that can be extracted from a state is regarded as an entanglement measure of fundamental operational importance [11–14].

Continuous variable (CV) platforms, based on communication over quantum optical modes [15,16], transmitted either via optical fibres or across free space [17,18], have been of paramount importance in the demonstration of QKD. Recently, they witnessed impressive experimental progress [19–22] and will likely play a major role in any future large-scale technological implementation of QKD [23–25].

Paradigmatic examples of CV QKD protocols are those based on Gaussian states and Gaussian measurements [26–37]. The main advantage of this all-Gaussian paradigm [23,38,39] is that it is relatively experimentally friendly: coherent states [40–43], squeezed states [44–49], homodyne and heterodyne detection [15,39] are nowadays relatively inexpensive ingredients, especially compared to general quantum states and operations. At the same time, it is still quite powerful in the context of QKD; in fact, it has been shown that any sufficiently entangled Gaussian state can be used, in combination with local Gaussian operations and public communication, to distil a secret key [50–52]. The effectiveness of the all-Gaussian paradigm in QKD is in stark contrast with its fundamentally limited performances at many other important tasks, such as universal quantum computation [53–56], entanglement distillation [57–59], error correction [60], and state transformations in general resource theories [61,62].

In this paper, we investigate the operational effectiveness of the all-Gaussian framework in the context of QKD, establishing ultimate limitations on the amount of secret key that can be extracted from arbitrary multimode Gaussian states by means of local Gaussian operations, local classical processing, and public communication—a quantity that we call *Gaussian secret key*. The fact that the initial state is Gaussian and that the available *quantum* operations are Gaussian does not mean

*ludovico.lami@gmail.com
†mista@optics.upol.cz
‡gerardo.adesso@nottingham.ac.uk

that the state will be Gaussian at all stages of the protocol, essentially because local classical operations are entirely unrestricted. For example, Alice could decide to apply a random displacement to her system (say, either $+s$ or $-s$, with equal probabilities), making the resulting state non-Gaussian.

In a nutshell we prove that, while key distillation is indeed possible in the Gaussian setting, it is not as efficient as it could be if also non-Gaussian measurements were allowed. Our bounds are given in terms of a Gaussian entanglement measure known as the *Rényi-2 Gaussian entanglement of formation* (denoted $E^{\mathrm{G}}_{F,2}$) [63–68], and thus endow this quantity with a sound operational meaning. In this context, after formalizing basic definitions on CV systems (Sec. II) and Gaussian key distillation protocols (Sec. III), we establish three main results in Sec. IV.

First, if only one-way public communication is allowed then the Gaussian secret key is at most $E^{\mathrm{G}}_{F,2}$, with the inequality saturated for pure Gaussian states (Theorem 4). Secondly, we argue that the Gaussian secret key is anyway limited by $2E^{\mathrm{G}}_{F,2}$ even in the most general setting where we allow two-way public communication (Theorem 5). Lastly, we show that the upper bound $E^{\mathrm{G}}_{F,2}$—without the factor 2—still holds even for two-way public communication, provided that Alice and Bob start the protocol with destructive Gaussian measurements (Theorem 6).

The Rényi-2 Gaussian entanglement of formation $E^{\mathrm{G}}_{F,2}$ is a monogamous and additive Gaussian entanglement monotone enjoying a wealth of properties [65–68]. Moreover, its computation amounts to a simple single-letter optimization problem that is analytically solvable for all two-mode mixed states [63,64]. Instrumental to our approach is the study of the connection between $E^{\mathrm{G}}_{F,2}$ and another Gaussian entanglement measure known as the *Gaussian intrinsic entanglement* (denoted $E^{\mathrm{G}}_{\downarrow}$) [69–71]. In Sec. V we prove that $E^{\mathrm{G}}_{\downarrow} \leqslant E^{\mathrm{G}}_{F,2}$ holds for all multimode Gaussian states and, more remarkably, we establish the recently conjectured [69] equality $E^{\mathrm{G}}_{\downarrow} = E^{\mathrm{G}}_{F,2}$ for the vast class of "normal" Gaussian states, which include in particular all two-mode Gaussian states (Theorem 7).

In Sec. VI we explore further applications and interpretations of our results. In particular, in the one-way communication scenario we show that $E^{\mathrm{G}}_{F,2}$ is often smaller than the one-way distillable entanglement on the physically relevant class of states obtained by sending one half of a two-mode squeezed vacuum across a pure loss channel, entailing that restricting to Gaussian operations leads to a decrease of distillable key. We also provide a general operational interpretation for $E^{\mathrm{G}}_{F,2}$ in a game-theoretical context based on quantum teleportation in the presence of a malicious jammer. We present our concluding remarks in Sec. VII.

II. CONTINUOUS VARIABLE BASICS

We start by recalling the formalism of CV Gaussian states and measurements [23,38,39,72]; see Appendix A for further details.

A. Phase space representations

For a CV system made of m harmonic oscillators (modes), the displacement operator associated with a vector $\xi \in \mathbb{R}^{2m}$ is defined by [[39], Sec. 3.1]

$$D(\xi) := e^{i\xi^{\intercal}\Omega r}. \tag{1}$$

Note that $D(\xi)$ is a unitary operator. Furthermore, for all ξ it holds that $D(\xi)^{\dagger} = D(-\xi)$. The canonical commutation relations can be rewritten in the so-called Weyl form in terms of the displacement operators. They read [[39], Eq. (3.11)]

$$D(\xi_1)D(\xi_2) = e^{-\frac{i}{2}\xi_1^{\intercal}\Omega\xi_2} D(\xi_1+\xi_2). \tag{2}$$

The characteristic function of an m-mode quantum state ρ is the function $\chi_\rho : \mathbb{R}^{2m} \to \mathbb{C}$ defined by [[39], Sec. 4.3]

$$\chi_\rho(\xi) := \mathrm{Tr}[\rho D(-\xi)]. \tag{3}$$

Its Fourier transform is the Wigner function, in formula

$$W_\rho(u) := \frac{1}{2^m\pi^{2m}} \int d^{2m}\xi\ \chi_\rho(\xi)\, e^{-i\xi^{\intercal}\Omega u}. \tag{4}$$

B. Gaussian states

Let x_j and p_j $(1 \leqslant j \leqslant m)$ be the canonical operators of an m-mode CV system, whose vacuum state we denote with $|0\rangle$. Defining the vector $r := (x_1, \ldots, x_m, p_1, \ldots, p_m)^{\intercal}$, the canonical commutation relations can be written in matrix notation as $[r, r^{\intercal}] = i\Omega$, where

$$\Omega := \begin{pmatrix} 0_m & \mathbb{1}_m \\ -\mathbb{1}_m & 0_m \end{pmatrix}. \tag{5}$$

A quadratic Hamiltonian is a self-adjoint operator of the form $H_q = \frac{1}{2} r^{\intercal} K r + t^{\intercal} r$, where $K > 0$ is a $2m \times 2m$ real matrix, and $t \in \mathbb{R}^{2m}$. *Gaussian states* are by definition thermal states of quadratic Hamiltonians (and limits thereof). They are uniquely defined by their mean or displacement vector, expressed as $s := \mathrm{Tr}[\rho\, r] \in \mathbb{R}^{2m}$ [73], and by their quantum covariance matrix (QCM), a $2m \times 2m$ real symmetric matrix given by $V := \mathrm{Tr}[\rho\{r-s, (r-s)^{\intercal}\}]$. Physical QCMs V satisfy the Robertson–Schrödinger uncertainty principle

$$V \geqslant i\Omega, \tag{6}$$

hereafter referred to as *bona fide* condition [74], which implies $V > 0$ and $\det V \geqslant 1$. Any real matrix V that obeys the bona fide condition is the QCM of some Gaussian state, which is pure iff $\det V = 1$. The Gaussian state with mean s and QCM V will be denoted by $\rho_{\mathrm{G}}[V, s]$. Note that mean vectors and QCMs compose with direct sum under tensor products, $\rho_{\mathrm{G}}[V, s] \otimes \rho_{\mathrm{G}}[W, t] = \rho_{\mathrm{G}}[V \oplus W,\ s \oplus t]$ [75].

The characteristic function as well as the Wigner function of Gaussian states are in fact Gaussian. More precisely,

$$\chi_{\rho_{\mathrm{G}}[V,s]}(\xi) = \exp\left[-\frac{1}{4}\xi^{\intercal}\Omega^{\intercal}V\Omega\xi + is^{\intercal}\Omega\xi\right], \tag{7}$$

$$W_{\rho_{\mathrm{G}}[V,s]}(u) = \frac{2^m}{\pi^m\sqrt{\det V}} \exp[-(u-s)^{\intercal}V^{-1}(u-s)]. \tag{8}$$

Note that $W_{\rho_{\mathrm{G}}[V,s]}$ is a Gaussian with mean s and covariance matrix $V/2$. In particular, the differential entropy $H(W_{\rho_{\mathrm{G}}[V,s]}) := -\int d^{2m}u\, W_{\rho_{\mathrm{G}}[V,s]}(u) \log_2 W_{\rho_{\mathrm{G}}[V,s]}(u)$ of the Wigner function associated with a Gaussian state $\rho_{\mathrm{G}}[V, s]$ evaluates to

$$\begin{aligned} H(W_{\rho_{\mathrm{G}}[V,s]}) &= \tfrac{1}{2}\log_2 \det V + m\log_2(\pi e) \\ &= M(V) + m\log_2(\pi e), \end{aligned} \tag{9}$$

where we used the notation

$$M(V) \coloneqq \tfrac{1}{2}\log_2 \det V. \tag{10}$$

If V is a QCM, then $\det V = \prod_{j=1}^{m} \nu_j^2(V)$ is the squared product of the symplectic eigenvalues. Since these are no smaller than 1, we conclude that $\det V \geqslant 1$ and hence $M(V) \geqslant 0$. Therefore, for all Gaussian states it holds that

$$H(W_{\rho_G[V,s]}) \geqslant m \log_2(\pi e). \tag{11}$$

C. Gaussian measurements

Quantum measurements are modelled by positive operator-valued measures (POVM) $E(dx)$ over a measure space $\mathcal{X}$, with outcome probability distribution being $p(dx) = \mathrm{Tr}[\rho\, E(dx)]$.

Gaussian measurements over an m-mode system are defined by the POVM

$$E(d^{2m}x) = \rho_G[\Gamma, x]\, \frac{d^{2m}x}{(2\pi)^m} \tag{12}$$

on the measure space $\mathcal{X} = \mathbb{R}^{2m}$, with the QCM Γ denoting the *seed* of the measurement. We will sometimes represent this as the quantum-classical channel

$$\mathcal{M}^{\mathrm{G}}_{\Gamma}(\cdot) \coloneqq \int \frac{d^{2m}x}{(2\pi)^m}\, \mathrm{Tr}[\rho_G[\Gamma, x](\cdot)]|x\rangle\langle x|, \tag{13}$$

where the vectors $|x\rangle$ are formally orthonormal [76].

On a Gaussian state $\rho_{\mathrm{G}}[V, s]$, the Gaussian measurement in (12) yields as outcome a random variable $X \in \mathbb{R}^{2m}$ whose probability density function reads [[39], Sec. 5.4.4]

$$p(x) = \frac{e^{-(x-s)^{\intercal}(V+\Gamma)^{-1}(x-s)}}{\pi^m \sqrt{\det(V+\Gamma)}}. \tag{14}$$

In other words, X is normally distributed with mean s and covariance matrix $(V+\Gamma)/2$ [77].

If the measured system A is part of a bipartite system AB initially in a Gaussian state $\rho_{\mathrm{G}}[V_{AB}, s_{AB}]$, the postmeasurement state on B conditioned on obtaining the outcome x is again Gaussian, has QCM given by the *Schur complement*

$$V'_B = (V_{AB} + \Gamma_A)/(V_A + \Gamma_A), \tag{15}$$

and displacement vector that depends on V_{AB}, s_{AB}, and x as reported in Ref. [[39], Sec. 5.4.5]. Importantly, note that the postmeasurement state of Gaussian measurements depends on the measurement outcome only through its mean vector and not through its QCM; indeed, the expression (15) is independent of x.

From the above interpretation of the expression (15) as the QCM of the reduced postmeasurement state it immediately follows that V'_B is also a QCM, i.e., it satisfies

$$V'_B \geqslant i\Omega_B. \tag{16}$$

Moreover, one can also conclude that V'_B must be pure if such are both V_{AB} and Γ_A. These important facts can also be established directly by exploiting the properties of Schur complements reviewed in Appendix A 3 [80].

The simplest unitary operations one can account for in the Gaussian formalism are so-called *Gaussian unitaries*, constructed as products of factors of the form $e^{-iH_q\tau}$, with H_q a quadratic Hamiltonian. For a Gaussian unitary $\mathcal{U}$, the induced state transformation $\rho \mapsto \mathcal{U}\rho\mathcal{U}^{\dagger}$ becomes $V \mapsto SVS^{\intercal}$ at the level of QCMs. Here S is a $2m \times 2m$ symplectic matrix, satisfying $S\Omega S^{\intercal} = \Omega$.

A *Gaussian measurement protocol* on a CV system A conditioned on a random variable U is a procedure of the following form: (i) We append to A a single-mode ancilla R_1 in the vacuum state; conditioned on U, we apply a Gaussian unitary to AR_1 and perform a Gaussian measurement with seed Γ_1^U on the last m_1 modes of the resulting state (possibly, $m_1 = 0$), obtaining a random variable $X_1 \in \mathbb{R}^{2m_1}$. Note that both the Gaussian unitary and Γ_1^U may depend on U. The modes remaining after the measurement form a system that we denote with A_1. (ii) We append to A_1 a single-mode ancilla R_2 in the vacuum state, and use X_1 together with U to decide on a Gaussian unitary to apply to A_1R_2 and on a Gaussian measurement with seed $\Gamma_2^{X_1U}$ to carry out on the last m_2 modes of the resulting state (possibly, $m_2 = 0$). (iii) We continue in this way, until after r rounds the protocol terminates. The output products are a random variable $X = (X_1, \ldots, X_r) \in \mathbb{R}^{2\sum_{i=1}^{r} m_i}$ (the *measurement outcome*) and a quantum system A_r [81].

D. Gaussian entanglement measures

In this paper we will relate the *secret key* that can be distilled by means of Gaussian protocols to the *quantum correlations* contained in Gaussian states. In general, operationally motivated correlation quantifiers for quantum states are usually based on the von Neumann entropy

$$S_1(\rho) \coloneqq -\mathrm{Tr}[\rho \log_2 \rho], \tag{17}$$

which is the correct quantum generalization of the Shannon entropy for classical random variables. Other Rényi-α entropies, given for $\alpha \geqslant 1$ by

$$S_\alpha(\rho) \coloneqq \frac{1}{1-\alpha}\log_2 \mathrm{Tr}[\rho^\alpha], \tag{18}$$

although mathematically important, are commonly thought not to have such a direct operational meaning. However, in the constrained Gaussian setting we study here our interest lies not in the correlations possessed by the state per se, but rather in that part of them that can be accessed by the local parties. Since we also assume that these are restricted to Gaussian measurements, we in fact want to look at the correlations displayed by the classical random variables that constitute the outcomes of those measurements. When the random variable X models the outcome of a Gaussian measurement with seed σ performed on the Gaussian state $\rho_{\mathrm{G}}[V, s]$, its Shannon differential entropy, generally defined by the formula

$H(X) = -\int d^{2n}x\, p_X(x) \log_2 p_X(x)$, takes the form [cf. (9)]

$$H(X) = \tfrac{1}{2}\log_2 \det(V+\sigma) + n\log_2(\pi e). \tag{19}$$

This kind of expression, basically the log-determinant of a QCM, up to additive constants, resembles that appearing in the formula for the Rényi-2 entropy of the state,

$$S_2(\rho_{\mathrm{G}}[V,s]) = \tfrac{1}{2}\log_2 \det V = M(V), \tag{20}$$

where M has already been defined in (10). Although (19) and (20) are not identical, they share the same functional form. Hence, in some sense it is the Rényi-2 entropy, and not the von Neumann entropy, that is connected to the Shannon entropy of the experimentally accessible measurement outcomes, when those measurements are also Gaussian. For this precise reason, one can expect the Rényi-2 entropy to play a role in quantifying those correlations of Gaussian states that can be extracted via Gaussian measurements [67]. In fact, quantifiers based on the Rényi-2 entropy and their applications have been extensively investigated [65–67,69,82,83].

Let us start by introducing a simple correlation quantifier known as the *classical mutual information* of the quantum state ρ [84,85]. It is formally given by

$$I^c(A:B)_\rho \coloneqq \sup_{\mathcal{M}_A,\mathcal{M}_B} I(X:Y), \tag{21}$$

where $\mathcal{M}_A$, $\mathcal{M}_B$ are measurements on A and B with outcomes being the classical random variables X and Y. When $\rho_{AB} = \rho_{\mathrm{G}}[V_{AB}, s_{AB}]$ is Gaussian, and $\mathcal{M}_A$, $\mathcal{M}_B$ are also restricted to be Gaussian measurements with seeds Γ_A, Γ_B, the maximal mutual information between the local outcomes becomes the *Gaussian mutual information*, given by [86]

$$I^c_M(A:B)_V \coloneqq \sup_{\Gamma_A,\Gamma_B} I(X:Y)_Q = \sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{V_{AB}+\Gamma_A\oplus\Gamma_B},$$
$$Q_{XY} \coloneqq \left(\mathcal{M}^{\mathrm{G}}_{\Gamma_A}, \mathcal{M}^{\mathrm{G}}_{\Gamma_B}\right)(\rho_{\mathrm{G}}[V_{AB},0]), \tag{22}$$

where the log-determinant mutual information of a bipartite QCM V_{AB} is given by [67]

$$I_M(A:B)_V \coloneqq M(V_A) + M(V_B) - M(V_{AB}) = \frac{1}{2}\log_2 \frac{(\det V_A)(\det V_B)}{\det V_{AB}}. \tag{23}$$

Proving (22) using (14) and (19) is an elementary exercise that is left to the reader. Its solution rests upon the fact that the conditional mutual information is a balanced entropic expression, and hence the "spurious" constant terms in (19) cancel out.

While (22) is difficult to compute in general, it is known that [70,86,87]

$$I^c_M(A:B)_\gamma = \tfrac{1}{2} I_M(A:B)_\gamma = M(\gamma_A) \tag{24}$$

for all pure bipartite QCMs γ_{AB}. We present a self-contained proof of this fact in Appendix A 4, Lemma 16. Note that the last equality simply follows from the fact that the local reductions of a pure state all have the same Rényi entropies.

Moving on from total correlations to entanglement, we can rely on (20) and (10) to form a version of the entanglement of formation called the *Rényi-2 Gaussian entanglement of formation* [65],

$$E^{\mathrm{G}}_{F,2}(V_{AB}) \coloneqq \inf_{\substack{i\Omega_{AB}\leqslant\gamma_{AB}\leqslant V_{AB},\\ \gamma_{AB}\text{ pure}}} \tfrac{1}{2}\log_2\det(\gamma_A). \tag{25}$$

This quantity obeys several properties, most notably it is faithful and *monogamous*: for all QCMs V_{ABC}, it holds that [[66], Corollary 7]

$$E^{\mathrm{G}}_{F,2}(V_{A:BC}) \geqslant E^{\mathrm{G}}_{F,2}(V_{A:B}) + E^{\mathrm{G}}_{F,2}(V_{A:C}), \tag{26}$$

where we use colons to signify the partition we are referring to. When combined with the fact that it comes from a convex roof construction, this implies that $E^{\mathrm{G}}_{F,2}$ is also additive [[67], Corollary 17],

$$E^{\mathrm{G}}_{F,2}\left(V_{AB}^{\oplus n}\right) = n\, E^{\mathrm{G}}_{F,2}(V_{AB}) \qquad \forall\, n. \tag{27}$$

Incidentally, both (26) and (27) are easy corollaries of the identity [[67], Theorem 15]

$$E^{\mathrm{G}}_{F,2}(V_{AB}) = \tfrac{1}{2}\inf_{V_{ABC}} I_M(A:B|C)_V, \tag{28}$$

where

$$I_M(A:B|C)_V \coloneqq M(V_{AC}) + M(V_{BC}) - M(V_C) - M(V_{ABC}) = \frac{1}{2}\log_2 \frac{(\det V_{AC})(\det V_{BC})}{(\det V_C)(\det V_{ABC})} \tag{29}$$

is the *log-determinant conditional mutual information* [67], and the infimum ranges over all extensions V_{ABC} of V_{AB}, i.e., over all QCMs V_{ABC} such that $\Pi_{AB} V_{ABC} \Pi_{AB}^{\intercal} = V_{AB}$. Furthermore, the measure (25) is known to coincide [67] with a Gaussian version of the *squashed entanglement* [12,14,88–90], and it can be analytically computed in a variety of cases of strong physical interest [63,64].

Following an entirely different path, a new entanglement quantifier for Gaussian states has been recently introduced [69–71]. The *Gaussian intrinsic entanglement* $E^{\mathrm{G}}_{\downarrow}(V_{AB})$ of a bipartite Gaussian state with QCM V_{AB} is defined as the minimal *intrinsic information* [9,11,91–97] of the classical random variables obtained upon measuring it with Gaussian measurements, assuming that Eve holds a purification of it but her measurement and classical postprocessing are also Gaussian. Denoting with γ_{ABE} a purification of V_{AB}, we get

$$E^{\mathrm{G}}_{\downarrow}(V_{AB}) \coloneqq \sup_{\Gamma_A,\Gamma_B} \inf_{\Gamma_E} I_M(A:B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E}, \tag{30}$$

where Γ_A, Γ_B, and Γ_E are arbitrary QCM on systems A, B, and E, respectively, and I_M is defined in (29). It is an easy exercise to show that the objective function on the right-hand side of (30) coincides with the conditional mutual information of the triple of random variables generated by carrying out Gaussian measurements with seeds Γ_A, Γ_B, Γ_E on the Gaussian state with QCM V_{ABE}. In formula,

$$I_M(A:B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E} = I(X:Y|Z)_Q,$$
$$Q_{XYZ} = \left(\mathcal{M}^{\mathrm{G}}_{\Gamma_A}\otimes\mathcal{M}^{\mathrm{G}}_{\Gamma_B}\otimes\mathcal{M}^{\mathrm{G}}_{\Gamma_E}\right)(\rho_{\mathrm{G}}[V_{ABE},0]). \tag{31}$$

The proof of (31) is entirely analogous to that of (22). One can show that (30) does not depend on the choice of the purification γ_{ABE} of V_{AB} [69–71]. In order to investigate the asymptotic setting, we will consider the regularization of (30) as well, given by

$$E^{\mathrm{G},\infty}_{\downarrow}(V_{AB}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} E^{\mathrm{G}}_{\downarrow}\left(V_{AB}^{\oplus n}\right). \tag{32}$$

It is also worth noticing that (29) can be cast into the form of an unconditional log-determinant mutual information (23) with the help of Schur complements. Namely, by iteratively applying Schur's determinant factorization formula (A16) one can easily verify that [[67], Eq. (28)]

$$I_M(A:B|E)_{V_{ABE}} = I_M(A:B)_{V_{ABE}/V_E}. \tag{33}$$

III. GAUSSIAN SECRET KEY DISTILLATION PROTOCOLS

We now consider a communication scenario where two separate parties, Alice and Bob, hold a large number n of copies of a bipartite state ρ_{AB} and want to exploit them to generate a secret key by employing only Gaussian local operations and public communication (GLOPC). It is always understood that we grant them access to local randomness, modelled by random variables that are independent of everything else.

A generic *GLOPC protocol* can be formalized as a quantum-to-classical channel from the bipartite CV system AB to a set of classical alphabets $\mathcal{K}\mathcal{K}'\mathcal{C}$ (with $\mathcal{K}$ and $\mathcal{K}'$ finite and identical) controlled by Alice, Bob, and the eavesdropper Eve, respectively. Such a protocol will thus be composed of the following steps: (i) Alice performs a Gaussian measurement protocol on A conditioned on some local random variable U_1. (ii) She uses the measurement outcome X_1 together with U_1 to prepare a message C_1, which is sent to Bob and Eve. (iii) Bob performs a Gaussian measurement protocol on B conditioned on C_1 and on some other local random variable V_1. He uses the measurement outcome Y_1 together with V_1 and C_1 to prepare a message C_1', which is sent to Alice and Eve. (iv) After $2r$ back-and-forth rounds the communication ceases. Alice uses her local random variables $U_1, \ldots, U_r$, the measurement outcomes $X_1, \ldots, X_r$, and Bob's messages $C_1', \ldots, C_r'$ to prepare a random variable S stored in $\mathcal{K}$, that is, her share of the secret key. Bob does the same with his local random variables $V_1, \ldots, V_r$, his measurement outcomes $Y_1, \ldots, Y_r$, and Alice's messages $C_1, \ldots, C_r$, generating his share of the key S' and storing it into $\mathcal{K}'$.

In what follows, we will also consider two restricted classes of Gaussian protocols. First, the **1**-*GLOPC protocols*, in which public communication is permitted only in one direction, say from Alice to Bob (see Fig. 1). Second, the protocols that can be implemented with Gaussian local (destructive) measurements and public communication (*GLMPC protocols*); these start with Alice and Bob making preliminary Gaussian measurements on their entire local subsystems, and then processing only the obtained classical variables with the help of two-way public communication.

Unless otherwise specified, we will always assume that Eve has access to a purification of the initial quantum state of Alice and Bob and can intercept all publicly exchanged messages (denoted with C), storing them in her register $\mathcal{C}$.

A. Distillable secret key

Generally speaking, we say that a number $R > 0$ is an *achievable rate* for secret key distillation from the state ρ_{AB} with a class of protocols $\mathscr{P}$ if there exist transformations $\Lambda_n \in \mathscr{P}$ taking as inputs states on A^nB^n and producing as outputs random variables S_n, S_n', C_n in classical registers $\mathcal{K}_n\mathcal{K}_n'\mathcal{C}_n$, with the range of S_n, S_n' being $\{1, \ldots, 2^{\lceil Rn \rceil}\}$, in such a way that [97]

$$\lim_{n\to\infty} \inf_{\substack{\Lambda_n : A^nB^n \to \mathcal{K}_n\mathcal{K}_n'\mathcal{C}_n, \\ \omega_{\mathcal{C}_nE^n}}} \left\| \Lambda_n\left(\Psi_{ABE}^{\otimes n}\right) - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n\mathcal{K}_n'} \otimes \omega_{\mathcal{C}_nE^n} \right\|_1 = 0. \tag{34}$$

Here, Ψ_{ABE} denotes a purification of ρ_{AB}, $\kappa_N := \sum_{i=1}^N |ii\rangle\langle ii|$ is an ideal secret key of length $\lceil Rn \rceil$, and the minimization is over all classical-quantum states $\omega_{\mathcal{C}_nE^n}$. The meaning of (34) is that the key held by Alice and Bob is asymptotically decoupled from Eve's system, and is thus sufficiently secure to be used in applications [98].

Definition 1. The *$\mathscr{P}$-distillable secret key* $K_{\mathscr{P}}$ of the state ρ_{AB} is the supremum of all rates achievable with protocols in $\mathscr{P}$, $K_{\mathscr{P}}(\rho_{AB}) := \sup R > 0$ such that Eq. (34) holds.

In this paper we are naturally interested in the case where ρ_{AB} is a Gaussian state with QCM V_{AB}, and the considered protocols are either GLOPC, or 1-GLOPC, or GLMPC. The associated secret keys are easily seen to depend on V_{AB} only; we will denote them with the shorthand notation $K_{\leftrightarrow}^{\mathrm{G}}(V_{AB})$, $K_{\rightarrow}^{\mathrm{G}}(V_{AB})$, and $K_{\leftrightarrow}^{\mathrm{G,M}}(V_{AB})$, respectively.

A particularly useful upper bound on $K_{\mathscr{P}}(V_{AB})$ can be established by forcing Eve to apply a Gaussian measurement with pure seed of her choice before the beginning of the

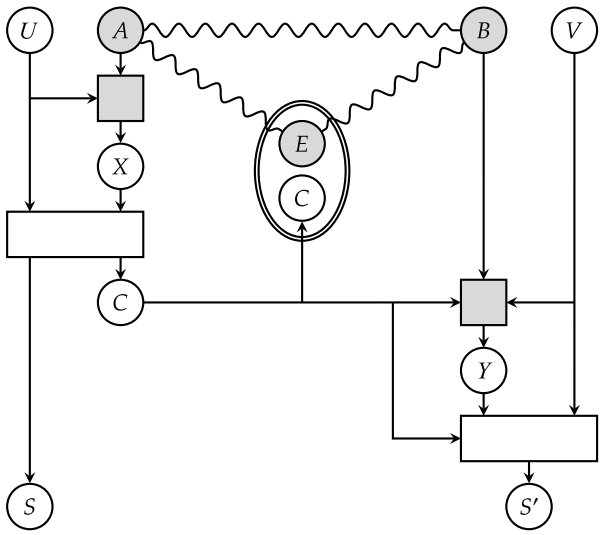

FIG. 1. A pictorial representation of a generic 1-GLOPC protocol. (i) Alice performs a Gaussian measurement protocol on A conditioned on some local random variable U, obtaining an outcome X. (ii) She uses X together with U to prepare two random variables, S (her share of the secret key) and C (message, sent to Bob and intercepted by Eve). (iii) Bob performs a Gaussian measurement protocol on B conditioned on C and on some other local random variable V, obtaining an outcome Y. (iv) Bob uses Y together with V and C to prepare a random variable S' (his share of the secret key). In the picture, white circles stand for classical random variables, grey circles for quantum systems, and wavy lines for correlations (possibly quantum entanglement). Processes are represented by rectangles, either grey, if they involve quantum systems, or white, if they are purely classical. The central ellipse is Eve's system, which may contain a quantum part E correlated with the initial state of Alice and Bob.

protocol, and to broadcast the obtained outcome to Alice and Bob together with the description of Γ_E. From (15) we know that in this case the state that Alice and Bob share is Gaussian and has QCM

$$\tau_{AB} = (\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E), \tag{35}$$

where γ_{ABE} is a purification of the QCM V_{AB}. Since Alice and Bob also know Eve's measurement outcome, they can easily apply local displacements and have their state's mean vanish. The protocols then proceed as detailed earlier in this section. Note that Eve's measurement outcome is now independent of Alice and Bob's state and is thus useless. We summarize this discussion by giving the following definition.

Definition 2. For $\mathscr{P} \in \{GLOPC, 1\text{-}GLOPC, GLMPC\}$, the *modified* $\mathscr{P}$*-distillable secret key* associated with a Gaussian state with QCM V_{AB}, denoted $\widetilde{K}_{\mathscr{P}}(V_{AB})$—or more succinctly $\widetilde{K}^{\mathrm{G}}_{\leftrightarrow}(V_{AB})$, $\widetilde{K}^{\mathrm{G}}_{\rightarrow}(V_{AB})$, $\widetilde{K}^{\mathrm{G,M}}_{\leftrightarrow}(V_{AB})$—is the supremum of all numbers $R > 0$ such that

$$\lim_{n\to\infty} \sup_{\Gamma_{E^n}} \inf_{\substack{\Lambda_n : A^nB^n \to \mathcal{K}_n\mathcal{K}'_n\mathcal{C}_n, \\ Q_{\mathcal{C}_n}}} \Big\| \Lambda_n\big(\rho_{\mathrm{G}}\big[\big(\gamma^{\oplus n}_{ABE} + \Gamma_{E^n}\big) \big/ \big(\gamma^{\oplus n}_{E} + \Gamma_{E^n}\big),\, 0\big]\big) - (\kappa_{2^{\lceil Rn\rceil}})_{\mathcal{K}_n\mathcal{K}'_n} \otimes Q_{\mathcal{C}_n} \Big\|_1 = 0, \tag{36}$$

where $Q_{\mathcal{C}_n}$ is an arbitrary probability distribution over the alphabet $\mathcal{C}_n$.

It should be clear that the new class of protocols in Definition 2 allows for a secret key distillation rate that is never smaller than that corresponding to the protocols in Definition 1, because in the former case Eve is forced to lose access to her quantum system at an early stage. We give a formal proof of this below.

Lemma 3. For all $\mathscr{P} \in \{GLOPC, 1\text{-}GLOPC, GLMPC\}$ and all QCMs V_{AB}, it holds that

$$K_{\mathscr{P}}(V_{AB}) \leqslant \widetilde{K}_{\mathscr{P}}(V_{AB}), \tag{37}$$

where $K_{\mathscr{P}}(V_{AB})$ and $\widetilde{K}_{\mathscr{P}}(V_{AB})$ are given in Definitions 1 and 2, respectively.

Proof. Let $R > 0$ be an achievable rate for $K_{\mathscr{P}}(V_{AB})$. Construct a sequence of protocols $\Lambda_n : A^nB^n \to \mathcal{K}_n\mathcal{K}'_n\mathcal{C}_n$ of class $\mathscr{P}$, where $\mathcal{K}_n$, $\mathcal{K}'_n$ are two copies of an alphabet of size $2^{\lceil Rn\rceil}$, and a sequence of states $\omega_{\mathcal{C}_nE^n}$, such that

$$\lim_{n\to\infty} \big\| \Lambda_n\big(\rho^{\otimes n}_{ABE}\big) - (\kappa_{2^{\lceil Rn\rceil}})_{\mathcal{K}_n\mathcal{K}'_n} \otimes \omega_{\mathcal{C}_nE^n} \big\|_1 = 0. \tag{38}$$

For a fixed n, consider an arbitrary QCM Γ_{E^n}. For a vector $x \in \mathcal{F}_n := \mathbb{R}^{2nm_E}$, with m_E being the number of modes of E, let $p(x)$ denote the value on x of the probability density function of the outcome of the Gaussian measurement with seed Γ_{E^n} on Eve's share of the state $\rho^{\otimes n}_{ABE}$. Also, let $t^x_{A^nB^n} = (t^x_{A^n},\, t^x_{B^n}) \in \mathbb{R}^{2n(m_A+m_B)}$ be the displacement vector of the post-measurement state on A^nB^n corresponding to the outcome x.

We now construct a modified protocol $\Lambda'_n : A^nB^n \to \mathcal{K}_n\mathcal{K}'_n\mathcal{C}_n\mathcal{F}_n$ of class $\mathscr{P}$, where the measurable space $\mathcal{F}_n = \mathbb{R}^{2nm_E}$ pertains to Eve. To do this, we distinguish two separate cases. If $\mathscr{P} \in \{\mathrm{GLOPC}, 1\text{-GLOPC}\}$, then Λ'_n proceeds as follows: (i) Alice draws a local random variable X on $\mathcal{F}_n$ distributed according to p, applies to A^n the displacement unitary $D(t^X_{A^n})$, and then continues with her (first) Gaussian measurement protocol as prescribed by Λ_n. (ii) During the (first) round of communication, Alice sends to Bob and Eve not only the message originally prescribed by Λ_n, but also the random variable X. (iii) Before continuing with his (first) Gaussian measurement protocol dictated by Λ_n, Bob applies a displacement unitary $D(t^X_{B^n})$ to his share of the system. (iv) The protocol continues with further communication rounds (if $\mathscr{P} = \mathrm{GLOPC}$) or directly with key generation (if $\mathscr{P} = 1\text{-GLOPC}$) as prescribed by Λ_n.

If instead $\mathscr{P} = \mathrm{GLMPC}$, the modified protocol Λ'_n is even simpler: (i) Alice and Bob apply global Gaussian measurements to their entire subsystems as dictated by Λ_n, obtaining measurement outcomes Z_n and W_n, respectively. (ii) Before preparing her first message for Bob, Alice draws a local random variable X on $\mathcal{F}_n$ distributed according to p and translates Z_n by $t^X_{A^n}$. (iii) Alice then sends to Bob not only the message originally prescribed by Λ_n, but also X. (iv) Before preparing his first message for Alice, Bob translates W_n by $t^X_{B^n}$. (v) The protocol continues with further communication rounds and then with key generation as prescribed by Λ_n.

It is not too difficult to verify that in all three cases

$$\Lambda'_n(\cdot) = \int d^{2nm_E}x\; p(x) \big(\Lambda_n \circ \mathscr{D}\big(t^x_{A^nB^n}\big)\big)(\cdot) \otimes |x\rangle\langle x|_{\mathcal{F}_n},$$
$$\mathscr{D}\big(t^x_{A^nB^n}\big)(\cdot) := D\big(t^x_{A^n}\big) \otimes D\big(t^x_{B^n}\big)\,(\cdot)\, D\big(-t^x_{A^n}\big) \otimes D\big(-t^x_{B^n}\big), \tag{39}$$

with the system $\mathcal{F}_n$ storing X being on Eve's side. Let us now estimate the figure of merit in (36) for this protocol. We have that

$$\begin{aligned}
&\inf_{Q_{\mathcal{C}_n\mathcal{F}_n}} \big\| \Lambda'_n\big(\rho_{\mathrm{G}}\big[\big(\gamma^{\oplus n}_{ABE} + \Gamma_{E^n}\big)\big/\big(\gamma^{\oplus n}_{E} + \Gamma_{E^n}\big),\, 0\big]\big) - \kappa_{2^{\lceil Rn\rceil}} \otimes Q_{\mathcal{C}_n\mathcal{F}_n} \big\|_1 \\
&\overset{1}{=} \inf_{Q_{\mathcal{C}_n\mathcal{F}_n}} \left\| \int d^{2nm_E}x\; p(x) (\Lambda_n \circ \mathscr{D}(t^x_{A^nB^n}))\big(\rho_{\mathrm{G}}\big[\big(\gamma^{\oplus n}_{ABE} + \Gamma_{E^n}\big)\big/\big(\gamma^{\oplus n}_{E} + \Gamma_{E^n}\big),\, 0\big]\big) \otimes |x\rangle\langle x|_{\mathcal{F}_n} - \kappa_{2^{\lceil Rn\rceil}} \otimes Q_{\mathcal{C}_n\mathcal{F}_n} \right\|_1 \\
&\overset{2}{\leqslant} \left\| \int d^{2nm_E}x \left(p(x)\, \Lambda_n\big(\rho_{\mathrm{G}}\big[\big(\gamma^{\oplus n}_{ABE} + \Gamma_{E^n}\big)\big/\big(\gamma^{\oplus n}_{E} + \Gamma_{E^n}\big),\, t^x_{A^nB^n}\big]\big) \otimes |x\rangle\langle x|_{\mathcal{F}_n} - \kappa_{2^{\lceil Rn\rceil}} \otimes \mathrm{Tr}_{E^n}[\omega_{\mathcal{C}_nE^n}\rho_{\mathrm{G}}[\Gamma_{E^n}, x]] \otimes |x\rangle\langle x|_{\mathcal{F}_n}\right) \right\|_1 \\
&\overset{3}{\leqslant} \big\| \Lambda_n\big(\rho_{\mathrm{G}}\big[\gamma^{\oplus n}_{ABE},\, 0\big]\big) - \kappa_{2^{\lceil Rn\rceil}} \otimes \omega_{\mathcal{C}_nE^n} \big\|_1.
\end{aligned}$$

Here, in 1 we used (39); in 2 we let the displacement act on the Gaussian state and considered the ansatz $Q_{\mathcal{C}_n\mathcal{F}_n} = \int d^{2nm_E}x \;\; \mathrm{Tr}_{E^n}[\omega_{\mathcal{C}_nE^n}\rho_{\mathrm{G}}[\Gamma_{E^n}, x]] \otimes |x\rangle\langle x|_{\mathcal{F}_n}$, which is nothing but the probability distribution obtained by making the Gaussian measurement with seed Γ_{E^n} on $\omega_{\mathcal{C}_n\mathcal{F}_n}$; finally, 3 follows from the data processing inequality for the trace norm. Taking the supremum over Γ_{E^n} yields $\sup_{\Gamma_{E^n}} \inf_{Q_{\mathcal{C}_n\mathcal{F}_n}} \|\Lambda'_n(\rho_{\mathrm{G}}[(\gamma_{ABE}^{\oplus n} + \Gamma_{E^n})/(\gamma_E^{\oplus n} + \Gamma_{E^n}),\, 0]) - \kappa_{2^{\lceil Rn\rceil}} \otimes Q_{\mathcal{C}_n\mathcal{F}_n}\|_1 \leqslant \|\Lambda_n(\rho_{\mathrm{G}}[\gamma_{ABE}^{\oplus n},\, 0]) - \kappa_{2^{\lceil Rn\rceil}} \otimes \omega_{\mathcal{C}_nE^n}\|_1 \xrightarrow[n\to\infty]{} 0$, where we used (38). In light of Definition 2, this shows that R is also an achievable rate for $\widetilde{K}_{\mathscr{P}}(V_{AB})$, concluding the proof. ■

IV. BOUNDS TO GAUSSIAN SECRET KEY DISTILLATION

We now present our main results establishing fundamental upper bounds on the secret key that can be distilled by means of the Gaussian protocols introduced in Sec. III. To keep the presentation accessible, some auxiliary results and more technical derivations will be deferred to Appendixes.

A. One-way public communication

As announced, our first result is a bound on the 1-GLOPC distillable secret key of an arbitrary Gaussian state.

Theorem 4. For all QCMs V_{AB}, it holds that

$$K^{\mathrm{G}}_{\rightarrow}(V_{AB}) \leqslant E^{\mathrm{G}}_{F,2}(V_{AB}). \tag{40}$$

If $V_{AB} = \gamma_{AB}$ is pure, then (40) is tight, i.e.,

$$K^{\mathrm{G}}_{\rightarrow}(\gamma_{AB}) = E^{\mathrm{G}}_{F,2}(\gamma_{AB}) = \tfrac{1}{2}\log_2 \det(\gamma_A). \tag{41}$$

Since the right-hand side of (40) does not depend on the direction of communication, (40) holds irrespectively of whether we consider Alice-to-Bob or Bob-to-Alice public communication, as long as we do not allow both. The protocol achieving (41) consists in the application of local homodyne measurements followed by a classical secret key distillation protocol [8,9]. To prove (40), we will make use of the modified secret key $\widetilde{K}^{\mathrm{G}}_{\rightarrow}(V_{AB})$ introduced in Definition 2 and establish the following chain of inequalities, $K^{\mathrm{G}}_{\rightarrow}(V_{AB}) \leqslant \widetilde{K}^{\mathrm{G}}_{\rightarrow}(V_{AB}) \leqslant E^{\mathrm{G}}_{F,2}(V_{AB})$, where the leftmost one follows from Lemma 3.

Proof. Let γ_{ABE} be a purification of V_{AB}, and let us consider a 1-GLOPC protocol applied on the corresponding Gaussian state. Let us look at the situation right before Bob's measurement (see Fig. 1). Almost all "quantumness" has disappeared, in the sense that the only party still holding a quantum state is Bob. From the point of view of Alice, who knows the value of U, the Gaussian measurement protocol she has applied in the first step, and the associated outcome X, Bob's state $\rho_{B|U,X}$ is Gaussian.

We now claim that this situation can be simulated by an entirely classical system. Namely, let W_B be a random variable on the phase space $\mathbb{R}^{2m_B}$ of Bob's system whose probability distribution conditioned on the values of U and X coincides with the Wigner function of $\rho_{B|U,X}$, which is everywhere positive because $\rho_{B|U,X}$ is Gaussian. Noting that (a) the vacuum itself has positive Wigner function; (b) any Gaussian unitary amounts to a linear transformation at the phase space level, and thus preserves the positivity of the Wigner function; and (c) the POVM elements describing Gaussian measurements also have positive Wigner function, by inspecting the definition of Gaussian measurement protocol (Sec. II C) we see that step (iii) in Fig. 1 can be simulated by purely classical operations on W_B, C, and V. We are therefore in the situation depicted in Fig. 2.

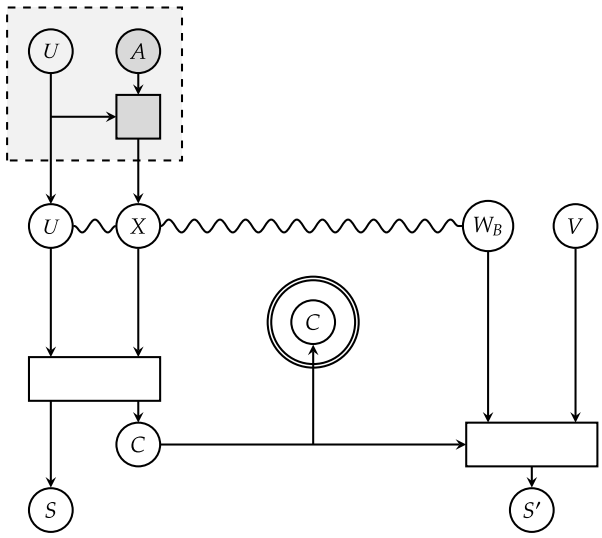

FIG. 2. The modified protocol used in the proof of Theorem 4. Once the Gaussian protocol on A has been carried out, we can think of the B system as formally simulated by the classical random variable W_B whose distribution conditioned on UX coincides with the Wigner function of the (Gaussian) reduced state on B corresponding to the recorded values of U and X.

We can proceed by following to a certain extent the technique introduced by Maurer [5]. In what follows, we will compute conditional entropies and mutual informations between random variables that are both discrete (U, S, C, S', V) and continuous (X and W_B). In the latter case it is understood that we employ the differential entropy (measured in bits) instead of the discrete one, although we will denote both with the symbol H for simplicity. Remember that a linear entropy inequality involving differential entropies is valid if and only if its discrete counterpart is "balanced" and valid [99]. Our derivation rests only upon balanced inequalities. We start by writing

$$H(S) = I(S:C) + H(S|C). \tag{42}$$

Now,

$$\begin{aligned} H(S|C) &= H(SUX|C) - H(UX|SC) \\ &= H(UX|C) - H(UX|SC) \\ &\overset{1}{\leqslant} H(UX|C) - H(UX|SCVW_B) \\ &= H(UX|C) - H(UXS|CVW_B) + H(S|CVW_B) \\ &\overset{2}{=} H(UX|C) - H(UX|CVW_B) + H(S|CVW_B) \\ &= I(UX:VW_B|C) + H(S|CVW_B) \\ &\overset{3}{\leqslant} I(UX:VW_B|C) + H(S|S') \\ &\overset{4}{=} I(UX:W_B|C) + H(S|S'). \end{aligned} \tag{43}$$

Here, 1 comes from data processing; 2 is a consequence of the fact that S is a deterministic function of U and X; 3 is again data processing, using the fact that S' is a deterministic function of C, V, and W_B; finally, 4 uses that V is independent of U, X, and W_B, even conditioned on C. Now, observe that

$$\begin{aligned} I(UX : W_B|C) &= H(W_B|C) - H(W_B|UXC) \\ &= H(W_B|C) - H(W_B|UX) \\ &\overset{5}{\leqslant} H(W_B) - H(W_B|UX) \\ &\overset{6}{\leqslant} H(W_B) - m_B \log_2(\pi e) \\ &\overset{7}{=} M(\tau_B). \end{aligned} \tag{44}$$

Note that 5 is just the positivity of the mutual information $I(W_B : C) \geqslant 0$, 6 is a rephrase of (11), and 7 comes from (9). Combining (42)–(44) yields

$$H(S) \leqslant I(S : C) + H(S|S') + M(\tau_B). \tag{45}$$

We now consider a sequence of 1-GLOPC protocols $\Lambda_n : A^n B^n \to \mathcal{K}_n \mathcal{K}'_n \mathcal{C}_n$ with rate R as in Definition 2. Pick numbers $\epsilon_n > 0$ such that

$$\begin{aligned} \epsilon_n > \sup_{\Gamma_{E^n}} \inf_{Q_{\mathcal{C}_n}} \Big\| \Lambda_n\Big(\rho_{\mathrm{G}}\Big[\big(\gamma_{ABE}^{\oplus n} + \Gamma_{E^n}\big)\big/\big(\gamma_E^{\oplus n} + \Gamma_{E^n}\big),\ 0\Big]\Big) \\ - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes Q_{\mathcal{C}_n} \Big\|_1 \end{aligned} \tag{46}$$

and

$$\lim_{n\to\infty} \epsilon_n = 0. \tag{47}$$

Now, consider a fixed sequence of QCMs Γ_{E^n}. Set

$$\tau_{A^n B^n} \coloneqq \big(\gamma_{ABE}^{\oplus n} + \Gamma_{E^n}\big)\big/\big(\gamma_E^{\oplus n} + \Gamma_{E^n}\big), \tag{48}$$

denote by S_n, S'_n the keys produced by the protocol Λ_n run with input $\rho_{\mathrm{G}}[\tau_{A^n B^n},\ 0]$, and let C_n be the message exchanged. Applying (45), we see that

$$H(S_n) \leqslant I(S_n : C_n) + H(S_n|S'_n) + M(\tau_{B^n}). \tag{49}$$

By tracing away E_n, from (46) we deduce that the probability distribution $P_{S_n S'_n}$ is at least ϵ_n-close in total variation norm to that of two perfectly correlated copies of the key. In turn, this ensures that $\Pr\{S_n \neq S'_n\} < \epsilon_n$. Hence, Fano's inequality [100] gives

$$H(S_n|S'_n) < h_2(\epsilon_n) + \epsilon_n \log_2(|S_n| - 1) \leqslant h_2(\epsilon_n) + \lceil Rn \rceil \epsilon_n, \tag{50}$$

where $h_2(x) \coloneqq -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy, and we remembered that $|S_n| = 2^{\lceil Rn \rceil}$.

The same reasoning guarantees that P_{S_n} is at least ϵ_n-close in total variation norm to the uniform distribution over an alphabet of size $2^{\lceil Rn \rceil}$, whose entropy (measured in bits, as usual) is naturally given by $\lceil Rn \rceil$. The Fannes–Auedenaert inequality [101,102] thus guarantees that

$$\begin{aligned} H(S_n) &\geqslant \lceil Rn \rceil - \frac{\epsilon_n}{2} \log_2\big(2^{\lceil Rn \rceil} - 1\big) - h_2\Big(\frac{\epsilon_n}{2}\Big) \\ &\geqslant \lceil Rn \rceil - \frac{\epsilon_n}{2} \lceil Rn \rceil - h_2\Big(\frac{\epsilon_n}{2}\Big). \end{aligned} \tag{51}$$

The last consequence of (46) we are interested in can be deduced by tracing away the K' system. By doing so we see that the joint random variable $S_n C_n$ is at least ϵ_n-close in total variation norm to a pair $\widetilde{S}_n \widetilde{C}_n$ of independent random variables such that $\widetilde{S}_n$ is uniformly distributed over an alphabet of size $2^{\lceil Rn \rceil}$. We deduce that

$$\begin{aligned} I(S_n : C_n) &= H(S_n) - H(S_n|C_n) \\ &\overset{8}{\leqslant} H(\widetilde{S}_n) - H(S_n|C_n) \\ &\overset{9}{=} H(\widetilde{S}_n|\widetilde{C}_n) - H(S_n|C_n) \\ &\overset{10}{\leqslant} \frac{\epsilon_n}{2} \log_2\big(2^{\lceil Rn \rceil} - 1\big) + h_2\Big(\frac{\epsilon_n}{2}\Big) \\ &\leqslant \frac{\epsilon_n}{2} \lceil Rn \rceil + h_2\Big(\frac{\epsilon_n}{2}\Big). \end{aligned} \tag{52}$$

The above derivation is justified as follows: In 8 we observed that $H(\widetilde{S}_n) = \lceil Rn \rceil \geqslant H(S_n)$; in 9 we used the fact that $\widetilde{S}_n$ and $\widetilde{C}_n$ are independent; finally, in 10 we exploited the asymptotic continuity of the conditional entropy [103–106].

Combining (48)–(52) yields the bound

$$\begin{aligned} \lceil Rn \rceil < 2\epsilon_n \lceil Rn \rceil + 2\, h_2\Big(\frac{\epsilon_n}{2}\Big) + h_2(\epsilon_n) \\ + M\big(\big(\gamma_{AE}^{\oplus n} + \Gamma_{E^n}\big)\big/\big(\gamma_E^{\oplus n} + \Gamma_{E^n}\big)\big). \end{aligned} \tag{53}$$

Since this holds for all pure QCMs Γ_{E^n}, we can take the infimum of the last addend over Γ_{E^n}. Note that

$$\begin{aligned} \inf_{\Gamma_{E^n} \text{ pure QCM}} & M\big(\big(\gamma_{AE}^{\oplus n} + \Gamma_{E^n}\big)\big/\big(\gamma_E^{\oplus n} + \Gamma_{E^n}\big)\big) \\ &\overset{11}{=} \frac{1}{2} \inf_{\Gamma_{E^n} \text{ pure QCM}} I_M(A^n : B^n)_{(\gamma_{ABE}^{\oplus n} + \Gamma_{E^n})/(\gamma_E^{\oplus n} + \Gamma_{E^n})} \\ &\overset{12}{=} E_{F,2}^{\mathrm{G}}\big(V_{AB}^{\oplus n}\big) \\ &\overset{13}{=} n\, E_{F,2}^{\mathrm{G}}(V_{AB}). \end{aligned} \tag{54}$$

Here, 11 is a consequence of (A26), while 12 is an application of the nontrivial fact that the Rényi-2 Gaussian entanglement of formation coincides with the Rényi-2 Gaussian squashed entanglement for all Gaussian states [[67], Theorem 5 and Remark 2] [cf. (28); remember that γ_{ABE} is a purification of V_{AB}]. Finally, 13 follows from the additivity of the Rényi-2 Gaussian entanglement of formation [[67], Corollary 1]. Therefore, optimizing (53) over pure QCMs Γ_{E^n} and using (54) yields

$$\lceil Rn \rceil < 2\epsilon_n \lceil Rn \rceil + 2\, h_2\Big(\frac{\epsilon_n}{2}\Big) + h_2(\epsilon_n) + n\, E_{F,2}^{\mathrm{G}}(V_{AB}). \tag{55}$$

Dividing by n, taking the limit $n \to \infty$ and using the continuity of the binary entropy together with the fact that $\epsilon_n \xrightarrow[n\to\infty]{} 0$ finally gives that

$$R < E_{F,2}^{\mathrm{G}}(V_{AB}). \tag{56}$$

Taking the supremum over achievable rates R, we then see that

$$\widetilde{K}_{\to}^{\mathrm{G}}(V_{AB}) \leqslant E_{F,2}^{\mathrm{G}}(V_{AB}), \tag{57}$$

which together with (37) proves (40).

It remains to prove (41). Fortunately, this is much easier to do: Indeed, it suffices to exhibit a protocol that starting with

an arbitrary number of copies of a pure QCM γ_{AB} achieves a secret key distillation rate that is arbitrarily close to $M(\gamma_A)$. To do this, fix $\epsilon > 0$, and apply (24) to select two Gaussian measurements with seeds Γ_A and Γ_B such that

$$I_M(A:B)_{\gamma_{AB}+\Gamma_A\oplus\Gamma_B} \geqslant M(\gamma_A) - \frac{\epsilon}{3}. \tag{58}$$

Calling X and Y the outcomes of those measurements, we know that $I(X:Y) = I_M(A:B)_{\gamma_{AB}+\Gamma_A\oplus\Gamma_B}$. Hence, $I(X:Y) \geqslant M(\gamma_A) - \frac{\epsilon}{3}$ also holds. If Alice and Bob carry out the aforementioned Gaussian measurements separately on every single copy of γ_{AB} they share, by applying the above procedure they obtain n independent copies of the jointly Gaussian random variables X and Y. Now, let Alice and Bob "bin" the continuous variables X and Y so as to obtain discrete random variables X' and Y' with the property that $I(X':Y') \geqslant I(X:Y) - \epsilon/3 \geqslant M(\gamma_A) - 2\epsilon/3$. This is known to be possible [107], and indeed can be verified by elementary means, e.g., exploiting the uniform continuity of Gaussian distributions.

At this point, we can use a special case of a result proved by Maurer [[8], Theorem 4] (see also previous works by Maurer himself [5] as well as Ahlswede and Csiszar [[9], Proposition 1]), and later generalized to the classical-quantum case in the fundamental work by Devetak and Winter [[108], Theorem 1]. For the case where Eve has no prior information, it states that the secret key distillation rate that one can achieve from i.i.d. copies of a correlated pair (X', Y') of discrete random variables by means of one-way public communication [109] coincides with the mutual information $I(X':Y')$ [110]. To apply Maurer's achievability result, we need to verify that his security criterion is stronger than ours. Writing out everything for the case where Eve has no prior information, a side-by-side comparison of the two security criteria is as follows:

$$\text{Maurer [8 Definition 2]:} \quad \begin{aligned} &\Pr\{S \neq S'\} \leqslant \epsilon, \\ &I(S:C) \leqslant \epsilon \\ &H(S) \geqslant \lceil Rn \rceil - \epsilon. \end{aligned} \tag{59}$$

$$\text{This paper (Definition 1):} \quad \inf_{Q_C} \left\| P_{SS'C} - \frac{\delta_{SS'}}{2^{\lceil Rn \rceil}} \otimes Q_C \right\|_1 \leqslant \epsilon'. \tag{60}$$

Here, $|S|$ is the size of the alphabet of S, and $\delta_{SS'}/N$ is the perfectly correlated uniform distribution of size N. We now verify that (59) implies (60) for some ϵ' universally related to ϵ. For the sake of simplicity, we write out the argument in the case where the random variable C ranges over a discrete alphabet. We have that

$$\begin{aligned}
&\inf_{Q_C} \left\| P_{SS'C} - \frac{\delta_{SS'}}{2^{\lceil Rn \rceil}} \otimes Q_C \right\|_1 \\
&\leqslant \left\| P_{SS'C} - \frac{\delta_{SS'}}{2^{\lceil Rn \rceil}} \otimes P_C \right\|_1 \\
&= \sum_{s,s',c} \left| P_{SS'C}(s,s',c) - \frac{\delta_{s,s'}}{2^{\lceil Rn \rceil}} P_C(c) \right| \\
&= \sum_{s\neq s',\, c} P_{SS'C}(s,s',c) + \sum_{s,c} \left| P_{SS'C}(s,c) - \frac{\delta_{s,s'}}{2^{\lceil Rn \rceil}} P_C(c) \right| \\
&= \Pr\{S \neq S'\} + \sum_{s,c} \left| P_{SS'C}(s,c) - \frac{1}{2^{\lceil Rn \rceil}} P_C(c) \right| \\
&\leqslant \Pr\{S \neq S'\} + \sum_{s,c} |P_{SS'C}(s,s,c) - P_{SC}(s,c)| \\
&\quad + \sum_{s,c} |P_{SC}(s,c) - P_S(s)P_C(c)| \\
&\quad + \sum_{s,c} \left| P_S(s)P_C(c) - \frac{1}{2^{\lceil Rn \rceil}} P_C(c) \right| \\
&= 2\Pr\{S \neq S'\} + \|P_{SC} - P_S \otimes P_C\|_1 + \left\| P_S - \frac{\mathbb{1}}{2^{\lceil Rn \rceil}} \right\|_1 \\
&\leqslant 2\Pr\{S \neq S'\} + \sqrt{2\ln 2\, I(S:C)} \\
&\quad + \sqrt{2\ln 2(\lceil Rn \rceil - H(S))} \\
&\leqslant 2(\epsilon + \sqrt{2\ln 2\,\epsilon}).
\end{aligned}$$

Here, in the second to last line we applied twice Pinsker's inequality [111–113], while the last line follows directly from (59).

The above argument shows that $I(X':Y')$ is indeed the supremum of all achievable secret key rates for the random variables (X', Y'). Therefore, any rate of the form $I(X':Y') - \epsilon/3 \geqslant M(\gamma_A) - \epsilon$ is achievable. Since this holds for an arbitrary $\epsilon > 0$, we see that in fact

$$M(\gamma_A) \geqslant \sup\{R\text{: } R \text{ is an achievable rate}\} = K^{\mathrm{G}}_{\rightarrow}(\gamma_{AB}). \tag{61}$$

Together with (40), this establishes (41) and concludes the proof [114]. ■

It is important at this point to recall that, when arbitrary local operations are permitted in conjunction with one- or two-way public communication (1-LOPC or LOPC, respectively), the secret key of any *pure* state ψ_{AB} is well known to equal its local von Neumann entropy $S_1(\psi_A)$, as defined in (17). Instead, (41) features the Rényi-2 entropy (20) of the local state. Since this is typically smaller, $S_2 \leqslant S_1$, our result (41) shows that the Gaussian secret key of any pure Gaussian state is smaller than its unrestricted LOPC secret key, highlighting a fundamental limitation in the ability of Gaussian operations to extract secrecy from quantum states. Later in Sec. VI A we will explore an example of such a limitation in a relevant family of *mixed* Gaussian states as well.

B. Two-way public communication

We now turn to our second main result, a weaker bound on the Gaussian secret key of an arbitrary Gaussian state in the presence of two-way public communication.

Theorem 5. For all QCMs V_{AB}, it holds that

$$K^{\mathrm{G}}_{\leftrightarrow}(V_{AB}) \leqslant 2E^{\mathrm{G}}_{F,2}(V_{AB}). \tag{62}$$

Proof. We will prove that $K^{\mathrm{G}}_{\leftrightarrow}(V_{AB}) \leqslant \widetilde{K}^{\mathrm{G}}_{\leftrightarrow}(V_{AB}) \leqslant 2E^{\mathrm{G}}_{F,2}(V_{AB})$, where the first inequality follows from the case $\mathscr{P} = \mathrm{GLOPC}$ of Lemma 3. To establish the second one, consider as usual a sequence of GLOPC protocols

$\Lambda_n : A^n B^n \to \mathcal{K}_n \mathcal{K}'_n \mathcal{C}_n$ with rate R as in Definition 2. Pick numbers $\epsilon_n > 0$ such that (46) and (47) hold, consider an arbitrary sequence of QCMs Γ_{E^n}, and define the QCM $\tau_{A^n B^n}$ by (48).

Similar to what we saw in the proof of Theorem 4, since the global input state is Gaussian and all measurements, ancillary states, and unitaries are Gaussian, the whole protocol can be simulated by a purely classical process. The input of this simulation is the pair of correlated random variables (W_{A^n}, W_{B^n}), whose joint distribution coincides with the Wigner function of $\rho_{\mathrm{G}}[\tau_{A^n B^n}, 0]$. Let S_n, S'_n be the pair of keys generated by Alice and Bob, and let C_n the messages exchanged. By a result of Maurer, we have that [[5], Theorem 1]

$$H(S_n) \leqslant I(W_{A^n} : W_{B^n}) + H(S_n|S'_n) + I(S_n : C_n). \tag{63}$$

Employing (9) we see immediately that

$$\begin{aligned} I(W_{A^n} : W_{B^n}) &= H(W_{A^n}) + H(W_{B^n}) - H(W_{A^n} W_{B^n}) \\ &= M(\tau_{A^n}) + n m_A \log_2(\pi e) + M(\tau_{B^n}) \\ &\quad + n m_B \log_2(\pi e) - M(\tau_{A^n B^n}) \\ &\quad - n(m_A + m_B) \log_2(\pi e) \\ &= M(\tau_{A^n}) + M(\tau_{B^n}) - M(\tau_{A^n B^n}) \\ &= 2M(\tau_{A^n}), \end{aligned} \tag{64}$$

where the last identity follows because thanks to the discussion following (16) we know that $\tau_{A^n B^n}$ is a pure QCM. Plugging (64), (50), (51), and (52) inside (63) yields $\lceil Rn \rceil < 2\epsilon_n \lceil Rn \rceil + 2\, h_2(\frac{\epsilon_n}{2}) + h_2(\epsilon_n) + 2\, M((\gamma_{AE}^{\oplus n} + \Gamma_{E^n})/(\gamma_E^{\oplus n} + \Gamma_{E^n}))$, and in turn $\lceil Rn \rceil < 2\epsilon_n \lceil Rn \rceil + 2\, h_2(\frac{\epsilon_n}{2}) + h_2(\epsilon_n) + 2n\, E^{\mathrm{G}}_{F,2}(V_{AB})$ upon taking the infimum over Γ_{E^n} as in (54). Dividing by n and taking the limit for $n \to \infty$ gives $R < 2E^{\mathrm{G}}_{F,2}(V_{AB})$, and then

$$\widetilde{K}^{\mathrm{G}}_{\leftrightarrow}(V_{AB}) \leqslant 2E^{\mathrm{G}}_{F,2}(V_{AB}) \tag{65}$$

upon an optimization over all achievable rates R. ■

We conjecture that the factor of 2 in (62) is not tight, and that in fact $K^{\mathrm{G}}_{\leftrightarrow}(V_{AB}) \leqslant E^{\mathrm{G}}_{F,2}(V_{AB})$ holds true for all QCMs V_{AB}. Establishing this would further bolster the operational significance of the Gaussian entanglement measure $E^{\mathrm{G}}_{F,2}$ in the context of QKD. As evidence in favour of our conjecture, we present partial proof of it for the class of protocols GLMPC, corresponding to a scenario where we allow two-way public communication, but only after Alice and Bob perform complete destructive Gaussian measurements on their subsystems. This is the third main result of this paper.

Theorem 6. For all QCMs V_{AB}, it holds that

$$K^{\mathrm{G,M}}_{\leftrightarrow}(V_{AB}) \leqslant E^{\mathrm{G},\infty}_{\downarrow}(V_{AB}) \leqslant E^{\mathrm{G}}_{F,2}(V_{AB}) \tag{66}$$

and moreover

$$E^{\mathrm{G}}_{\downarrow}(V_{AB}) \leqslant E^{\mathrm{G}}_{F,2}(V_{AB}). \tag{67}$$

The argument we use to prove Theorem 6 is very close in spirit to those proposed by Maurer [5], Ahlswede and Csiszar [9], and Maurer and Wolf [91] to upper bound the secret key capacity of a tripartite probability distribution. In the latter two papers, in particular, the notion of *intrinsic information* was introduced and discussed at length (see [[9], Theorem 1] and [[91], §II]).

Proof. We start by proving the first inequality in (66). Let Alice, Bob and Eve start with n copies of the pure Gaussian state with QCM γ_{ABE}, so that the global QCM reads $\gamma_{ABE}^{\oplus n}$. Consider a sequence of GLMPC protocols $\Lambda_n : A^n B^n \to \mathcal{K}_n \mathcal{K}'_n \mathcal{C}_n$ such that

$$\begin{aligned} &\inf_{\omega_{\mathcal{C}_n E^n}} \left\| \Lambda_n\big(\rho_{\mathrm{G}}\big[\gamma_{ABE}^{\otimes n}, 0\big]\big) - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes \omega_{\mathcal{C}_n E^n} \right\|_1 < \epsilon_n, \\ &\lim_{n \to \infty} \epsilon_n = 0, \end{aligned} \tag{68}$$

for some rate $R > 0$, as per Definition 1. By construction, the GLMPC protocol Λ_n can be decomposed as

$$\Lambda_n = \Lambda_n^c \circ \big(\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}}\big), \tag{69}$$

where $\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}}$ and $\mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}}$ are complete destructive Gaussian measurements with seeds Γ_{A^n} and Γ_{B^n} on Alice's and Bob's side, respectively, and Λ_n^c is a classical protocol involving only local operations and public communication. For a formal representation of the quantum-classical channels $\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}}, \mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}}$, see (13).

Now, consider an arbitrary Gaussian measurement $\mathcal{M}^{\mathrm{G}}_{\Gamma_{E^n}}$ with seed Γ_{E^n} on Eve's subsystem; denote the corresponding output alphabet with $\mathcal{Z}_n = \mathbb{R}^{2nm_E}$. Employing first the data processing inequality for the trace norm and then (69) yields

$$\begin{aligned} \epsilon_n &> \inf_{\omega_{\mathcal{C}_n E^n}} \left\| \Lambda_n\big(\rho_{\mathrm{G}}\big[\gamma_{ABE}^{\otimes n}, 0\big]\big) - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes \omega_{\mathcal{C}_n E^n} \right\|_1 \\ &\geqslant \inf_{Q_{\mathcal{C}_n \mathcal{Z}_n}} \sup_{\Gamma_{E^n}} \Big\| \big(\Lambda_n \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{E^n}}\big)\big(\rho_{\mathrm{G}}\big[\gamma_{ABE}^{\otimes n}, 0\big]\big) \\ &\quad - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes Q_{\mathcal{C}_n \mathcal{Z}_n} \Big\|_1 \\ &= \inf_{Q_{\mathcal{C}_n \mathcal{Z}_n}} \sup_{\Gamma_{E^n}} \Big\| \Lambda_n^c\Big(\big(\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{E^n}}\big)\big(\rho_{\mathrm{G}}\big[\gamma_{ABE}^{\otimes n}, 0\big]\big)\Big) \\ &\quad - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes Q_{\mathcal{C}_n \mathcal{Z}_n} \Big\|_1. \end{aligned} \tag{70}$$

Now, the probability distribution $(\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{E^n}})\,(\rho_{\mathrm{G}}[\gamma_{ABE}^{\otimes n}, 0])$ defines a triple of random variables X_n, Y_n, Z_n. Denoting with C_n the message exchanged during the execution of Λ_n^c and with S_n, S'_n the locally generated secret keys, the celebrated result of Maurer [[5], Theorem 1] that we have already used multiple times states that

$$H(S_n) \leqslant I(X_n : Y_n|Z_n) + H(S_n|S'_n) + I(S_n : C_n Z_n). \tag{71}$$

It is now an elementary exercise to verify that analogous conditions to (50)–(52) apply to our case. The only one, which needs a very slight modification is (52). Construct the triple of random variables $\widetilde{S}_n, \widetilde{C}_n, \widetilde{Z}_n$ such that $\widetilde{S}_n$ and $\widetilde{C}_n, \widetilde{Z}_n$ are independent; $\widetilde{S}_n$ is uniformly distributed over $\{1, \ldots, 2^{\lceil Rn \rceil}\}$; and $\widetilde{C}_n, \widetilde{Z}_n$ has probability distribution $Q_{\mathcal{C}_n \mathcal{Z}_n}$, where $\|\Lambda_n^c((\mathcal{M}^{\mathrm{G}}_{\Gamma_{A^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{B^n}} \otimes \mathcal{M}^{\mathrm{G}}_{\Gamma_{E^n}})(\rho_{\mathrm{G}}[\gamma_{ABE}^{\otimes n}, 0])) - (\kappa_{2^{\lceil Rn \rceil}})_{\mathcal{K}_n \mathcal{K}'_n} \otimes Q_{\mathcal{C}_n \mathcal{Z}_n}\|_1 \leqslant \epsilon_n$. Then,

$$\begin{aligned} I(S_n : C_n Z_n) &= H(S_n) - H(S_n|C_n Z_n) \\ &\leqslant H(\widetilde{S}_n) - H(S_n|C_n Z_n) \\ &= H(\widetilde{S}_n|\widetilde{C}_n \widetilde{Z}_n) - H(S_n|C_n Z_n) \\ &\leqslant \frac{\epsilon_n}{2} \log_2\left(2^{\lceil Rn \rceil} - 1\right) + h_2\Big(\frac{\epsilon_n}{2}\Big) \\ &\leqslant \frac{\epsilon_n}{2} \lceil Rn \rceil + h_2\Big(\frac{\epsilon_n}{2}\Big). \end{aligned} \tag{72}$$

Also, observe that

$$I(X_n : Y_n|Z_n) = I_M(A^n : B^n|E^n)_{\gamma_{ABE}^{\oplus n}+\Gamma_{A^n}\oplus\Gamma_{B^n}\oplus\Gamma_{E^n}} \tag{73}$$

by (31). Plugging (51), (73), (50), and (72) inside (71) yields

$$\begin{aligned}\lceil Rn\rceil &< 2\epsilon_n\lceil Rn\rceil + 2\,h_2\Big(\frac{\epsilon_n}{2}\Big) + h_2(\epsilon_n)\\ &\quad + I_M(A^n : B^n|E^n)_{\gamma_{ABE}^{\oplus n}+\Gamma_{A^n}\oplus\Gamma_{B^n}\oplus\Gamma_{E^n}}.\end{aligned} \tag{74}$$

Since this holds for all QCMs Γ_{E^n},

$$\begin{aligned}\lceil Rn\rceil &< 2\epsilon_n\lceil Rn\rceil + 2\,h_2\Big(\frac{\epsilon_n}{2}\Big) + h_2(\epsilon_n)\\ &\quad + \inf_{\Gamma_{E^n}} I_M(A^n : B^n|E^n)_{\gamma_{ABE}^{\oplus n}+\Gamma_{A^n}\oplus\Gamma_{B^n}\oplus\Gamma_{E^n}}.\end{aligned} \tag{75}$$

Taking a further supremum on Γ_{A^n}, Γ_{B^n} and remembering the definition of the Gaussian intrinsic entanglement (30) gives

$$\lceil Rn\rceil < 2\epsilon_n\lceil Rn\rceil + 2\,h_2\Big(\frac{\epsilon_n}{2}\Big) + h_2(\epsilon_n) + E_{\downarrow}^{\mathrm{G}}\big(\gamma_{ABE}^{\oplus n}\big). \tag{76}$$

Dividing by n and taking the liminf for $n\to\infty$ produces

$$R < E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}). \tag{77}$$

Since this holds for all achievable rates R, we also obtain that

$$K_{\leftrightarrow}^{\mathrm{G},\mathrm{M}}(V_{AB}) \leqslant E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}), \tag{78}$$

which proves the first inequality in (66).

We now move on to the proof of (67). To start off, we massage the expression (30) thanks to (33), obtaining

$$E_{\downarrow}^{\mathrm{G}}(V_{AB}) = \sup_{\Gamma_A,\Gamma_B}\inf_{\Gamma_E} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B}. \tag{79}$$

Before we proceed further, let us define one more quantity via a slight modification of (79). More precisely, we set

$$\widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB}) \coloneqq \inf_{\Gamma_E\text{ pure}}\sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B}. \tag{80}$$

Let us show that $E_{\downarrow}^{\mathrm{G}}(V_{AB}) \leqslant \widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB})$. We have that

$$\begin{aligned}E_{\downarrow}^{\mathrm{G}}(V_{AB}) &\overset{1}{\leqslant} \sup_{\Gamma_A,\Gamma_B}\inf_{\Gamma_E\text{ pure}} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B}\\ &\overset{2}{\leqslant} \inf_{\Gamma_E\text{ pure}}\sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B}\\ &= \widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB}).\end{aligned} \tag{81}$$

Here, in 1 we restricted the infimum in (79) to pure QCMs Γ_E, while in 2 we exchanged supremum and infimum according to the max-min inequality $\sup_{x\in\mathcal{X}}\inf_{y\in\mathcal{Y}} f(x,y) \leqslant \inf_{y\in\mathcal{Y}}\sup_{x\in\mathcal{X}} f(x,y)$ [115]. We now show that in fact $\widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB}) = E_{F,2}^{\mathrm{G}}(V_{AB})$ holds

$$\begin{aligned}\widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB}) &\overset{3}{=} \inf_{\Gamma_E\text{ pure}} I_M^c(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)}\\ &\overset{4}{=} \frac{1}{2}\inf_{\Gamma_E\text{ pure}} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)}\\ &\overset{5}{=} \frac{1}{2}\inf_{\Gamma_E\text{ pure}} I_M(A:B|E)_{\gamma_{ABE}+\Gamma_E}\\ &\overset{6}{=} E_{F,2}^{\mathrm{G}}(V_{AB}).\end{aligned} \tag{82}$$

In 3 we recalled the definition (22), in 4 we used (24), in 5 we exploited (33), and finally in 6 we leveraged a recently established result on the equality between Rényi-2 Gaussian squashed entanglement and Rényi-2 Gaussian entanglement of formation [[67], Theorem 5 and especially Remark 2].

We have therefore established (67). Applying it to the QCM $V_{AB}^{\oplus n}$ and taking the liminf for $n\to\infty$ yields

$$\begin{aligned}E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}) &= \liminf_{n\to\infty}\frac{1}{n}E_{\downarrow}^{\mathrm{G}}\big(V_{AB}^{\oplus n}\big)\\ &\leqslant \liminf_{n\to\infty}\frac{1}{n}E_{F,2}^{\mathrm{G}}\big(V_{AB}^{\oplus n}\big)\\ &= E_{F,2}^{\mathrm{G}}(V_{AB}),\end{aligned} \tag{83}$$

where the last identity is a consequence of the additivity (27) of the Rényi-2 Gaussian entanglement of formation. This establishes the second inequality in (66) and concludes the proof. ■

Note that the upper bound on $K_{\leftrightarrow}^{\mathrm{G},\mathrm{M}}$ provided by Lemma 3 would lead straight to the inequality $K_{\leftrightarrow}^{\mathrm{G},\mathrm{M}} \leqslant E_{F,2}^{\mathrm{G}}$. However, this is *a priori* less tight than the estimate $K_{\leftrightarrow}^{\mathrm{G},\mathrm{M}} \leqslant E_{\downarrow}^{\mathrm{G},\infty}$ established in Theorem 6. This discrepancy is due to the type of constraints we impose on Eve's action: in Lemma 3 we assumed that she performs a destructive Gaussian measurement at the very beginning of the protocol, subsequently broadcasting the obtained outcome to Alice and Bob; in Theorem 6, instead, we assumed that *first* Alice and Bob make their destructive Gaussian measurements, and *then* Eve makes hers, keeping the outcome secret.

V. EQUIVALENCE OF GAUSSIAN ENTANGLEMENT MEASURES

In the previous section we have seen that Theorem 6 brings into play, in addition to the Rényi-2 Gaussian entanglement of formation (25), also the (regularized) Gaussian intrinsic entanglement (30). As mentioned in the Introduction, these two measures have been conjectured to be identical on all Gaussian states [69–71], and in Theorem 6 we established that at least $E_{\downarrow}^{\mathrm{G}} \leqslant E_{F,2}^{\mathrm{G}}$ holds true in general. For a particular—but, in fact, quite vast—class of Gaussian states we are able to prove the opposite inequality as well, thus confirming the conjecture.

We call the QCM V_{AB} of a bipartite Gaussian state *normal* if it can be brought into a form in which all xp cross terms vanish (referred to as xp form) using local symplectic operations alone; see Appendix A 2 for an explicit definition. Here, the xp cross terms of an m-mode QCM W are all the entries W_{jk} with $|j-k| > m$, and a local symplectic operation is a map of the form $V_{AB} \mapsto (S_A \oplus S_B)V_{AB}(S_A^{\intercal} \oplus S_B^{\intercal})$, where S_A, S_B are symplectic matrices. All pure QCMs [87] as well as all two-mode mixed QCMs [116,117] are normal.

Our fourth main result then amounts to the following.

Theorem 7. For a normal QCM V_{AB}, it holds that

$$E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}) = E_{\downarrow}^{\mathrm{G}}(V_{AB}) = E_{F,2}^{\mathrm{G}}(V_{AB}). \tag{84}$$

In particular, (84) holds for all two-mode QCMs.

The proof of Theorem 7 makes use of additional facts and technical results presented in Appendixes A 4 and A 5.

Proof. In the proof of Theorem 6, and more precisely in (80), we introduced an auxiliary quantity $\widetilde{E}^{\mathrm{G}}_{\downarrow}$. In (81) and (82) we also showed that $E^{\mathrm{G}}_{\downarrow} \leqslant \widetilde{E}^{\mathrm{G}}_{\downarrow} = E^{\mathrm{G}}_{F,2}$ on all QCMs. We now prove that the opposite inequality $E^{\mathrm{G}}_{\downarrow}(V_{AB}) \geqslant \widetilde{E}^{\mathrm{G}}_{\downarrow}(V_{AB})$ holds as well, at least for normal QCMs V_{AB}.

Since V_{AB} is normal and both $E^{\mathrm{G}}_{\downarrow}$ and $\widetilde{E}^{\mathrm{G}}_{\downarrow}$ are invariant under local symplectics, we can assume directly that V_{AB} is in xp form, $V_{AB} = \left(\begin{smallmatrix} Q & 0 \\ 0 & P \end{smallmatrix}\right)$. Using Lemma 9 of Appendix A 2, we construct a symplectic matrix

$$S_{AB} = \begin{pmatrix} M^{-1} & 0 \\ 0 & M^{\intercal} \end{pmatrix}, \tag{85}$$

here written with respect to an xp block partition, such that

$$S_{AB} V_{AB} S_{AB}^{\intercal} = \Lambda_{AB} = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}, \tag{86}$$

again with respect to the same partition. This is useful because we can now construct very conveniently a purification γ_{ABE} of V_{AB},

$$\gamma_{ABE} = (S_{AB} \oplus \mathbb{1}_E)\, \gamma^{(0)}_{ABE}\, (S_{AB} \oplus \mathbb{1}_E)^{\intercal}. \tag{87}$$

Here, with respect to an $AB|E$ block partition we have that

$$\gamma^{(0)}_{ABE} = \begin{pmatrix} \Lambda & \sqrt{\Lambda^2 - \mathbb{1}}\, \Sigma \\ \sqrt{\Lambda^2 - \mathbb{1}}\, \Sigma & \Lambda \end{pmatrix}, \tag{88}$$

where $\Sigma \coloneqq (\Pi^x)^{\intercal} \Pi^x - (\Pi^p)^{\intercal} \Pi^p$. An important observation to make is that $\gamma^{(0)}_{ABE}$, S_{AB}, and hence also γ_{ABE} are all in xp form.

Let us now go back to the sought inequality $E^{\mathrm{G}}_{\downarrow}(V_{AB}) \geqslant \widetilde{E}^{\mathrm{G}}_{\downarrow}(V_{AB})$. Since the left-hand side is defined by a supremum over Gaussian measurements, parametrized by Γ_A, Γ_B, we estimate it as

$$\begin{aligned} E^{\mathrm{G}}_{\downarrow}(V_{AB}) &\overset{1}{=} \sup_{\Gamma_A, \Gamma_B} \inf_{\Gamma_E} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A \oplus \Gamma_B} \\ &\overset{2}{\geqslant} \lim_{t\to\infty} \inf_{\Gamma_E} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A(t) \oplus \Gamma_B(t)} \\ &\overset{3}{=} \inf_{\Gamma_E} I_M(A_x:B_x)_{((\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E))^x}. \end{aligned} \tag{89}$$

In the above derivation, the equality in 1 is simply (79), the inequality in 2 follows by choosing $\Gamma_A(t), \Gamma_B(t)$ as defined in (A13), and the inequality in 3, which is the real technical hurdle here, follows by combining Lemma 17 and Proposition 18 of Appendix A 5.

We now look at the set of matrices $((\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E))^x$, where Γ_E is an *arbitrary* QCM on E, not necessarily in xp form. With respect to an xp block partition, let us parametrize it as

$$\Gamma_E = \begin{pmatrix} K & J \\ J^{\intercal} & L \end{pmatrix}. \tag{90}$$

We now compute

$$\begin{aligned} &((\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E))^x \\ &\quad = \Pi^x \big((\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E)\big)(\Pi^x)^{\intercal} \\ &\quad \overset{4}{=} \Pi^x (S_{AB} \oplus \mathbb{1}_E)\big(\big(\gamma^{(0)}_{ABE} + \Gamma_E\big)\big/\big(\gamma^{(0)}_E + \Gamma_E\big)\big) \\ &\qquad \times (S_{AB} \oplus \mathbb{1}_E)^{\intercal} (\Pi^x)^{\intercal} \\ &\quad \overset{5}{=} M^{-1} \Pi^x \big(\big(\gamma^{(0)}_{ABE} + \Gamma_E\big)\big/\big(\gamma^{(0)}_E + \Gamma_E\big)\big)(\Pi^x)^{\intercal} M^{-\intercal} \\ &\quad \overset{6}{=} M^{-1} \Pi^x (\Lambda - \sqrt{\Lambda^2 - \mathbb{1}}\, \Sigma\, (\Lambda + \Gamma_E)^{-1} \Sigma \sqrt{\Lambda^2 - \mathbb{1}}) \\ &\qquad \times (\Pi^x)^{\intercal} M^{-\intercal} \\ &\quad \overset{7}{=} M^{-1} (D - \sqrt{D^2 - \mathbb{1}}\, \Pi^x\, (\Lambda + \Gamma_E)^{-1} (\Pi^x)^{\intercal} \\ &\qquad \times \sqrt{D^2 - \mathbb{1}}) M^{-\intercal} \\ &\quad \overset{8}{=} M^{-1} (D - \sqrt{D^2 - \mathbb{1}}(K + D - J(L + D)^{-1} J^{\intercal})^{-1} \\ &\qquad \times \sqrt{D^2 - \mathbb{1}}) M^{-\intercal}, \end{aligned}$$

where $M^{-\intercal} \coloneqq (M^{-1})^{\intercal}$. The justification of the above derivation is as follows. 4: We made use of (87) and of the covariance property (A20). 5: We applied (85). 6: We computed the Schur complement with the help of (88). 7: We used the fact that Λ and Σ are all in xp form. 8: We calculated

$$\begin{aligned} (\Lambda + \Gamma_E)^{-1} &= \begin{pmatrix} D + K & J \\ J^{\intercal} & D + L \end{pmatrix} \\ &= \begin{pmatrix} \big(K + D - J(L + D)^{-1} J^{\intercal}\big)^{-1} & * \\ * & * \end{pmatrix} \end{aligned}$$

thanks to the block inversion formulas (A18). Here, the symbols $*$ indicate unspecified matrices of appropriate size.

By the above calculation, the function on the right-hand side of (89) depends only on the combination $K - J(L + D)^{-1} J^{\intercal}$, which is a rather special function of the free variable Γ_E. Now, on the one hand

$$K - J(L + D)^{-1} J^{\intercal} = (\Gamma_E + 0 \oplus D)/(L + D) \geqslant \Gamma_E / L > 0,$$

where we applied the monotonicity of Schur complements (A22), and then observed that $\Gamma_E / L > 0$ follows from the block positivity conditions (A19), once one remembers that $\Gamma_E > 0$ as Γ_E is a QCM. On the other hand, every positive definite matrix $T > 0$ can be written as $T = K - J(L + D)^{-1} J^{\intercal}$ for some K, J, L forming—according to (90)—a *pure* QCM Γ_E in xp form. In fact, it suffices to set $K = T = L^{-1}$ and $J = 0$; this makes the corresponding Γ_E pure, as can be seen, e.g., by comparing it with (A11), and clearly in xp form. We have just proved that

$$\begin{aligned} &\{K - J(L + D)^{-1} J^{\intercal} : \Gamma_E \geqslant i\Omega_E\} = \{T : T > 0\} \\ &\quad = \{K - J(L + D)^{-1} J^{\intercal} : \Gamma_E \text{ pure QCM in } xp \text{ form}\}, \end{aligned} \tag{91}$$

which can be rephrased as

$$\begin{aligned} &\{((\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E))^x : \Gamma_E \geqslant i\Omega_E\} \\ &\quad = \{((\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E))^x : \Gamma_E \text{ pure QCM in } xp \text{ form}\}. \end{aligned} \tag{92}$$

We make use of this crucial fact to further massage the right-hand side of (89), obtaining that

$$\begin{aligned} E_{\downarrow}^{\mathrm{G}}(V_{AB}) &\geqslant \inf_{\Gamma_E} I_M(A_x : B_x)_{((\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E))^x} \\ &\overset{9}{=} \inf_{\substack{\Gamma_E \text{ pure} \\ \text{in } xp\text{-form}}} I_M(A_x : B_x)_{((\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E))^x} \\ &\overset{10}{=} \frac{1}{2} \inf_{\substack{\Gamma_E \text{ pure} \\ \text{in } xp\text{-form}}} I_M(A : B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)} \\ &\overset{11}{=} \inf_{\substack{\Gamma_E \text{ pure} \\ \text{in } xp\text{-form}}} \sup_{\Gamma_A,\Gamma_B} I_M(A : B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B} \\ &\overset{12}{\geqslant} \inf_{\Gamma_E \text{ pure}} \sup_{\Gamma_A,\Gamma_B} I_M(A : B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B} \\ &= \widetilde{E}_{\downarrow}^{\mathrm{G}}(V_{AB}). \end{aligned} \tag{93}$$

Here, in 9 we used (92); in 10 we observed that both γ_{ABE}, Γ_E, and hence also the pure QCM $(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)$, are in xp form, which allowed us to apply Corollary 14 of Appendix A 4; in 11 we recalled (24), and finally 12 follows elementarily from enlarging the set over which we compute the infimum. Combining the above inequality with (81) and (82) proves that $E_{\downarrow}^{\mathrm{G}}(V_{AB}) = E_{F,2}^{\mathrm{G}}(V_{AB})$ for all normal QCMs V_{AB}.

To complete the proof, it suffices to observe that the direct sum $V_{AB}^{\oplus n}$ of normal matrices V_{AB} is still normal. Hence,

$$\begin{aligned} E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}) &= \liminf_{n\to\infty} \frac{1}{n} E_{\downarrow}^{\mathrm{G}}\big(V_{AB}^{\oplus n}\big) \\ &= \liminf_{n\to\infty} \frac{1}{n} E_{F,2}^{\mathrm{G}}\big(V_{AB}^{\oplus n}\big) = E_{F,2}^{\mathrm{G}}(V_{AB}), \end{aligned}$$

where the last equality comes from (27). ∎

Theorem 7 establishes a powerful equivalence of two originally quite distinct Gaussian entanglement measures, for all two-mode Gaussian states and more generally all normal QCMs. The reader could wonder whether normal QCMs constitute a proper subset of all QCMs beyond the two-mode case. In Appendix B we show that this is indeed the case, by constructing an explicit example of a non-normal QCM over a $(1+2)$-mode system. The validity of the conjecture $E_{\downarrow}^{\mathrm{G},\infty}(V_{AB}) \overset{?}{=} E_{F,2}^{\mathrm{G}}(V_{AB})$ for non-normal QCMs V_{AB} remains open in general.

VI. APPLICATIONS AND EXAMPLES

A. Secret key from noisy two-mode squeezed states

We now apply our results, and in particular Theorem 4, to study secret key distillation from a class of Gaussian states of immediate physical interest. The states we will look at are obtained by sending one half of a two-mode squeezed vacuum $|\psi_s\rangle$ across a pure loss channel $\mathcal{E}_\lambda$ (also known as a quantum-limited attenuator). We recall that a two-mode squeezed vacuum is defined by

$$|\psi_s\rangle := \frac{1}{\cosh(r_s)} \sum_{n=0}^{\infty} \tanh^n r_s |nn\rangle, \tag{94}$$

where $|n\rangle$ denote local Fock states, and the squeeze parameter $r_s := \frac{s \ln 10}{20}$ is expressed as a function of the squeezing intensity s measured in dB. The pure loss channel $\mathcal{E}_\lambda$ is a Gaussian channel whose action at the level of density operators can be expressed as

$$\mathcal{E}_\lambda(\rho) := \mathrm{Tr}_2[\mathcal{U}_\lambda(\rho \otimes |0\rangle\langle 0|)\mathcal{U}_\lambda^\dagger], \tag{95}$$

where $\mathcal{U}_\lambda := e^{i \arccos\sqrt{\lambda}\,(x_1 p_2 - x_2 p_1)}$ is the Gaussian unitary that represents the action of a beam splitter with transmissivity λ, Tr_2 stands for the partial trace over the second mode, and as usual x_j, p_j denote the canonical operators pertaining to the jth mode.

The Rényi-2 Gaussian entanglement of formation of the state $(\mathcal{E}_\lambda \otimes I)(\psi_s)$ can be expressed in closed form by adapting the results for the standard (von Neumann) Gaussian entanglement of formation, which has been computed in [118]. We find

$$E_{F,2}^{\mathrm{G}}((\mathcal{E}_\lambda \otimes I)(\psi_s)) = \log_2 \left(\frac{1 + (1+\lambda)\sinh^2 r_s}{1 + (1-\lambda)\sinh^2 r_s} \right). \tag{96}$$

No expression for the corresponding 1-LOPC secret key $K_{\rightarrow}((\mathcal{E}_\lambda \otimes I)(\psi_s))$ seems to be known. However, in order to demonstrate the effectiveness of our estimate (40), it suffices to consider suitable lower bounds on this quantity. One such bound is the one-way distillable entanglement [108,119,120], denoted with $D_{\rightarrow}$. We succeeded in computing $D_{\rightarrow}((\mathcal{E}_\lambda \otimes I)(\psi_s))$ because the state in question is "degradable", and hence its one-way distillable entanglement equals the readily found coherent information [121]. The resulting expression is

$$\begin{aligned} K_{\rightarrow}((\mathcal{E}_\lambda \otimes I)(\psi_s)) &\geqslant D_{\rightarrow}((\mathcal{E}_\lambda \otimes I)(\psi_s)) \\ &= g(\sinh^2 r_s) - g((1-\lambda)\sinh^2 r_s), \end{aligned} \tag{97}$$

where $g(x) := (x+1)\log_2(x+1) - x\log_2(x)$ is the *bosonic entropy function*.

In Fig. 3 we compare the upper bound (96) for $K_{\rightarrow}^{\mathrm{G}}((\mathcal{E}_\lambda \otimes I)(\psi_s))$ deduced from Theorem 4 and the lower bound (97) for $K_{\rightarrow}((\mathcal{E}_\lambda \otimes I)(\psi_s))$. The plots show that the former quantity is smaller than the latter for all $\lambda \in (0,1]$ when $s \leqslant s_0 \approx 4.22\,\mathrm{dB}$, and only for sufficiently large $\lambda \geqslant \lambda_0(s)$ when $s > s_0$. For example, for the nowadays experimentally feasible [123,124] value of $s = 10\,\mathrm{dB}$, the useful range becomes $\lambda \geqslant \lambda_0(10\,\mathrm{dB}) \approx 0.912$.

This shows that, in several physically interesting regimes (either low squeezing or high transmissivity), our bounds accurately capture and quantify the severity of the Gaussian restriction for the task of distilling secrecy.

B. A conditional mutual information game

Finally, we interpret our results in a game-theoretical context. We begin by observing, as an interesting side result, that our proof of Theorem 7 implies the following variant of the strong saddle-point property of the log-determinant conditional mutual information.

Proposition 8 (Saddle-point property of log-determinant conditional mutual information). Let V_{AB} be a normal QCM with purification γ_{ABE}. Then

$$\begin{aligned} E_{F,2}^{\mathrm{G}}(V_{AB}) &= \inf_{\Gamma_E} \sup_{\Gamma_A,\Gamma_B} I_M(A : B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E} \\ &= \sup_{\Gamma_A,\Gamma_B} \inf_{\Gamma_E} I_M(A : B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E}. \end{aligned} \tag{98}$$

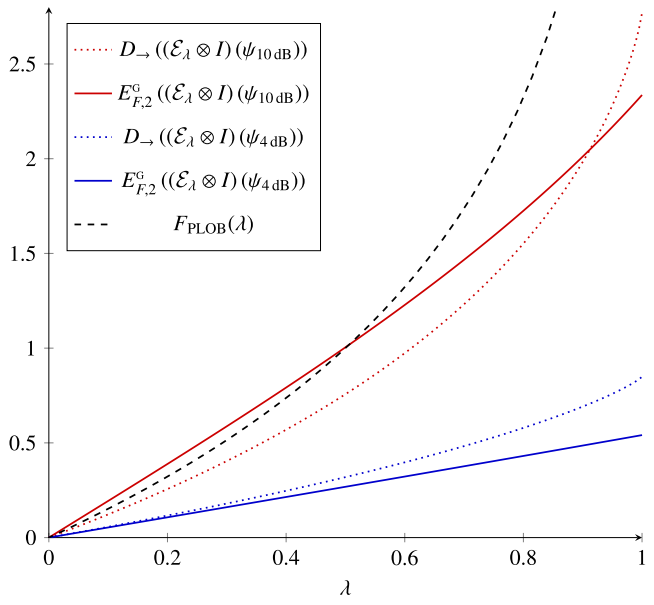

FIG. 3. A comparison between the one-way distillable entanglement (communication direction: first-to-second subsystem), which lower bounds the 1-LOPC secret key rate $K_{\rightarrow}$, and the Rényi-2 Gaussian entanglement of formation, which upper bounds the *Gaussian* 1-LOPC secret key rate. Both functions are computed for the states $(\mathcal{E}_\lambda \otimes I)(\psi_s)$. Explicit formulas are reported in (97) and (96), respectively. The comparison proves that the restriction to Gaussian operations reduces the distillable secret key appreciably for either low squeezing or high transmissivity. Our upper bound on the secret key rate can be and often is tighter than the one presented in [122], equal to $F_{\mathrm{PLOB}}(\lambda) \coloneqq -\log_2(1-\lambda)$ and plotted here as the black dashed line. This is because the bound in [122] applies to all (Gaussian and non-Gaussian) protocols with unbounded energy budget, while ours is tailored to Gaussian protocols and takes into account limitations to the available energy.

Proof. The topmost expression is obviously greater or equal to the bottommost one, owing to the max-min inequality $\sup_{x\in\mathcal{X}} \inf_{y\in\mathcal{Y}} f(x,y) \leqslant \inf_{y\in\mathcal{Y}} \sup_{x\in\mathcal{X}} f(x,y)$. For the opposite inequality, let us write

$$\begin{aligned}
\sup_{\Gamma_A,\Gamma_B} \inf_{\Gamma_E} I_M(A:B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E} &= E^{\mathrm{G}}_{\downarrow}(V_{AB}) \\
&\overset{1}{\geqslant} \widetilde{E}^{\mathrm{G}}_{\downarrow}(V_{AB}) \\
&= \inf_{\Gamma_E \text{ pure}} \sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B} \\
&\overset{2}{\geqslant} \inf_{\Gamma_E} \sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{(\gamma_{ABE}+\Gamma_E)/(\gamma_E+\Gamma_E)+\Gamma_A\oplus\Gamma_B}.
\end{aligned}$$

Here, 1 follows from (93), while 2 can be deduced by noting that infimum has been enlarged. The proof is then complete. ∎

Equalities of the form (98) represent a quintessence of application of methods of game theory in information theory. They appear in the context of a generic problem of finding optimal strategies for communication over a jamming channel. The task is linked to game theory by interpreting the communication as a two-player game between the sender-receiver pair on the one hand, and the malicious jammer on the other; here, the payoff function is some information measure, typically the mutual information [125–127]. The goal of the sender-receiver pair is to maximize the payoff function, whereas the goal of the jammer is to minimize it. If the payoff function exhibits a saddle-point property akin to (98) on the sets of allowed strategies of the players, then the saddle-point strategies are simultaneously optimal for both players. The game is then said to have a *value*, which is equal to the saddle-point value of the payoff function.

Viewed from a game-theoretical perspective, equation (98) then ensures the existence of a value of the following Gaussian quantum game with log-determinant conditional mutual information as the payoff function. At the beginning of the game, the players share a fixed pure Gaussian state with QCM

$$\gamma_{ABE} = \begin{pmatrix} V_{AB} & V_{ABE} \\ V_{ABE}^T & V_E \end{pmatrix}. \tag{99}$$

Clearly, we can see γ_{ABE} as a purification of the state with QCM V_{AB}. The participants holding subsystems A and B, called Alice and Bob in what follows, choose Gaussian measurements characterized by QCMs Γ_A and Γ_B to maximize the conditional mutual information $I_M(A:B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E}$, while the jammer Eve holding subsystem E chooses a Gaussian measurement with QCM Γ_E to minimize it. The equality (98) then guarantees that such a game has a value, and that this value is equal to $E^{\mathrm{G}}_{F,2}(V_{AB})$ by (30) and (84).

However, the game does not have the structure of a typical communication game with jamming. Namely, all participants appear symmetrically in the game and, in particular, it is not clearly seen, how the jammer disturbs the communication channel between the sender and the receiver. Nevertheless, we can transform the game into a teleportation game (different from the one presented in [128]) exhibiting all the features mentioned above. As a bonus, the obtained game reveals how the separability properties of the initial state across the $A:B$ partition and the measurement chosen by the jammer influence the effective state shared by Alice and Bob.

To find the latter game, we first rewrite equality (98) as

$$\inf_{\Gamma_E} \sup_{\Gamma_A,\Gamma_B} I_M(A:B)_{\sigma_{AB}+\Gamma_A\oplus\Gamma_B} = \sup_{\Gamma_A,\Gamma_B} \inf_{\Gamma_E} I_M(A:B)_{\sigma_{AB}+\Gamma_A\oplus\Gamma_B},$$

where

$$\sigma_{AB} = V_{AB} - V_{ABE}(V_E + R\Gamma_E R)^{-1} V_{ABE}^{\intercal}, \tag{100}$$

with $R = \mathrm{diag}(1,-1,1,-1,\ldots 1,-1)$ being the diagonal matrix representing on the QCM level the transposition operation $x_j \to x_j^{\intercal} = x_j$, $p_j \to p_j^{\intercal} = -p_j$. Here, we used property (33) of the conditional mutual information, together with the fact that $R\Gamma_E R$ is a physical QCM, which runs over the set of all QCMs as Γ_E is varied over the set of all QCMs.

Looking closely at the Schur complement σ_{AB}, Eq. (100), one further finds [58,59] that it can be viewed as an output of a Gaussian trace-decreasing completely-positive map characterized by the QCM (99) with the state with QCM Γ_E at the input. Here, E labels the input system and AB the output system. Since the map can be implemented deterministically [58] via the standard CV teleportation protocol [129], we arrive at the teleportation scheme in Fig. 4.

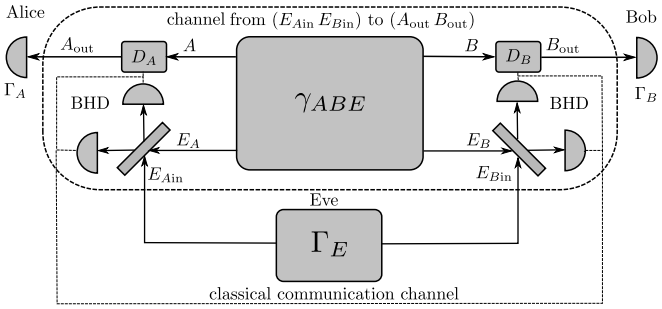

FIG. 4. Scheme of the teleportation game. The jammer Eve sends through a channel a bipartite Gaussian state of subsystem $E = E_{A\text{in}}E_{B\text{in}}$ with zero first moments and QCM Γ_E to subsystems A_{out} and B_{out} of spatially separated recipients Alice and Bob. The channel transforms QCM Γ_E as in Eq. (100) and it is realized by teleportation (dashed rectangular block) from Eve to Alice and Bob with the help of a shared fixed Gaussian state with QCM γ_{ABE}, Eq. (99). Here, the shortcut BHD stands for the balanced homodyne detection and D_A, D_B are displacements. Alice and Bob finally perform Gaussian measurements on their subsystems A_{out} and B_{out} characterized by QCMs Γ_A and Γ_B. The payoff function is the log-determinant conditional mutual information $I_M(A:B|E)_{\gamma_{ABE}+\Gamma_A\oplus\Gamma_B\oplus\Gamma_E}$ and Alice and Bob choose their measurement QCMs so as to maximize the payoff function, while Eve aims at minimizing it. Interestingly, such a game has a value and it is given by the Rényi-2 Gaussian entanglement of formation $E^{\text{G}}_{F,2}(V_{AB})$ of the reduced QCM V_{AB} of QCM γ_{ABE}, which belongs to subsystems A and B.

In view of the saddle-point property (98), the depicted teleportation game has a value, which is given exactly by the Rényi-2 Gaussian entanglement of formation $E^{\text{G}}_{F,2}(V_{AB})$. The optimal strategy for both players is to choose QCMs Γ_A, Γ_B and Γ_E, which achieve $E^{\text{G}}_{F,2}(V_{AB})$. This result makes $E^{\text{G}}_{F,2}(V_{AB})$ a unique instance of an entanglement measure equipped with such a game-theoretical interpretation.

VII. CONCLUSIONS

We studied the operational task of distilling a secret key from Gaussian states using local Gaussian operations, local classical processing, and public communication. When only one-way public communication is allowed, we determined the exact expression of the Gaussian secret key for all Gaussian pure states, and established upper bounds that hold for mixed multimode Gaussian states in all other cases. These bounds can be used to benchmark state-of-the-art CV QKD protocols against much simpler, Gaussian ones. Our findings imply that Gaussian secret key distillation, albeit often possible with positive yield, can be strictly less efficient than a general protocol would be. In the Gaussian-restricted scenario, our results often tighten the bounds obtained using the squashed entanglement [130] and the relative entropy of entanglement [122,131].

We also proved a recently proposed conjecture [69] on the equality between Gaussian intrinsic entanglement and Rényi-2 Gaussian entanglement of formation for all Gaussian states whose covariance matrix is "normal", and in particular for all two-mode Gaussian states. In conjunction with the already proven equality between the latter measure and a Gaussian version of the squashed entanglement [67], this establishes a coalescent and strongly operationally motivated highway to quantifying entanglement of Gaussian states. We further presented an alternative operational interpretation for this *treble* entanglement quantifier in a game-theoretical scenario. The unification presented in this paper stands in stark contrast with the recently uncovered fundamental nonuniqueness of general entanglement measures [132,133], and points to a much simpler picture in the special case of Gaussian entanglement.

The authors confirm that the data supporting the findings of this study are available within the article and its Appendixes.

ACKNOWLEDGMENTS

L.L. and L.M. contributed equally to this work. L.L. was supported by the Alexander von Humboldt Foundation. G.A. acknowledges support by the European Research Council (ERC) under the Starting Grant GQCOP (Grant No. 637352) and by the UK Research and Innovation (UKRI) under BBSRC Grant No. BB/X004317/1 and EPSRC Grant No. EP/X010929/1. L.M. acknowledges the project 8C22002 (CVStar) of MEYS of Czech Republic, which has received funding from the European Union's Horizon 2020 research and innovation framework program under Grant Agreement No. 731473 and No. 101017733. G.A. thanks S. Tserkis and M. Gideon for fruitful discussions.

APPENDIX A: ADDITIONAL NOTATION AND DEFINITIONS

1. Subgroups of the symplectic group

We start by fixing some notation. Recall that the symplectic form of an n-mode system takes the form

$$\Omega = \begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{pmatrix}, \tag{A1}$$

where all submatrices are $n \times n$. Let us also define

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{1} & \mathbb{1} \\ i\mathbb{1} & -i\mathbb{1} \end{pmatrix} \tag{A2}$$

as the unitary matrix that diagonalizes Ω, i.e., such that

$$H^\dagger \Omega H = \begin{pmatrix} i\mathbb{1} & 0 \\ 0 & -i\mathbb{1} \end{pmatrix}. \tag{A3}$$

The symplectic group $\mathbb{SP}(n)$ is formed by all those $2n \times 2n$ real matrices that preserve the symplectic form Ω,

$$\mathbb{SP}(n) := \{S : S\Omega S^\intercal = \Omega\}. \tag{A4}$$

The $2n \times 2n$ symplectic orthogonal matrices form a subgroup $\mathbb{K}(n) \subset \mathbb{SP}(n)$ that is isomorphic to the unitary group $\mathbb{U}(n)$. The isomorphism is given by [[134], §2.1.2]

$$\mathbb{U}(n) \ni U \longleftrightarrow K = H \begin{pmatrix} U & 0 \\ 0 & U^* \end{pmatrix} H^\dagger \in \mathbb{K}(n). \tag{A5}$$

Another important subgroup of the symplectic group is isomorphic to $\mathbb{GL}(n)$, the group of $n \times n$ invertible real matrices [[134], Example 2.5],

$$\mathbb{GL}(n) \simeq \left\{ \begin{pmatrix} M^{-1} & 0 \\ 0 & M^\intercal \end{pmatrix} : M \text{ invertible} \right\} \subset \mathbb{SP}(n). \tag{A6}$$

2. Normal covariance matrices

The phase space of an m-mode system is usually divided into its first m and last m components, called the x and p components, respectively. Let us denote by $\Pi^x : \mathbb{R}^{2m} \to \mathbb{R}^m$ and $\Pi^p : \mathbb{R}^{2m} \to \mathbb{R}^m$ the corresponding orthogonal projectors. Accordingly, we can write, e.g., $\Pi^x \Omega (\Pi^x)^\intercal = 0_n = \Pi^p \Omega (\Pi^p)^\intercal$, $\Pi^x \Omega (\Pi^p)^\intercal = \mathbb{1}_n = -\Pi^p \Omega (\Pi^x)^\intercal$. Observe that we think of Π^x as the $m \times 2m$ rectangular matrix $(\mathbb{1} \quad 0)$, and correspondingly of $(\Pi^x)^\intercal$ as the $2m \times m$ rectangular matrix $\binom{\mathbb{1}}{0}$. A matrix V expressed as

$$V = \begin{pmatrix} \Pi^x V (\Pi^x)^\intercal & \Pi^x V (\Pi^p)^\intercal \\ \Pi^p V (\Pi^x)^\intercal & \Pi^p V (\Pi^p)^\intercal \end{pmatrix} \tag{A7}$$

is said to be written with respect to the xp block partition. The representations in (A1) and (A2) are of this form.

This somehow pleonastic notation comes in handy when multiple systems are involved. In that case, we adopt the convention of indicating as subscripts the systems (A, B, and so on) and as superscripts the phase space components we want to project onto (x and p). For example, the projector onto the x component of the B system will be denoted by Π^x_B.

Particularly simple matrices are those that have no xp cross terms. We say that a matrix V is in *xp form* if

$$\Pi^x V (\Pi^p)^\intercal = 0. \tag{A8}$$

Observe that since V is symmetric, from the above identity it also follows that $\Pi^p V (\Pi^x)^\intercal = 0$. With respect to an xp block partition, a matrix in xp form then reads

$$V = \begin{pmatrix} Q & 0 \\ 0 & P \end{pmatrix}. \tag{A9}$$

When V is a QCM, it is not difficult to verify that the bona fide condition $V \geqslant i\Omega$ implies that $Q, P > 0$ and $Q \geqslant P^{-1}$. Williamson's theorem [135] states that all QCMs can be brought into a special kind of xp form via symplectic congruence: a QCM is in Williamson's form if it can be written as in (A9), with $Q = P = D$ diagonal. The diagonal entries of D, called symplectic eigenvalues of V, are uniquely determined by V up to the order and no smaller than 1 if V is a QCM. They can be characterized as the positive eigenvalues of the matrix $i\Omega V$. Moreover, $D = \mathbb{1}$ if and only if the QCM is pure. This also shows that a $2m \times 2m$ QCM V is pure if and only if

$$\mathrm{rk}(V + i\Omega) = m. \tag{A10}$$

Note that upon taking the complex conjugate we can also rephrase this condition as $\mathrm{rk}(V - i\Omega) = m$. For more details, see the discussion below [[67], Lemma 7].

It is important to realize that if a QCM is in xp form in the first place, it can be brought into Williamson's form by means of symplectics in the subgroup (A6), as we argue below. Note that the subgroup in (A6) is also composed of matrices in xp form!

Lemma 9. Let V be a QCM in xp form. Then there exists a symplectic matrix S in xp form [i.e., belonging to the subgroup (A6)] such that $SVS^\intercal$ is in Williamson's form.

Proof. Let V be as in (A9), and call m the number of modes. Using the spectral theorem, choose an orthogonal $m \times m$ matrix O with the property that $O^\intercal Q^{1/2} P Q^{1/2} O = D^2$ is diagonal. Set $M := Q^{1/2} O D^{-1/2}$. We have that

$$M^{-1} Q M^{-\intercal} = D^{1/2} O^\intercal Q^{-1/2}\, Q\, Q^{-1/2} O D^{1/2} = D,$$
$$M^\intercal P M = D^{-1/2} O^\intercal Q^{1/2}\, P\, Q^{1/2} O D^{-1/2} = D,$$

from which it follows that

$$\begin{pmatrix} M^{-1} & 0 \\ 0 & M^\intercal \end{pmatrix} \begin{pmatrix} Q & 0 \\ 0 & P \end{pmatrix} \begin{pmatrix} M^{-\intercal} & 0 \\ 0 & M \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$$

is in Williamson's form. ∎

For more background on Williamson's decomposition, we refer the reader to [134]. A particularly instructive case is that of pure QCMs: a pure QCM γ is in xp form if and only if

$$\gamma = \begin{pmatrix} Q & 0 \\ 0 & Q^{-1} \end{pmatrix} \tag{A11}$$

with respect to an xp block partition, with $Q > 0$. To see that this is the case, it suffices to remember that pure QCMs are symmetric symplectic matrices, and to use the relation that defines symplecticity. Observe that pure QCMs in xp form are exactly those symmetric matrices that belong to the subgroup (A6) of the symplectic group.

We can now give the following definition.

Definition 10. A bipartite QCM V_{AB} is called normal if it can be brought into xp form by local symplectic operations, i.e., if there are local symplectic matrices S_A, S_B such that

$$\Pi^x_{AB} (S_A \oplus S_B) V_{AB} \left(S_A^\intercal \oplus S_B^\intercal\right) \left(\Pi^p_{AB}\right)^\intercal = 0. \tag{A12}$$

The following is an easy consequence of results of [87].

Lemma 11 ([83]). All pure QCMs with arbitrary many modes on each side are normal.

The following result is due to Simon [116] and independently to Duan *et al.* [117].

Lemma 12 ([109,110]). All two-mode QCMs are normal.

For a real parameter $t > 0$, consider the QCMs on systems A and B defined by

$$\Gamma_A(t) := t \left(\Pi^x_A\right)^\intercal \Pi^x_A + t^{-1} \left(\Pi^p_A\right)^\intercal \Pi^p_A = \begin{pmatrix} t\mathbb{1}^x_A & 0 \\ 0 & t^{-1}\mathbb{1}^p_A \end{pmatrix},$$
$$\Gamma_B(t) := t \left(\Pi^x_B\right)^\intercal \Pi^x_B + t^{-1} \left(\Pi^p_B\right)^\intercal \Pi^p_B = \begin{pmatrix} t\mathbb{1}^x_B & 0 \\ 0 & t^{-1}\mathbb{1}^p_B \end{pmatrix}, \tag{A13}$$

where the block matrices on the right-hand side are written with respect to an xp block partition. In the limit $t \to 0^+$, these QCMs are the seeds of two measurements of the x quadrature, while in the opposite limit $t \to \infty$ they identify measurements of the p quadrature. Occasionally, if there is no ambiguity on the partition used, we will remove superscripts and subscripts from expressions like (A13).

3. Properties of Schur complements

Here we discuss some applications of the notion of Schur complement. We have seen in the main text that for a 2×2

block matrix

$$R = \begin{pmatrix} X & Z \\ Z^\intercal & Y \end{pmatrix} \tag{A14}$$

one sets

$$R/X \coloneqq Y - Z^\intercal X^{-1} Z, \tag{A15}$$

provided that X is invertible. The expression in (A15) is called the Schur complement of R with respect to X. Schur complements are instrumental in matrix analysis [136], and have found widespread applications in the context of CV quantum information as well [66,67]. Here we limit ourselves to recalling a few notable properties of these objects, referring the interested reader to [136].

(i) Schur determinant factorization formula,

$$\det R = (\det X)(\det(R/X)). \tag{A16}$$

(ii) Inertia additivity formula,

$$\mathrm{rk} R = \mathrm{rk} X + \mathrm{rk}(R/X). \tag{A17}$$

(iii) Block inverse,

$$R^{-1} = \begin{pmatrix} (R/Y)^{-1} & -X^{-1}Y(R/X)^{-1} \\ -(R/X)^{-1}Y^T X^{-1} & (R/X)^{-1} \end{pmatrix}, \tag{A18}$$

provided that R as well as X are invertible.

(iv) Block positivity conditions,

$$R > 0 \iff X > 0 \quad \text{and} \quad R/X > 0. \tag{A19}$$

(v) Covariance under congruences: for all invertible M, N, it holds that

$$((M \oplus N) R (M \oplus N)^\intercal)/(MXM^\intercal) = N(R/X)N^\intercal. \tag{A20}$$

(vi) Variational representation: when $R > 0$ is positive definite, it holds that

$$R/X = \max\{T : R \geqslant 0 \oplus T\}. \tag{A21}$$

Note that the set on the right-hand side is a matrix set, hence it is not *a priori* guaranteed to have a maximum. What (A21) tells us is that such a maximum, however, does exist, and that it coincides with the Schur complement of R with respect to X. From (A21) it is straightforward to deduce the following monotonicity property: if $R > 0$ and $R' = \left(\begin{smallmatrix} X' & Z' \\ (Z')^\intercal & Y' \end{smallmatrix}\right) > 0$, then

$$R \geqslant R' \implies R/X \geqslant R'/X'. \tag{A22}$$

4. Properties of the log-determinant mutual information

Here we summarize known properties of the log-determinant mutual information (23) and establish some new ones—such as a type of uniform continuity—that will play an important role in the proof of Theorem 7. A list of basic properties is as follows.

(1) Invariance under local symplectics: for all pairs of symplectic matrices S_A, S_B, it holds that

$$I_M(A:B)_{(S_A \oplus S_B) V_{AB} (S_A^\intercal \oplus S_B^\intercal)} \equiv I_M(A:B)_{V_{AB}}. \tag{A23}$$

(2) Invariance under rescaling: whenever $t > 0$, we have that

$$I_M(A:B)_V \equiv I_M(A:B)_{tV}. \tag{A24}$$

(3) Data processing inequality: for every positive semidefinite matrix $K_A \geqslant 0$ on system A, it holds that

$$I_M(A:B)_{V_{AB}+K_A} \leqslant I_M(A:B)_{V_{AB}}, \tag{A25}$$

where K_A is a shorthand for $K_A \oplus 0_B$. This is clear if one thinks of $I_M(A:B)_V$ as the Shannon mutual information of a Gaussian random variable with covariance matrix V. Adding a local positive semidefinite matrix corresponds to adding an independent and normal local random variable.

(4) For every pure QCM γ_{AB}, it holds that

$$I_M(A:B)_\gamma = 2M(\gamma_A) = 2M(\gamma_B). \tag{A26}$$

This follows trivially from the fact that the local reduced states corresponding to the pure Gaussian state with QCM γ_{AB} have the same Rényi-2 entropies, and moreover $M(\gamma_{AB}) = 0$ as $\det \gamma_{AB} = 1$.

(5) For all positive matrices $V > 0$, it holds that [[67], Eq. (29)]

$$I_M(A:B)_V = I_M(A:B)_{V^{-1}}. \tag{A27}$$

We now explore some further properties of the log-determinant mutual information (23). Consider a bipartite QCM V_{AB}, and define

$$V_{AB}^x \coloneqq \Pi_{AB}^x V_{AB} \left(\Pi_{AB}^x\right)^\intercal, \tag{A28}$$

$$V_{AB}^p \coloneqq \Pi_{AB}^p V_{AB} \left(\Pi_{AB}^p\right)^\intercal. \tag{A29}$$

Since V_{AB}^x and V_{AB}^p are principal submatrices of V_{AB}, we can take Schur complements with respect to them. Also, since they still retain formally a block form with respect to the partition $A:B$, we can also compute their log-determinant mutual information, which we denote for instance by $I_M(A_x:B_x)_{V_{AB}^x}$. With this notation in mind, we start by showing the following.

Lemma 13. For all bipartite QCMs V_{AB}, the log-determinant mutual information admits the decomposition

$$I_M(A:B)_{V_{AB}} = I_M(A_x:B_x)_{V_{AB}^x} + I_M(A_p:B_p)_{V_{AB}/V_{AB}^x}. \tag{A30}$$

Proof. It suffices to apply repeatedly the Schur determinant factorization formula (A16)

$$\begin{aligned} &I_M(A:B)_{V_{AB}} \\ &\quad = \frac{1}{2}\log_2 \frac{(\det V_A)(\det V_B)}{\det V_{AB}} \\ &\quad = \frac{1}{2}\log_2 \frac{\left(\det V_A^x\right)\left(\det V_A/V_A^x\right)\left(\det V_B^x\right)\left(\det V_B/V_B^x\right)}{\left(\det V_{AB}^x\right)\left(\det V_{AB}/V_{AB}^x\right)} \\ &\quad = \frac{1}{2}\log_2 \frac{\left(\det V_A^x\right)\left(\det V_B^x\right)}{\left(\det V_{AB}^x\right)} \\ &\qquad + \frac{1}{2}\log_2 \frac{\left(\det V_A/V_A^x\right)\left(\det V_B/V_B^x\right)}{\left(\det V_{AB}/V_{AB}^x\right)} \\ &\quad = I_M(A_x:B_x)_{V_{AB}^x} + I_M(A_p:B_p)_{V_{AB}/V_{AB}^x}. \end{aligned}$$

This concludes the proof. ∎

Corollary 14. Let γ_{AB} be a pure QCM in xp form, i.e., let it be as in (A11). Then

$$I_M(A_x : B_x)_{\gamma^x_{AB}} = I_M(A_p : B_p)_{\gamma^p_{AB}} = \tfrac{1}{2} I_M(A : B)_{\gamma_{AB}} = M(\gamma_A). \tag{A31}$$

Proof. Remembering (A11) and (A27), we see that

$$I_M(A_x : B_x)_{\gamma^x_{AB}} = I_M(A_p : B_p)_{(\gamma^p_{AB})^{-1}} = I_M(A_p : B_p)_{\gamma^p_{AB}}.$$

Also, since γ_{AB} has no off-diagonal terms, it holds that $\gamma_{AB}/\gamma^x_{AB} = \gamma^p_{AB}$. Combining this with (A30) and (A26) yields

$$\begin{aligned} 2M(\gamma_A) &= I_M(A : B)_{\gamma_{AB}} = I_M(A_x : B_x)_{\gamma^x_{AB}} + I_M(A_p : B_p)_{\gamma^p_{AB}} \\ &= 2 I_M(A_x : B_x)_{\gamma^x_{AB}}, \end{aligned}$$

completing the proof. ∎

Lemma 15 (Uniform continuity of log-determinant mutual information). Let $\kappa \geqslant 1$, and consider two matrices V_{AB}, W_{AB} such that $V_{AB}, W_{AB} \geqslant \kappa^{-1} \mathbb{1}_{AB}$. Then it holds that

$$|I_M(A : B)_V - I_M(A : B)_W| \leqslant \kappa \log_2(e) \, \|V_{AB} - W_{AB}\|_1, \tag{A32}$$

where $\|\cdot\|_1$ denotes the trace norm.

Proof. Let us start by proving that for any two matrices $M, N \geqslant \kappa^{-1} \mathbb{1}$, it holds that

$$|\log_2 \det(MN^{-1})| \leqslant \kappa \log_2(e) \, \|M - N\|_1. \tag{A33}$$

To see this, we write

$$\begin{aligned} |\log_2 \det(MN^{-1})| &= |\log_2 \det(M) - \log_2 \det(N)| \\ &\overset{1}{=} \left| \sum_i (\log_2 \mu_i - \log_2 \nu_i) \right| \\ &\leqslant \sum_i |\log_2 \mu_i - \log_2 \nu_i| \\ &\overset{2}{\leqslant} \kappa \log_2(e) \sum_i |\mu_i - \nu_i| \\ &\overset{3}{\leqslant} \kappa \log_2(e) \, \|M - N\|_1. \end{aligned}$$

Here, in 1 we called μ_i, ν_i the eigenvalues of M, N, sorted in descending order. To justify 2, instead, start by applying Lagrange's theorem to a continuously differentiable function $f : [a, b] \to \mathbb{R}$,

$$\frac{|f(\mu) - f(\nu)|}{|\mu - \nu|} \leqslant \max_{a \leqslant \xi \leqslant b} |f'(\xi)|.$$

Setting $f(x) = \log_2 x$, $a = \kappa^{-1}$, and $b = \infty$, we obtain the desired inequality $|\log_2 \mu_i - \log_2 \nu_i| \leqslant \kappa \log_2(e) \, |\mu_i - \nu_i|$. Finally, in 3 we used the well-known estimate $\|M - N\|_1 \geqslant \sum_i |\mu_i - \nu_i|$, which is due to Mirsky [[137], Theorem 5] {see also [[138], Eq. (IV.62)]}.

We now come to the proof of (A32),

$$\begin{aligned} &|I_M(A : B)_V - I_M(A : B)_W| \\ &= \left| \frac{1}{2} \log_2 \frac{\det(V_A) \det(V_B)}{\det(V_{AB})} - \frac{1}{2} \log_2 \frac{\det(W_A) \det(W_B)}{\det(W_{AB})} \right| \\ &= \left| \frac{1}{2} \log_2 \det\left(V_A W_A^{-1}\right) + \frac{1}{2} \log_2 \det\left(V_B W_B^{-1}\right) \right. \\ &\quad \left. - \frac{1}{2} \log_2 \det\left(V_{AB} W_{AB}^{-1}\right) \right| \\ &\overset{3}{\leqslant} \frac{\kappa \log_2(e)}{2} (\|V_A - W_A\|_1 + \|V_B - W_B\|_1 + \|V_{AB} - W_{AB}\|_1) \\ &\overset{4}{\leqslant} \kappa \log_2(e) \, \|V_{AB} - W_{AB}\|_1. \end{aligned}$$

Here, 3 comes from inequality (A33) applied to $M = V_A, V_B, V_{AB}$ and $N = W_A, W_B, W_{AB}$, respectively. Note that under the operation of taking principal submatrices the minimal eigenvalue never decreases, hence $V_A, W_A \geqslant \kappa^{-1} \mathbb{1}_A$ and $V_B, W_B \geqslant \kappa^{-1} \mathbb{1}_B$. Finally, 4 descends from the observation that since the "pinching" operation that maps $V_{AB} \mapsto V_A \oplus V_B$ and $W_{AB} \mapsto W_A \oplus W_B$ is a quantum channel, it never increases the trace norm, and hence

$$\begin{aligned} \|V_{AB} - W_{AB}\|_1 &\geqslant \|V_A \oplus V_B - W_A \oplus W_B\|_1 \\ &= \|V_A - W_A\|_1 + \|V_B - W_B\|_1. \end{aligned}$$

This concludes the proof. ∎

For the sake of completeness, here we further present a simple justification of the known fact [70,86,87] that in the Gaussian setting the classical mutual information of Gaussian pure states coincides with the local Rényi-2 entropy, as claimed in (24).

Lemma 16. For all pure QCMs γ_{AB}, it holds that $I^c_M(A : B)_\gamma = \frac{1}{2} I_M(A : B)_\gamma = M(\gamma_A)$. Moreover, if γ_{AB} is in xp form, the optimal Gaussian measurements in (22) are identical homodynes.

Proof. Start by employing (A25) to deduce that

$$I_M(A : B)_{\gamma_{AB} + \Gamma_A \oplus \Gamma_B} \leqslant I_M(A : B)_{\gamma_{AB} + \Gamma_B},$$

for all $\Gamma_A \geqslant 0$. Using the determinant factorization formula (A16), it is not difficult to show that

$$\begin{aligned} I_M(A : B)_{\gamma_{AB} + \Gamma_B} &= M(\gamma_A) - M((\gamma_{AB} + \Gamma_B)/(\gamma_B + \Gamma_B)) \\ &\leqslant M(\gamma_A), \end{aligned}$$

where the last inequality follows because $(\gamma_{AB} + \Gamma_B)/(\gamma_B + \Gamma_B)$ is a QCM by (16), and hence the corresponding log-determinant entropy must be non-negative. Consequently, one obtains that $I_M(A : B)_{\gamma_{AB} + \Gamma_A \oplus \Gamma_B} \leqslant M(\gamma_A)$. Since Γ_A, Γ_B were arbitrary, we conclude that

$$I^c_M(A : B)_\gamma \leqslant M(\gamma_A), \tag{A34}$$

To prove the converse inequality, we can use the normality of pure QCMs (Lemma 11) to find local symplectics S_A, S_B such that

$$\gamma_{AB} = (S_A \oplus S_B) \, \gamma^{(0)}_{AB} \, (S_A \oplus S_B)^\intercal, \tag{A35}$$

where $\gamma^{(0)}_{AB}$ is in xp form. Observe that because of (A11) we have that $\gamma^{(0)}_{AB} = \left(\begin{smallmatrix} Q & 0 \\ 0 & Q^{-1} \end{smallmatrix}\right)$ with respect to an xp block partition, where $Q > 0$. Obviously, if γ is in xp form we can set $S_A = \mathbb{1}_A$ and $S_B = \mathbb{1}_B$ in the first place. Now, construct

$$\begin{aligned} \widetilde{\Gamma}_A(t) &= S_A \Gamma_A(t) S_A^\intercal, \\ \widetilde{\Gamma}_B(t) &= S_B \Gamma_B(t) S_B^\intercal, \end{aligned}$$

where $\Gamma_A(t)$, $\Gamma_B(t)$ are the seeds of a homodyne as given by (A13). With respect to an xp block partition, one has that

$$\gamma_{AB}^{(0)} = \begin{pmatrix} Q + t\mathbb{1} & 0 \\ 0 & Q^{-1} + t^{-1}\mathbb{1} \end{pmatrix},$$

and hence that

$$\begin{aligned}
&\lim_{t\to 0} I_M(A:B)_{\gamma_{AB}+\widetilde{\Gamma}_A(t)\oplus\widetilde{\Gamma}_B(t)} \\
&\quad \overset{1}{=} \lim_{t\to 0} I_M(A:B)_{\gamma_{AB}^{(0)}+\Gamma_A(t)\oplus\Gamma_B(t)} \\
&\quad \overset{2}{=} \lim_{t\to 0} (I_M(A_x:B_x)_{Q+t\mathbb{1}} + I_M(A_p:B_p)_{Q^{-1}+t^{-1}\mathbb{1}}) \\
&\quad \overset{3}{=} \lim_{t\to 0} (I_M(A_x:B_x)_{Q+t\mathbb{1}} + I_M(A_p:B_p)_{\mathbb{1}+tQ^{-1}}) \\
&\quad \overset{4}{=} I_M(A_x:B_x)_Q \\
&\quad \overset{5}{=} M\big(\gamma_A^{(0)}\big) \\
&\quad = M(\gamma_A).
\end{aligned}$$

The above identities can be justified as follows: 1 descends from (A23); 2 is an application of (A30); 3 uses the identity (A24); 4 comes from Lemma 15, which implies that

$$\begin{aligned}
I_M(A_p:B_p)_{\mathbb{1}+tQ^{-1}} &= |I_M(A_p:B_p)_{\mathbb{1}+tQ^{-1}} - I_M(A:B)_{\mathbb{1}}| \\
&\leqslant t\log_2(e)\,\|Q^{-1}\|_1 \underset{t\to 0}{\longrightarrow} 0
\end{aligned}$$

and that

$$\begin{aligned}
&|I_M(A_p:B_p)_{Q+t\mathbb{1}} - I_M(A_p:B_p)_Q| \\
&\quad \leqslant t\log_2(e)\,\|\mathbb{1}_p\|_1\|Q^{-1}\|_1 \underset{t\to 0}{\longrightarrow} 0;
\end{aligned}$$

finally, 5 is a consequence of Corollary 14. ∎

5. A few more technical lemmata

Here we need to establish a couple of technical lemmata, which will be useful for the proof of Theorem 7.

Lemma 17. Let V_{AB} be any bipartite QCM, and let γ_{ABE} be any extension of it, i.e., let it satisfy $\gamma_{AB} = V_{AB}$. For some QCM Γ_E, define

$$W_{AB} \coloneqq (\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E). \tag{A36}$$

Then

$$\lambda_{\max}(V_{AB})^{-1}\mathbb{1}_{AB} \leqslant \Omega_{AB}^{\intercal} V_{AB}^{-1}\Omega_{AB} \leqslant W_{AB} \leqslant V_{AB}, \tag{A37}$$

where $\lambda_{\max}(V_{AB})$ denotes the maximal eigenvalue of V_{AB}.

Proof. The very definition of Schur complement implies that $W_{AB} \leqslant \gamma_{AB} = V_{AB}$. As for the opposite inequality, since $\Gamma_E \geqslant 0$ is positive semidefinite and the Schur complement is monotonic (A22), one has that $(\gamma_{ABE} + \Gamma_E)/(\gamma_E + \Gamma_E) \geqslant \gamma_{ABE}/\gamma_E \geqslant \Omega_{AB}^{\intercal}\gamma_{AB}^{-1}\Omega_{AB} = \Omega_{AB}^{\intercal}V_{AB}^{-1}\Omega_{AB}$, where the second inequality is an application of [[66], Theorem 3]. ∎

Proposition 18. Let $\Gamma_A(t)$ and $\Gamma_B(t)$ be the seeds of homodyne measurements defined by (A13). For some $0 < \kappa \leqslant 1$, let $\mathcal{W}_{AB} \geqslant \kappa^{-1}\mathbb{1}_{AB}$ be a compact set of bipartite QCMs that is bounded away from zero [139]. Then

$$\begin{aligned}
&\lim_{t\to 0^+} \inf_{W_{AB}\in\mathcal{W}_{AB}} I_M(A:B)_{W_{AB}+\Gamma_A(t)\oplus\Gamma_B(t)} \\
&\qquad = \inf_{W_{AB}\in\mathcal{W}_{AB}} I_M(A_x:B_x)_{W_{AB}^x},
\end{aligned} \tag{A38}$$

where W_{AB}^x is defined analogously to (A28).

Proof. Let us define the functions $F_t : \mathcal{W}_{AB} \to \mathbb{R}$ and $F : \mathcal{W}_{AB} \to \mathbb{R}$ via

$$F_t(W_{AB}) \coloneqq I_M(A:B)_{W_{AB}+\Gamma_A(t)\oplus\Gamma_B(t)}, \tag{A39}$$

$$F(W_{AB}) \coloneqq I_M(A_x:B_x)_{W_{AB}^x}. \tag{A40}$$

Then (A38) becomes

$$\lim_{t\to 0^+} \inf_{W_{AB}\in\mathcal{W}_{AB}} F_t(W_{AB}) = \inf_{W_{AB}\in\mathcal{W}_{AB}} F(W_{AB}). \tag{A41}$$

To prove (A41), it suffices to show that $F_t \underset{t\to 0^+}{\overset{\mathrm{u}}{\longrightarrow}} F$ *uniformly*, i.e., that

$$\lim_{t\to 0^+} \|F_t - F\|_\infty = 0, \tag{A42}$$

where

$$\begin{aligned}
\|F_t - F\|_\infty &\coloneqq \sup_{W_{AB}\in\mathcal{W}_{AB}} |F_t(W_{AB}) - F(W_{AB})| \qquad \text{(A43)} \\
&= \sup_{W_{AB}\in\mathcal{W}_{AB}} \big|I_M(A:B)_{W_{AB}+\Gamma_A(t)\oplus\Gamma_B(t)} \\
&\qquad - I_M(A_x:B_x)_{W^x}\big|. \qquad \text{(A44)}
\end{aligned}$$

The fact that (A42) implies (A41) is well known, see for instance [[140], Chapter 7]. We thus proceed to prove (A42). Note that we are not in the position to apply Lemma 15 on the continuity of mutual information, for example because the QCMs $W_{AB} + \Gamma_A(t) \oplus \Gamma_B(t)$ do not converge to anything as $t \to 0^+$, due to the presence of the diverging term t^{-1} in (A13). To proceed further, let us write down an explicit decomposition of an arbitrary matrix $W_{AB} \in \mathcal{W}_{AB}$ with respect to an xp block partition as

$$W_{AB} = \begin{pmatrix} W_{AB}^x & Z_{AB} \\ Z_{AB}^{\intercal} & W_{AB}^p \end{pmatrix}. \tag{A45}$$

Observe that according to the same splitting one has that

$$\Gamma_A(t) \oplus \Gamma_B(t) = \begin{pmatrix} t\,\mathbb{1}_{AB}^x & 0 \\ 0 & t^{-1}\mathbb{1}_{AB}^p \end{pmatrix}. \tag{A46}$$

We now massage (A39) as follows:

$$\begin{aligned}
F_t(W_{AB}) &= I_M(A:B)_{W_{AB}+\Gamma_A(t)\oplus\Gamma_B(t)} \\
&\overset{1}{=} I_M(A_x:B_x)_{W_{AB}^x+\Gamma_A^x(t)\oplus\Gamma_B^x(t)} + I_M(A_p:B_p)_{(W_{AB}+\Gamma_A(t)\oplus\Gamma_B(t))/(W_{AB}^x+\Gamma_A^x(t)\oplus\Gamma_B^x(t))} \\
&\overset{2}{=} I_M(A_x:B_x)_{W_{AB}^x+t\,\mathbb{1}_{AB}^x} + I_M(A_p:B_p)_{W_{AB}^p+t^{-1}\mathbb{1}_{AB}^p - Z_{AB}^{\intercal}(W_{AB}^x+t\,\mathbb{1}_{AB}^x)^{-1}Z_{AB}} \\
&\overset{3}{=} I_M(A_x:B_x)_{W_{AB}^x+t\,\mathbb{1}_{AB}^x} + I_M(A_p:B_p)_{\mathbb{1}_{AB}^p+t(W_{AB}^p - Z_{AB}^{\intercal}(W_{AB}^x+t\,\mathbb{1}_{AB}^x)^{-1}Z_{AB})}.
\end{aligned}$$

Note that in 1 we applied Lemma 13, in 2 we made use of (A45) and (A46), and in 3 we employed (A24). Now, we see that

$$\begin{aligned}|F_t(W_{AB}) - F(W_{AB})| &\overset{4}{\leqslant} \left|I_M(A_x : B_x)_{W^x_{AB}+t\,\mathbb{1}^x_{AB}} - I_M(A_x : B_x)_{W^x_{AB}}\right| + \left|I_M(A_p : B_p)_{\mathbb{1}^p_{AB}+t(W^p_{AB}-Z^{\intercal}_{AB}(W^x_{AB}+t\,\mathbb{1}^x_{AB})^{-1}Z_{AB})} - I_M(A_p : B_p)_{\mathbb{1}^p_{AB}}\right| \\ &\overset{5}{\leqslant} \kappa\log_2(e)\left\|W^x_{AB}+t\,\mathbb{1}^x_{AB} - W^x_{AB}\right\|_1 + \log_2(e)\left\|\mathbb{1}^p_{AB}+t\left(W^p_{AB}-Z^{\intercal}_{AB}(W^x_{AB}+t\,\mathbb{1}^x_{AB})^{-1}Z_{AB}\right)-\mathbb{1}^p_{AB}\right\|_1 \\ &\overset{6}{=} t\log_2(e)\left(\kappa(m_A+m_B) + \max_{W_{AB}\in\mathcal{W}_{AB}}\mathrm{Tr}\left[W^p_{AB}\right]\right).\end{aligned}$$

Note that the inequality in 4 comes directly from the definitions (A39) and (A40), together with the observation that $I_M(A_p : B_p)_{\mathbb{1}^p_{AB}} = 0$. For 5, instead, we applied Lemma 15 twice, which is possible because (i) $W_{AB} \geqslant \kappa^{-1}\mathbb{1}_{AB}$ and hence $W^x_{AB} \geqslant \kappa^{-1}\mathbb{1}^x_{AB}$ (also, $t > 0$); and (ii) from the block positivity conditions (A19) for $W_{AB} + t\,\mathbb{1}_{AB}$ it follows that $W^p_{AB} - Z^{\intercal}_{AB}(W^x_{AB} + t\,\mathbb{1}^x_{AB})^{-1}Z_{AB} = (W_{AB} + t\,\mathbb{1}^x_{AB})/(W^x_{AB} + t\,\mathbb{1}^x_{AB}) > 0$. To justify 6, note that exploiting again positivity one has that $\|(W_{AB} + t\,\mathbb{1}^x_{AB})/(W^x_{AB} + t\,\mathbb{1}^x_{AB})\|_1 = \mathrm{Tr}[(W_{AB} + t\,\mathbb{1}^x_{AB})/(W^x_{AB} + t\,\mathbb{1}^x_{AB})] \leqslant \mathrm{Tr}[W^p_{AB}]$. The quantity $\max_{W_{AB}\in\mathcal{W}_{AB}}\mathrm{Tr}[W^p_{AB}]$ is finite thanks to the compactness of $\mathcal{W}_{AB}$. Also, we denoted by m_A and m_B the number of modes on systems A and B, respectively. From the above estimate it is clear that $\lim_{t\to 0^+}\sup_{W_{AB}\in\mathcal{W}_{AB}}|F_t(W_{AB}) - F(W_{AB})| = 0$, completing the argument. ■

APPENDIX B: A NON-NORMAL QUANTUM COVARIANCE MATRIX

Here we construct an explicit example of a non-normal QCM over a $(1 + 2)$-mode system. Let us start by recalling a well-known result in symplectic geometry.

Lemma 19 ([127, Proposition 8.12]). Let $A > 0$ be a $2n \times 2n$ positive definite matrix. Let S_1, S_2 be two symplectic matrices that bring A into Williamson's form, i.e., let them satisfy

$$A = S_1\begin{pmatrix} D & 0 \\ 0 & D\end{pmatrix}S_1^{\intercal} = S_2\begin{pmatrix} D & 0 \\ 0 & D\end{pmatrix}S_2^{\intercal}, \tag{B1}$$

where $D = \sum_{j=1}^n d_j|j\rangle\langle j| > 0$ is diagonal. Then

$$S_2 = S_1K, \quad K = H\begin{pmatrix} U & 0 \\ 0 & U^*\end{pmatrix}H^{\dagger} \in \mathbb{K}(n), \quad [U, D] = 0. \tag{B2}$$

The last condition means that U only mixes vectors $|j\rangle$ with the same coefficients d_j. If these are all distinct, then necessarily $U = \sum_j e^{i\theta_j}|j\rangle\langle j|$ for some phases $\theta_j \in \mathbb{R}$.

Corollary 20. Let $D > 0$ be an $n \times n$ diagonal matrix. A $2n \times 2n$ symplectic matrix S is such that $S\left(\begin{smallmatrix} D & 0 \\ 0 & D\end{smallmatrix}\right)S^{\intercal}$ is in xp form, i.e.,

$$S\begin{pmatrix} D & 0 \\ 0 & D\end{pmatrix}S^{\intercal} = \begin{pmatrix} X & 0 \\ 0 & P\end{pmatrix}, \tag{B3}$$

if and only if

$$S = \begin{pmatrix} M^{-1} & 0 \\ 0 & M^{\intercal}\end{pmatrix}H\begin{pmatrix} U & 0 \\ 0 & U^*\end{pmatrix}H^{\dagger}, \tag{B4}$$

where M is an arbitrary $n \times n$ invertible matrix, H is given by (A2), and $[U, D] = 0$.

Proof. By Lemma 9, we can find an invertible matrix M such that

$$\begin{pmatrix} M & 0 \\ 0 & M^{-\intercal}\end{pmatrix}S\begin{pmatrix} D & 0 \\ 0 & D\end{pmatrix}S^{\intercal}\begin{pmatrix} M^{\intercal} & 0 \\ 0 & M^{-1}\end{pmatrix} = \begin{pmatrix} \widetilde{D} & 0 \\ 0 & \widetilde{D}\end{pmatrix},$$

where $M^{-\intercal} := (M^{-1})^{\intercal}$, and $\left(\begin{smallmatrix} M & 0 \\ 0 & M^{-\intercal}\end{smallmatrix}\right)$ is symplectic by (A6). Thanks to the uniqueness of symplectic eigenvalues, we must have that $\widetilde{D} = D$, up to an immaterial permutation that can always be absorbed into M. We can then apply Lemma 19, guaranteeing that

$$\begin{pmatrix} M & 0 \\ 0 & M^{-\intercal}\end{pmatrix}S = H\begin{pmatrix} U & 0 \\ 0 & U^*\end{pmatrix}H^{\dagger},$$

with $[U, D] = 0$. Multiplying by $\left(\begin{smallmatrix} M^{-1} & 0 \\ 0 & M^{\intercal}\end{smallmatrix}\right)$ from the left proves (B4). ■

Proposition 21 (A family of non-normal QCMs). Consider a bipartite three-mode system composed by modes A on one side and B_1, B_2 on the other. Construct the QCM

$$V_{AB} := \begin{pmatrix} a\mathbb{1} & F & G \\ F^{\intercal} & b_1\mathbb{1} & 0 \\ G^{\intercal} & 0 & b_2\mathbb{1}\end{pmatrix}, \tag{B5}$$

where the first and second rows and columns refer to A, the third and fourth to B_1, and the fifth and sixth to B_2. Assume that $\|F\|_\infty, \|G\|_\infty \leqslant 1$, $a \geqslant 3$, and $b_1, b_2 \geqslant 2$, so that $V_{AB} \geqslant \mathbb{1}_{AB}$ is a valid QCM. Further assume that $b_1 \neq b_2$ and that $[FF^{\intercal}, GG^{\intercal}] \neq 0$. Then V_{AB} is not normal.

Proof. Assume by contradiction that $(S_A \oplus S_B)\,V_{AB}\,(S_A \oplus S_B)^{\intercal}$ is in xp form. Then there are scalars $x, p > 0$ and 2×2 matrices $X', P' > 0$ such that

$$S_A\begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix}S_A^{\intercal} = \begin{pmatrix} x & 0 \\ 0 & p\end{pmatrix},$$

$$S_B\begin{pmatrix} b_1 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ 0 & 0 & b_1 & 0 \\ 0 & 0 & 0 & b_2\end{pmatrix}S_B^{\intercal} = \begin{pmatrix} X' & 0 \\ 0 & P'\end{pmatrix}.$$

If $b_1 \neq b_2$, any unitary U satisfying $[U, \left(\begin{smallmatrix} b_1 & 0 \\ 0 & b_2\end{smallmatrix}\right)] = 0$ must be of the form $U = \left(\begin{smallmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2}\end{smallmatrix}\right)$. Hence, Corollary 20 tells

us that

$$S_A = \begin{pmatrix} m^{-1} & 0 \\ 0 & m \end{pmatrix} H \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} H^\dagger$$

$$= \begin{pmatrix} m^{-1} & 0 \\ 0 & m \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

$$= \begin{pmatrix} m^{-1} & 0 \\ 0 & m \end{pmatrix} R(\varphi),$$

and

$$S_B = \begin{pmatrix} N^{-1} & 0 \\ 0 & N^\intercal \end{pmatrix} H \begin{pmatrix} e^{i\theta_1} & 0 & 0 & 0 \\ 0 & e^{i\theta_2} & 0 & 0 \\ 0 & 0 & e^{-i\theta_1} & 0 \\ 0 & 0 & 0 & e^{-i\theta_2} \end{pmatrix} H^\dagger$$

$$= \begin{pmatrix} N^{-1} & 0 \\ 0 & N^\intercal \end{pmatrix} \begin{pmatrix} \cos\theta_1 & 0 & \sin\theta_1 & 0 \\ 0 & \cos\theta_2 & 0 & \sin\theta_2 \\ -\sin\theta_1 & 0 & \cos\theta_1 & 0 \\ 0 & -\sin\theta_2 & 0 & \cos\theta_2 \end{pmatrix}$$

$$= \begin{pmatrix} N^{-1} & 0 \\ 0 & N^\intercal \end{pmatrix} (R_{B_1}(\theta_1) \oplus R_{B_2}(\theta_2)),$$

where $\varphi, \theta_1, \theta_2 \in \mathbb{R}$, $m \neq 0$, and N is 2×2 and invertible. In order for the AB_1 and AB_2 off-diagonal blocks to be brought into xp form as well, we must also request that

$$R(\varphi) F R_{B_1}(\theta_1)^\intercal = D_1, \quad R(\varphi) G R_{B_2}(\theta_2)^\intercal = D_2$$

be both diagonal. This would imply that

$$\begin{aligned} 0 &= \left[D_1^2, D_2^2\right] \\ &= \left[R(\varphi) F F^\intercal R(\varphi)^\intercal,\ R(\varphi) G G^\intercal R(\varphi)^\intercal\right] \\ &= R(\varphi)\left[F F^\intercal,\ G G^\intercal\right] R(\varphi)^\intercal, \end{aligned}$$

so that $[FF^\intercal,\ GG^\intercal] = 0$, contrary to the hypotheses. ■

[1] C. H. Bennett, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Quantum Cryptography Using Any Two Nonorthogonal States, Phys. Rev. Lett. **68**, 3121 (1992).

[4] C. E. Shannon, Communication theory of secrecy systems, Bell Labs Tech. J. **28**, 656 (1949).

[5] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[6] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 1355 (1975).

[7] I. Csiszar and J. Körner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory **24**, 339 (1978).

[8] U. M. Maurer, The strong secret key rate of discrete random triples, in *Communications and Cryptography: Two Sides of One Tapestry*, edited by R. E. Blahut, D. J. Costello, U. Maurer, and T. Mittelholzer (Springer US, Boston, MA, 1994), pp. 271–285.

[9] R. Ahlswede and I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing, IEEE Trans. Inf. Theory **39**, 1121 (1993).

[10] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[11] M. Christandl, The quantum analog to intrinsic information, Master's thesis, ETH Zurich, 2002.

[12] M. Christandl and A. Winter, Squashed entanglement: An additive entanglement measure, J. Math. Phys. **45**, 829 (2004).

[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[14] F. G. S. L. Brandão, M. Christandl, and J. Yard, Faithful squashed entanglement, Commun. Math. Phys. **306**, 805 (2011).

[15] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[16] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, 2nd ed., Texts and Monographs in Theoretical Physics (De Gruyter, New York, 2019).

[17] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).

[18] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone *et al.*, Advances in space quantum communications, IET Quantum Commun. **2**, 182 (2021).

[19] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, Entanglement-based quantum communication over 144 km, Nat. Phys. **3**, 481 (2007).

[20] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. **98**, 010504 (2007).

[21] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science **356**, 1140 (2017).

[22] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).

[23] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[24] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).

[25] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations, Adv. Quantum Technol. **1**, 1800011 (2018).

[26] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[27] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[28] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[29] D. Gottesman and J. Preskill, Secure quantum key distribution using squeezed states, Phys. Rev. A **63**, 022309 (2001).

[30] N. J. Cerf, M. Levy, and G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

[31] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[32] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangiera, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[33] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography Without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[34] R. García-Patrón and N. J. Cerf, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Phys. Rev. Lett. **102**, 130501 (2009).

[35] R. García-Patrón, Quantum information with optical continuous variables: From Bell tests to key distribution, Ph.D. thesis, Université libre de Bruxelles, 2007.

[36] S. Tserkis, N. Hosseinidehaj, N. Walk, and T. C. Ralph, Teleportation-based collective attacks in Gaussian quantum key distribution, Phys. Rev. Res. **2**, 013208 (2020).

[37] A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution, Phys. Rev. Res. **4**, 013099 (2022).

[38] G. Adesso, S. Ragy, and A. R. Lee, Continuous variable quantum information: Gaussian states and beyond, Open Syst. Inf. Dyn. **21**, 1440001 (2014).

[39] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Boca Raton, FL, 2017).

[40] E. Schrödinger, Der stetige Übergang von der Mikro- zur Makromechanik, Naturwissenschaften **14**, 664 (1926).

[41] J. R. Klauder, The action option and a Feynman quantization of spinor fields in terms of ordinary c-numbers, Ann. Phys. **11**, 123 (1960).

[42] R. J. Glauber, Coherent and incoherent states of the radiation field, Phys. Rev. **131**, 2766 (1963).

[43] E. C. G. Sudarshan, Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams, Phys. Rev. Lett. **10**, 277 (1963).

[44] E. H. Kennard, Zur Quantenmechanik einfacher Bewegungstypen, Z. Phys. **44**, 326 (1927).

[45] D. Stoler, Equivalence classes of minimum uncertainty packets, Phys. Rev. D **1**, 3217 (1970).

[46] H. P. Yuen, Two-photon coherent states of the radiation field, Phys. Rev. A **13**, 2226 (1976).

[47] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, Observation of Squeezed States Generated by Four-Wave Mixing in an Optical Cavity, Phys. Rev. Lett. **55**, 2409 (1985).

[48] U. L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, 30 years of squeezed light generation, Phys. Scr. **91**, 053001 (2016).

[49] R. Schnabel, Squeezed states of light and their applications in laser interferometers, Phys. Rep. **684**, 1 (2017).

[50] M. Navascués, J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acín, Quantum Key Distillation from Gaussian States by Gaussian Operations, Phys. Rev. Lett. **94**, 010502 (2005).

[51] M. Navascués and A. Acín, Gaussian operations and privacy, Phys. Rev. A **72**, 012303 (2005).

[52] C. Rodó, O. Romero-Isart, K. Eckert, and A. Sanpera, Efficiency in quantum key distribution protocols with entangled Gaussian states, Open Syst. Inf. Dyn. **14**, 69 (2007).

[53] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Efficient Classical Simulation of Continuous Variable Quantum Information Processes, Phys. Rev. Lett. **88**, 097904 (2002).

[54] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Universal Quantum Computation with Continuous-Variable Cluster States, Phys. Rev. Lett. **97**, 110501 (2006).

[55] M. Ohliger, K. Kieling, and J. Eisert, Limitations of quantum computing with Gaussian cluster states, Phys. Rev. A **82**, 042336 (2010).

[56] A. Mari and J. Eisert, Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient, Phys. Rev. Lett. **109**, 230503 (2012).

[57] J. Eisert, S. Scheel, and M. B. Plenio, Distilling Gaussian States with Gaussian Operations is Impossible, Phys. Rev. Lett. **89**, 137903 (2002).

[58] J. Fiurášek, Gaussian Transformations and Distillation of Entangled Gaussian States, Phys. Rev. Lett. **89**, 137904 (2002).

[59] G. Giedke and J. I. Cirac, Characterization of Gaussian operations and distillation of Gaussian states, Phys. Rev. A **66**, 032316 (2002).

[60] J. Niset, J. Fiurášek, and N. J. Cerf, No-Go Theorem for Gaussian Quantum Error Correction, Phys. Rev. Lett. **102**, 120501 (2009).

[61] L. Lami, B. Regula, X. Wang, R. Nichols, A. Winter, and G. Adesso, Gaussian quantum resource theories, Phys. Rev. A **98**, 022335 (2018).

[62] L. Lami, R. Takagi, and G. Adesso, Assisted distillation of Gaussian resources, Phys. Rev. A **101**, 052305 (2020).

[63] M. M. Wolf, G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, Gaussian entanglement of formation, Phys. Rev. A **69**, 052320 (2004).

[64] G. Adesso and F. Illuminati, Gaussian measures of entanglement versus negativities: Ordering of two-mode Gaussian states, Phys. Rev. A **72**, 032334 (2005).

[65] G. Adesso, D. Girolami, and A. Serafini, Measuring Gaussian Quantum Information and Correlations Using the Rényi Entropy of Order 2, Phys. Rev. Lett. **109**, 190502 (2012).

[66] L. Lami, C. Hirche, G. Adesso, and A. Winter, Schur Complement Inequalities for Covariance Matrices and Monogamy of Quantum Correlations, Phys. Rev. Lett. **117**, 220502 (2016).

[67] L. Lami, C. Hirche, G. Adesso, and A. Winter, From log-determinant inequalities to Gaussian entanglement via recoverability theory, IEEE Trans. Inf. Theory **63**, 7553 (2017).

[68] L. Lami, S. Khatri, G. Adesso, and M. M. Wilde, Extendibility of Bosonic Gaussian States, Phys. Rev. Lett. **123**, 050501 (2019).

[69] L. Mišta and R. Tatham, Gaussian Intrinsic Entanglement, Phys. Rev. Lett. **117**, 240505 (2016).

[70] L. Mišta and R. Tatham, Gaussian intrinsic entanglement: An entanglement quantifier based on secret correlations, Phys. Rev. A **91**, 062313 (2015).

[71] L. Mišta and K. Baksová, Gaussian intrinsic entanglement for states with partial minimum uncertainty, Phys. Rev. A **97**, 012305 (2018).

[72] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Quantum information with Gaussian states, Phys. Rep. **448**, 1 (2007).

[73] We usually assume $s = 0$, since the mean can be changed by local unitaries (displacements), and these do not affect the entanglement nor the (Gaussian) secret key properties of the state.

[74] R. Simon, N. Mukunda, and B. Dutta, Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms, Phys. Rev. A **49**, 1567 (1994).

[75] The direct sum is understood to correspond to a partition of the canonical operators into those pertaining to each subsystem. For instance, for a two-mode bipartite system we have the decomposition $r_{AB} = (x_A, x_B, p_A, p_B)^\intercal = (x_A, p_A)^\intercal \oplus (x_B, p_B)^\intercal = r_A \oplus r_B$.

[76] For a mathematically rigorous notion of quantum-classical channel, see Barchielli and Lupieri [78] and also Holevo and Kuznetsova [79].

[77] The factor $1/2$ depends on the different conventions chosen for QCMs and classical covariance matrices. For example, we have defined the first entry of the QCM of an m-mode state ρ with vanishing displacement vector to be $V_{11} = 2\mathrm{Tr}[x_1^2\rho]$, which is twice the variance of the observable x_1 on ρ.

[78] A. Barchielli and G. Lupieri, Instruments and mutual entropies in quantum information, Banach Center Publ. **73**, 65 (2006).

[79] A. S. Holevo and A. A. Kuznetsova, The information capacity of entanglement-assisted continuous variable quantum measurement, J. Phys. A: Math. Theor. **53**, 375307 (2020).

[80] Doing this is a useful exercise that the interested reader is encouraged to solve on their own.

[81] Note that allowing general Gaussian states for the ancillae and general nondeterministic Gaussian operations instead of Gaussian unitaries does not lead to a wider set of protocols. In fact, recall that any Gaussian state can be prepared by applying a Gaussian unitary to the vacuum and discarding some modes, and that nondeterministic Gaussian operations can always be realized by appending ancillae in the vacuum state, acting with Gaussian unitaries, and performing Gaussian measurements on some of the modes [[39], Secs. 5.3–5.5].

[82] S.-W. Ji, M. S. Kim, and H. Nha, Quantum steering of multimode Gaussian states by Gaussian measurements: Monogamy relations and the Peres conjecture, J. Phys. A: Math. Theor. **48**, 135301 (2015).

[83] G. Adesso and R. Simon, Strong subadditivity for log-determinant of covariance matrices and its applications, J. Phys. A: Math. Theor. **49**, 34LT02 (2016).

[84] B. M. Terhal, M. Horodecki, D. W. Leung, and D. P. DiVincenzo, The entanglement of purification, J. Math. Phys. **43**, 4286 (2002).

[85] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Locking Classical Correlations in Quantum States, Phys. Rev. Lett. **92**, 067902 (2004).

[86] L. Mišta, R. Tatham, D. Girolami, N. Korolkova, and G. Adesso, Measurement-induced disturbances and nonclassical correlations of Gaussian states, Phys. Rev. A **83**, 042325 (2011).

[87] G. Giedke, J. Eisert, J. I. Cirac, and M. B. Plenio, Entanglement transformations of pure Gaussian states, Quantum Inf. Comput. **3**, 211 (2003).

[88] R. R. Tucci, Quantum entanglement and conditional information transmission, arXiv:quant-ph/9909041.

[89] M. Christandl and A. Winter, Uncertainty, monogamy, and locking of quantum correlations, IEEE Trans. Inf. Theory **51**, 3159 (2005).

[90] M. Takeoka, S. Guha, and M. M. Wilde, The squashed entanglement of a quantum channel, IEEE Trans. Inf. Theory **60**, 4987 (2014).

[91] U. M. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Inf. Theory **45**, 499 (1999).

[92] N. Gisin, R. Renner, and S. Wolf, Linking classical and quantum key agreement: Is there a classical analog to bound entanglement? Algorithmica **34**, 389 (2002).

[93] R. Renner and S. Wolf, New bounds in secret-key agreement: The gap between formation and secrecy extraction, in *Advances in Cryptology — EUROCRYPT 2003*, edited by E. Biham (Springer, Berlin, 2003), pp. 562–577.

[94] M. Christandl, R. Renner, and S. Wolf, A property of the intrinsic mutual information, in *Proc. IEEE Int. Symp. Inf. Theory* (IEEE, Piscataway, NJ, 2003), pp. 258–258.

[95] M. Christandl and R. Renner, On intrinsic information, in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)* (IEEE, Piscataway, NJ, 2004), pp. 135.

[96] A. Winter, Secret, public and quantum correlation cost of triples of random variables, in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)* (IEEE, Piscataway, NJ, 2005), pp. 2270–2274.

[97] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Unifying classical and quantum key distillation, in *Theory of Cryptography*, edited by S. Vadhan (Springer, Berlin, 2007), pp. 456–478.

[98] R. König, R. Renner, A. Bariska, and U. Maurer, Small Accessible Quantum Information Does Not Imply Security, Phys. Rev. Lett. **98**, 140502 (2007).

[99] T. H. Chan, Balanced information inequalities, IEEE Trans. Inf. Theory **49**, 3261 (2003).

[100] R. M. Fano, *Transmission of Information: A Statistical Theory of Communications* (M.I.T. Press, Cambridge, MA, 1961), pp. x+389.

[101] M. Fannes, A continuity property of the entropy density for spin lattice systems, Commun. Math. Phys. **31**, 291 (1973).

[102] K. M. R. Audenaert, A sharp continuity estimate for the von Neumann entropy, J. Phys. A: Math. Theor. **40**, 8127 (2007).

[103] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A: Math. Gen. **37**, L55 (2004).

[104] A. Winter, Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints, Commun. Math. Phys. **347**, 291 (2016).

[105] M. A. Alhejji and G. Smith, A tight uniform continuity bound for equivocation, in *2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA* (IEEE, Piscataway, NJ, 2020), pp. 2270–2274 .

[106] M. M. Wilde, Optimal uniform continuity bound for conditional entropy of classical–quantum states, Quantum Inf. Process. **19**, 61 (2020).

[107] A. Kraskov, H. Stögbauer, and P. Grassberger, Estimating mutual information, Phys. Rev. E **69**, 066138 (2004).

[108] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A. **461**, 207 (2005).

[109] Actually, Maurer's result [[8], Theorem 4] as stated holds for two-way public communication. However, a quick glance at the proof reveals that the two bounds in [[8], Eq. (10)] require only one-way communication—either from Alice to Bob or vice versa. Devetak and Winter are more explicit in clarifying that they only need one-way communication [108].

[110] Remember that in our case the variable Z, representing Eve's prior information, is absent. Then our claim follows by combining Theorem 4 and the unnumbered equation above (10) in Maurer's paper [8].

[111] We note that in the last part of the above proof, we could have equally well leveraged the result of Devetak and Winter [108] instead of that by Maurer. Verifying that their security criterion is stronger than ours is elementary, and has already been observed, e.g., by Christandl *et al.* [97].

[112] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*, edited by A. Feinstein, Holden-Day series in time series analysis (Holden-Day, San Francisco, 1964).

[113] I. Csiszár, Information-type measures of difference of probability distributions and indirect observations, Studia Sci. Math. Hungarica **2**, 299 (1967).

[114] S. Kullback, A lower bound for discrimination information in terms of variation (corresp.), IEEE Trans. Inf. Theory **13**, 126 (1967).

[115] S. P. Boyd and L. Vandenberghe, *Convex Optimization*, Berichte über verteilte messysteme (Cambridge University Press, Cambridge, 2004).

[116] R. Simon, Peres–Horodecki Separability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2726 (2000).

[117] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Inseparability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2722 (2000).

[118] S. Tserkis, J. Dias, and T. C. Ralph, Simulation of Gaussian channels via teleportation and error correction of Gaussian states, Phys. Rev. A **98**, 052335 (2018).

[119] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[120] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[121] F. Leditzky, N. Datta, and G. Smith, Useful states and entanglement distillation, IEEE Trans. Inf. Theory **64**, 4689 (2018).

[122] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[123] H. Vahlbruch, M. Mehmet, S. Chelkowski, B. Hage, A. Franzen, N. Lastzka, S. Goßler, K. Danzmann, and R. Schnabel, Observation of Squeezed Light with 10-dB Quantum-Noise Reduction, Phys. Rev. Lett. **100**, 033602 (2008).

[124] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency, Phys. Rev. Lett. **117**, 110801 (2016).

[125] J. M. Borden, D. M. Mason, and R. J. McEliece, Some information theoretic saddlepoints, SIAM J. Control Optim. **23**, 129 (1985).

[126] W. E. Stark and R. J. McEliece, On the capacity of channels with block memory, IEEE Trans. Inf. Theor. **34**, 322 (1988).

[127] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications and Signal Processing (Wiley-Interscience, New York, 2006).

[128] S. Pirandola, A quantum teleportation game, Int. J. Quantum Inform. **03**, 239 (2005).

[129] S. L. Braunstein and H. J. Kimble, Teleportation of Continuous Quantum Variables, Phys. Rev. Lett. **80**, 869 (1998).

[130] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[131] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, Theory of channel simulation and bounds for private communication, Quantum Sci. Technol. **3**, 035009 (2018).

[132] L. Lami and B. Regula, No second law of entanglement manipulation after all, Nat. Phys. **19**, 184 (2023).

[133] M. Berta, F. G. S. L. Brandão, G. Gour, L. Lami, M. B. Plenio, B. Regula, and M. Tomamichel, On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources, arXiv:2205.02813.

[134] M. A. de Gosson, *Symplectic Geometry and Quantum Mechanics*, Operator Theory: Advances and Applications (Birkhäuser, Basel, 2006).

[135] J. Williamson, On the algebraic problem concerning the normal forms of linear dynamical systems, Am. J. Math. **58**, 141 (1936).

[136] F. Zhang, *The Schur Complement and its Applications* (Springer Science & Business Media, New York, 2006), Vol. 4.

[137] L. Mirsky, Symmetric gauge functions and unitarily invariant norms, Q. J. Math. **11**, 50 (1960).

[138] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer, New York, 2013).

[139] Here we mean that every element $W_{AB} \in \mathcal{W}_{AB}$ satisfies $W_{AB} \geqslant \kappa^{-1}\mathbb{1}_{AB}$.

[140] W. Rudin, *Principles of Mathematical Analysis*, International Series in Pure and Applied Mathematics (McGraw-Hill, New York, 1964).