

Gaussian two-mode attacks in one-way quantum cryptography

Carlo Ottaviani,^{1,*} Stefano Mancini,^{2,3} and Stefano Pirandola¹

¹*Department of Computer Science & York Center for Quantum Technologies, University of York, York YO10 5GH, United Kingdom*

²*School of Science and Technology, University of Camerino, Camerino (MC), I-62032, Italy*

³*INFN Sezione di Perugia, I-61023, Perugia, Italy*

(Received 20 December 2016; published 3 May 2017)

We investigate the asymptotic security of one-way continuous variable quantum key distribution against Gaussian two-mode coherent attacks. The one-way protocol is implemented by arranging the channel uses in two-mode blocks. By applying symmetric random permutations over these blocks, the security analysis is in fact reduced to study two-mode coherent attacks and, in particular, Gaussian ones, due to the extremality of Gaussian states. We explicitly show that the use of two-mode Gaussian correlations by an eavesdropper leads to asymptotic secret key rates which are *strictly* larger than the rate obtained under standard single-mode Gaussian attacks.

DOI: [10.1103/PhysRevA.95.052310](https://doi.org/10.1103/PhysRevA.95.052310)

I. INTRODUCTION

Quantum technologies are becoming reality, with huge efforts being devoted to developing scalable quantum computers and robust quantum communications, e.g., for building a future quantum internet [1–5]. In this global scenario, quantum key distribution (QKD) [6–8] is certainly one of the most advanced areas, with intense research activities directed towards practical implementations. QKD represents a set of strategies that, integrating both quantum and classical communication, allow two authorized remote users (Alice and Bob) to generate a random sequence of bits; this is then used as an encryption key in a one-time pad protocol [9], therefore providing an unconditionally secure (information-theoretic [10]) private communication between the remote users.

The effectiveness of QKD relies on the ground rule of encoding classical information in nonorthogonal quantum states [11], that are then transmitted through a noisy quantum channel controlled by the eavesdropper (Eve). This is also equivalent to sending the “nonorthogonal part” of discordant quantum states [12]. In this way, Eve’s attack is bounded by fundamental laws of quantum physics [13]: any information gained by Eve creates loss and noise on the quantum channel. Thanks to this trade-off, Alice and Bob can accurately quantify the amount of classical error correction and privacy amplification needed to reduce Eve’s stolen information to a negligible amount [6].

Since the first proposals to implement quantum information and computational tasks, continuous variable (CV) systems have attracted increasing attention [14,15]. The fact of using quantum systems with continuous spectra (infinite-dimensional Hilbert spaces) has several advantages with respect to the traditional approach based on discrete variables (qubits). In particular, one can implement QKD at *high rates* by using highly modulated coherent states and homodyne detections, not only in one-way schemes [16–21], but also in two-way protocols [22–26] and CV strategies based on measurement-device independence (MDI) [27–30].

Ideal implementations of CV-QKD provide the highest key rates, not so far from the ultimate repeaterless bound

recently established in Ref. [31]. For a lossy channel with transmissivity τ , the maximum rate achievable by any QKD protocol (secret-key capacity) is equal to [31] $K = -\log_2(1 - \tau)$, with a fundamental rate-loss scaling of $\tau/\ln 2 \simeq 1.44\tau$ bits per channel use for long distances, i.e., at high loss $\tau \simeq 0$. The most practical one-way CV-QKD protocols, i.e., the switching [16] and no-switching [17] protocols, can potentially reach an asymptotic long-distance rate of $\tau/\ln 4$ bits per use, which is half the secret key capacity. Similar performance occurs for CV-MDI-QKD in the most asymmetric configuration [32].

In this work we deepen the study of the secret key rates of the most known one-way CV-QKD protocols [16,17]. In particular, we explicitly study their security in the presence of Gaussian two-mode attacks, representing the residual eavesdropping strategy after the de Finetti symmetrization [33,34] over two-mode blocks. Under these attacks, we derive the analytical expressions of the asymptotic key rates [35]. With these in hand, we show that eavesdropping strategies based on correlated ancillas turn out to be *strictly* less effective than Gaussian attacks based on uncorrelated ancillas (single-mode attacks). In other words, any two-mode Gaussian attack with strictly nonzero correlations improves Alice and Bob’s key rate.

II. PROTOCOL AND GENERAL CONSIDERATIONS

Let us consider the communication scheme of Fig. 1(a). Alice sends to Bob $N \gg 1$ coherent states $|\alpha_k\rangle$. The amplitudes α_k , for $k = 1, \dots, N$, are independently and identically modulated by a bivariate zero mean Gaussian distribution of variance μ . The communication channel is under Eve’s control, and the output detections provide Bob with classical outcomes β_k . After N uses of the channel, the parties share two correlated random sequences of symbols given by the sets $\{\alpha_k\}$ and $\{\beta_k\}$.

For the sake of clarity, we consider reverse reconciliation (RR), so that the key is obtained by Alice inferring Bob’s variables. Now, when Bob applies homodyne detections, randomly switching between measurements on quadrature \hat{q}_k and \hat{p}_k , we have the switching protocol [16]. By contrast, when Bob measures both quadratures (heterodyne detection), we have the no-switching protocol [17]. Here we discuss the latter case, while we leave the analysis of the switching protocol in Appendix B.

*carlo.ottaviani@york.ac.uk

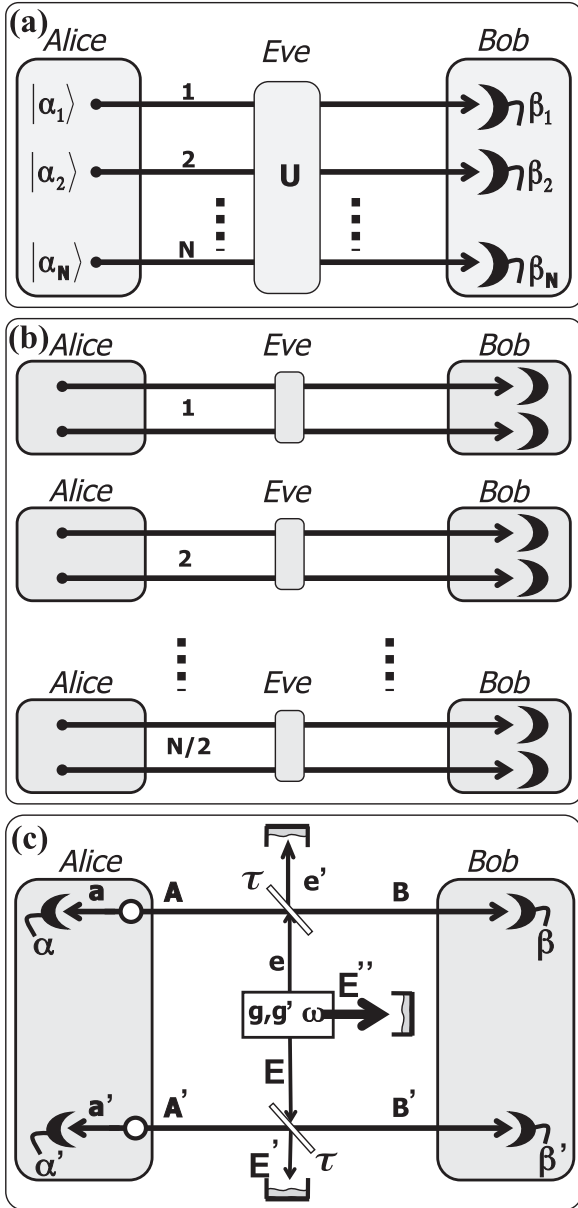


FIG. 1. Reduction to Gaussian two-mode attacks. (a) Alice Gaussianly modulates N coherent states $|\alpha_k\rangle$ in an independent and identical fashion. These are sent through a quantum channel (Eve) and received by Bob, whose measurements provide the classical variables β_k for $k = 1, \dots, N$. Eve's general eavesdropping is based on a global unitary operation, U , applied to the N instances of the one-way communication. (b) After random permutations, the coherence of the general attack is confined within each two-mode block. (c) Within an arbitrary block, we show a Gaussian two-mode attack against the protocol (in EB representation). A realistic Gaussian attack is simulated by two beam splitters, with transmissivity τ , mixing Alice's signals, A and A' , with Eve's ancillary modes, e and E , belonging to a larger set of modes $\{e, E, E''\}$ in her hands. The reduced state of modes e and E is Gaussian with thermal noise ω and correlation matrix \mathbf{G} as in Eq. (4).

In a general attack, Eve applies a global unitary operation U , which coherently processes her ancillary modes with all the N signals exchanged by the parties, with the ancillary outputs stored in a quantum memory. One has that the Bob-Eve joint

system is described by a quantum state in the following form:

$$\rho = U \left(\bigotimes_{k=1}^N |\alpha_k\rangle\langle\alpha_k| \otimes |\Phi\rangle_{\text{Eve}}\langle\Phi| \right) U^\dagger, \quad (1)$$

where $|\Phi\rangle_{\text{Eve}}$ is Eve's total input state. The security analysis considering this general scenario is not a practically solvable problem but, in the limit of $N \rightarrow \infty$, it has been proved [33,34] that one can get rid of the cross correlations between different uses of the channel. More specifically, with no loss of generality, the security analysis can be simplified by applying symmetric random permutations on the input ($\{\alpha_k\}$) and output ($\{\beta_k\}$) classical data sets.

Note that Alice and Bob may arrange the signals into two-mode blocks c_j , with $j = 1, \dots, N/2$. Then, they can apply random permutations over the blocks c_j rather than over the single uses of the channel. After such a symmetrization, the quantum state given in Eq. (1) can be rewritten as the following tensor product:

$$\rho \simeq \bigotimes_{j=1}^M \rho_{\text{block}}, \quad (2)$$

where $M = N/2$ is large. After this symmetrization, the initial global coherence of quantum state of Eq. (1) is reduced to that one enclosed within each two-mode state ρ_{block} , associated with the arbitrary block c_j , as also depicted in Fig. 1(b). Thus the only effective coherence to consider is two mode and this scenario can be further simplified using the extremality of Gaussian states [36].

In other words, the previous assumptions allow us to reduce the general eavesdropping strategy to a Gaussian two-mode attack within each block. In particular, we may consider the most realistic form of such an attack, where Eve exploits two beam splitters to combine Alice's signals with correlated ancillas prepared in an arbitrary Gaussian state. See Fig. 1(c). Note that this is a reduction which is often considered in practice. The security analysis of one-way CV-QKD protocols under collective (single-mode) Gaussian attacks [37] is typically restricted to the most practical case of entangling-cloner attacks, resulting in thermal-loss channels between Alice and Bob. The optimal key rate achievable over this channel has been recently upper bounded in Ref. [31] and lower bounded in Ref. [38].

III. ENTANGLEMENT-BASED REPRESENTATION AND GAUSSIAN TWO-MODE ATTACKS

The security analysis is performed in the entanglement based (EB) representation [15,39], as also shown in Fig. 1(c). Alice owns a source of two-mode squeezed vacuum (TMSV) states. These are zero-mean Gaussian states with covariance matrix (CM) of the form

$$\mathbf{V}_{\text{EPR}} = \begin{pmatrix} \mu \mathbf{I} & \sqrt{\mu^2 - 1} \mathbf{Z} \\ \sqrt{\mu^2 - 1} \mathbf{Z} & \mu \mathbf{I} \end{pmatrix}, \quad (3)$$

where $\mu \geq 1$, $\mathbf{I} = \text{diag}(1, 1)$ and $\mathbf{Z} = \text{diag}(1, -1)$. In each block, Alice's input state is Gaussian of the form $\rho_{aA} \otimes \rho_{a'A'}$ and CM $\mathbf{V}_{\text{EPR}} \oplus \mathbf{V}_{\text{EPR}}$. The signal coherent states $|\alpha\rangle$ and $|\alpha'\rangle$ are remotely projected on modes, A and A' , by applying

heterodyne detections on local modes a and a' . In this way, Alice modulates the amplitudes α and α' according to a zero-mean Gaussian distribution with variance $\mu - 1$ (which is typically large).

As previously mentioned, we assume a realistic Gaussian two-mode attack where Eve employs two identical beam splitters with transmissivity τ . These are used to mix Alice's input modes, A and A' , with Eve's ancillary modes, e and E , respectively. The latter belong to a larger set of ancillary states $\{e, E, E''\}$ owned by the eavesdropper. The reduced Gaussian state σ_{eE} is completely determined by the following CM [40]:

$$\mathbf{V}_{eE} = \begin{pmatrix} \omega \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega \mathbf{I} \end{pmatrix}, \quad \text{for } \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \quad (4)$$

where $\omega = 2\bar{n} + 1$ quantifies Eve's thermal noise, with \bar{n} mean number of thermal photons. The correlations between modes e and E are described by the parameters g and g' in the matrix \mathbf{G} . Their values are bounded by the constraints

$$|g| < \omega, \quad |g'| < \omega, \quad \omega|g + g'| \leq \omega^2 + gg' - 1, \quad (5)$$

which are imposed by the the uncertainty principle [27,40]. Note that from the CM of Eq. (4), one can recover the standard collective attack scenario (single-mode attack) for $g = g' = 0$.

In the ideal case of perfect RR efficiency, the key rate (bit per channel use) is defined as

$$R = \frac{I_{AB} - I_E}{2}, \quad (6)$$

where I_{AB} is the mutual information between variables $\{\alpha, \beta\}$ and $\{\alpha', \beta'\}$ and I_E is Eve's accessible information on Bob's variables (factor 2 accounts for the double use of the channel within each block). For many uses of the channel $N \gg 1$, I_E is bounded by the Holevo information

$$\chi = S_E - S_{E|\beta\beta'} = S_{AB} - S_{A|\beta\beta'}. \quad (7)$$

Here S_E is the entropy of Eve's output state, $\rho_{\text{Eve}} = \rho_{e'E'}$, and is then equal to the entropy S_{AB} of Alice and Bob's joint state $\rho_{AB} = \rho_{aa'BB'}$ (because the global state of Alice, Bob, and Eve is pure). Then, $S_{E|\beta\beta'}$ is the entropy of Eve's state $\rho_{e'E'|\beta\beta'}$ conditioned on Bob variables β and β' ; because these are the outcomes of a rank-1 measurement, we have that Alice's conditional state $\rho_{A|\beta\beta'}$ has entropy $S_{A|\beta\beta'} = S_{E|\beta\beta'}$.

Note that, for Gaussian states, the von Neumann entropy $S(\cdot)$ can be computed via the formula

$$S := \sum_x h(x), \quad (8)$$

where x are symplectic eigenvalues [15] and

$$h(x) := \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}. \quad (9)$$

By replacing I_E in Eq. (6) with the Holevo function of Eq. (7), one obtains the following ideal key rate (in RR):

$$R := \frac{I_{AB} - \chi}{2}. \quad (10)$$

IV. SECURITY ANALYSIS

A. Mutual information

As a consequence of the two-mode reduction strategy, Alice and Bob's mutual information is given by

$$I_{AB} = I + I', \quad (11)$$

where $I := I(\alpha, \beta)$ is the contribution from the first channel use, and $I' := I(\alpha', \beta')$ from the second use. Each contribution is given by the following expression:

$$I = \log_2 \frac{V_B + 1}{V_{B|\alpha} + 1},$$

$$I' = \log_2 \frac{V_B + 1}{V_{B|\alpha'} + 1}, \quad (12)$$

where $V_B = \tau\mu + (1-\tau)\omega$ describes the quadrature variance of the average thermal state arriving at Bob's side, while $V_{B|\alpha} = V_{B|\alpha'} = \tau + (1-\tau)\omega$ is the quadrature variance of Bob's state after Alice's heterodyne detection. Using these relations in Eqs. (11) and (12), and working in the limit of $\mu \gg 1$, one easily obtains

$$I_{AB} = 2 \log_2 \frac{\tau\mu}{1 + \tau + (1-\tau)\omega}. \quad (13)$$

We note that, as one would expect, this expression does not depend on the correlation parameters g and g' .

B. Holevo bound

We now describe the general steps to obtain the Holevo bound χ (more details are in Appendix A). Working in the EB representation, Alice and Bob's joint state $\rho_{aa'BB'}$ is described by the following CM:

$$\mathbf{V} = \begin{pmatrix} (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} & \\ & (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} \\ \Phi\mathbf{Z} & & \Lambda\mathbf{I} & (1-\tau)\mathbf{G} \\ & \Phi\mathbf{Z} & (1-\tau)\mathbf{G} & \Lambda\mathbf{I} \end{pmatrix}, \quad (14)$$

where we have set

$$\Lambda := \tau(\mu+1) + (1-\tau)\omega, \quad (15)$$

$$\Phi := \sqrt{\tau[(\mu+1)^2 - 1]}. \quad (16)$$

The symplectic spectrum is obtained from the ordinary eigenvalues of matrix $|i\Omega\mathbf{V}|$ [15] with

$$\Omega = \bigoplus_j^4 \omega_j, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (17)$$

In the limit of large μ , and after some simple algebra, we find the following symplectic eigenvalues:

$$v_+ = \sqrt{(\omega+g)(\omega+g')}, \quad (18)$$

$$v_- = \sqrt{(\omega-g)(\omega-g')}, \quad (19)$$

$$v_1 = v_2 = (1-\tau)\mu. \quad (20)$$

Using these eigenvalues and the expansion

$$h(x) \simeq \log_2 \frac{e}{2} x + O(x^{-1}), \quad (21)$$

we find the following expression for Alice and Bob's von Neumann entropy:

$$S_{AB} = h(v_+) + h(v_-) + 2 \log_2 \frac{e}{2} (1 - \tau) \mu. \quad (22)$$

The next step is to apply two sequential heterodyne detections on modes B and B' , to obtain the conditional CM \mathbf{V}_C describing the conditional quantum state $\rho_{aa'|\beta\beta'}$. The corresponding CM has a complicated expression that can be found in Eq. (A11) of Appendix A. Computing its symplectic eigenvalues in the limit of $\mu \gg 1$, we find the following conditional spectrum:

$$\{\bar{v}_+, \bar{v}_-\} = \left\{ \frac{\sqrt{\lambda_+ \lambda'_+}}{\tau}, \frac{\sqrt{\lambda_- \lambda'_-}}{\tau} \right\}, \quad (23)$$

where we have defined

$$\lambda_{\pm} := 1 + (1 - \tau)(\omega \pm g), \quad (24)$$

$$\lambda'_{\pm} := 1 + (1 - \tau)(\omega \pm g'). \quad (25)$$

The conditional entropy just reads

$$S_{A|\beta\beta'} = h(\bar{v}_+) + h(\bar{v}_-). \quad (26)$$

Finally, using Eqs. (22) and (26) in Eq. (7), we can write Eve's Holevo bound as

$$\chi = 2 \log_2 \frac{e}{2} (1 - \tau) \mu + \sum_{i=\pm} [h(v_i) - h(\bar{v}_i)]. \quad (27)$$

It is easy to check that Eq. (27) recovers the expression of the Holevo bound of standard collective (single-mode) Gaussian attacks for $g = g' = 0$.

C. Secret-key rate and its analysis

It is easy to compute the secret-key rate using Eqs. (13) and (27) in Eq. (10). After some algebra, we obtain the following expression for the rate of the no-switching protocol under realistic Gaussian two-mode attacks:

$$R = \log_2 \frac{2}{e} \frac{\tau}{(1 - \tau)[1 + \tau + (1 - \tau)\omega]} + \frac{1}{2} \sum_{i=\pm} [h(\bar{v}_i) - h(v_i)]. \quad (28)$$

In order to prove that Gaussian two-mode attacks with nonzero correlations are strictly less effective than single-mode attacks, we study the derivatives of this rate. We find the following strict inequality:

$$R(\tau, \omega, g, g') > R(\tau, \omega, 0, 0), \quad \forall g, g' \neq 0. \quad (29)$$

The details of the proof are in Appendix A, while here we limit the discussion to the general ideas. To show Eq. (29), we first seek for critical points of the function $R(\tau, \omega, g, g')$. Solving the equation $\nabla R = 0$ on the (g, g') plane, one finds that only the origin $P_0 := (0, 0)$ is critical. To determine the nature of P_0 , we then compute the second-order derivatives with respect to the correlation parameters g and g' . This allows us to compute the expression of the Hessian matrix H and study

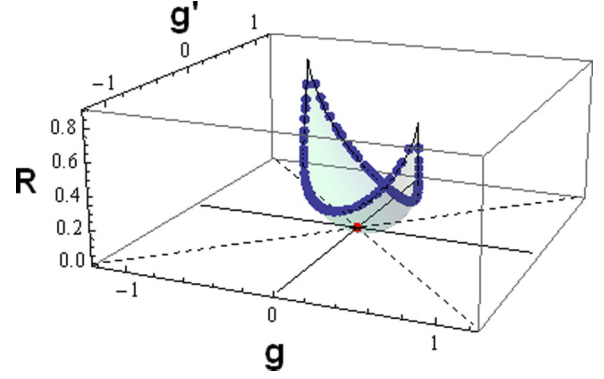


FIG. 2. We analyze the key rate of Eq. (28) over the plane of the correlation parameters, g and g' . Any two-mode attack corresponds to a point in the colored surface. Boundary attacks, verifying the condition $\omega|g + g'| = \omega^2 + gg' - 1$, are represented by the blue points. The rate of the single-mode attack $g = g' = 0$ is the red spot. Here we fix $\tau \simeq 0.44$ and $\omega = 1.2$. For these values, the single-mode attack provides zero key rate. On the other hand, we see that the key rate is positive for any two-mode attack with nonzero correlations.

its positive definiteness. We therefore find that P_0 corresponds to the absolute minimum of the rate in Eq. (28) within the domain defined by Eq. (5).

Finally we check that the attacks over the boundary, given by the condition $\omega|g + g'| = \omega^2 + gg' - 1$, also provide key rates which are strictly larger than that under the single-mode attack. In Fig. 2 we show a numerical example, which is obtained by fixing the transmissivity $\tau \simeq 0.44$, the thermal noise $\omega = 1.2$, and plotting the rate as a function of g and g' . We see that the secret-key rate under single-mode attack (red dot) is always strictly less than that of the rate which is obtained by any physically permitted two-mode attack (which is a point in the colored surface). The key rates for the attacks on the boundary of this region are the blue dots. The origin P_0 is therefore always an absolute minimum for R . As a consequence, any correlation injected into the channels by the eavesdropper to implement the coherent attack automatically increases the key rate.

V. CONCLUSION

In this work we have explicitly studied the security of one-way CV-QKD protocols against Gaussian two-mode attacks. The approach is based on an attack-reduction strategy where the parties pack the uses of the quantum channel in two-mode blocks. Then, they apply random permutations over these blocks. This allows them to get rid of any cross correlation engineered by the eavesdropper between different blocks. We solved this problem analytically, and we obtained the secret-key rates under Gaussian two-mode attacks, in particular, those more realistic and based on a suitable combination of entangling cloners.

We have then showed that any nonzero correlation used by the eavesdropper leads to a strictly higher key rate than the rate obtained under Gaussian single-mode attacks. This is achieved under the condition that infinite signals are exchanged (asymptotic rate), therefore not considering composable or finite-size analyses [41]. We conjecture that the use of

correlations is not effective even when the size of the blocks is greater than two modes. It would be interesting to check if this is still true if Alice adopted correlated encoding between different uses of the channel [42].

ACKNOWLEDGMENTS

This work has been supported by the EPSRC via the ‘‘UK Quantum Communications HUB’’ (Grant No. EP/M013472/1).

APPENDIX A: COMPUTATIONS FOR THE NO-SWITCHING PROTOCOL

Here we provide the calculations to prove Eq. (29) for the no-switching protocol.

1. Total covariance matrix

Let $\mathbf{X} = (\hat{q}_X, \hat{p}_X)$ be the vectorial quadrature operator describing a general mode X . The impact of the attenuation and noise on Alice’s modes, A and A' , through two identical beam splitters of transmissivity τ are given by the following expressions:

$$\mathbf{B} = \sqrt{\tau}\mathbf{A} + \sqrt{1-\tau}\mathbf{e}, \quad (\text{A1})$$

$$\mathbf{B}' = \sqrt{\tau}\mathbf{A}' + \sqrt{1-\tau}\mathbf{E}, \quad (\text{A2})$$

where \mathbf{e} and \mathbf{E} are the vectorial quadrature operators describing Eve’s ancillary modes, e and E , mixed at the beam splitters with modes A and A' , respectively. Eve’s reduced state σ_{eE} is zero-mean Gaussian with CM as in Eq. (4), with local thermal noise ω and correlation parameters $\mathbf{G} := \text{diag}(g, g')$ fulfilling the constraints of Eq. (5). We order Alice and Bob’s output modes as follows: a, a', B, B' ; then, we use Eqs. (A1) and (A2) to compute the CM describing Alice and Bob’s total state $\rho_{aa'BB'}$. It is simple to derive the following expression:

$$\mathbf{V} = \begin{pmatrix} (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} & \\ & (\mu+1)\mathbf{I} & & \Phi\mathbf{Z} \\ \Phi\mathbf{Z} & & \Lambda\mathbf{I} & (1-\tau)\mathbf{G} \\ & \Phi\mathbf{Z} & (1-\tau)\mathbf{G} & \Lambda\mathbf{I} \end{pmatrix}, \quad (\text{A3})$$

where $\mu - 1$ is the classical Gaussian modulation, while Λ and Φ are defined in Eqs. (15) and (16).

2. Alice and Bob’s mutual information

In the no-switching protocol, Bob performs heterodyne detections measuring both quadratures \hat{q} and \hat{p} . From the form of the attack, we have that the variances in \hat{q} and \hat{p} , relative to both Bob’s modes B and B' , are identical and given by $V_B = \Lambda$, with Λ specified in Eq. (15). The conditional variances, after Alice’s heterodyne detections, are given by

$$V_{B|\alpha, \alpha'} = \tau + (1-\tau)\omega. \quad (\text{A4})$$

Accounting for the double use of the channel within the block, we derive the mutual information

$$I_{AB} = 2 \log_2 \frac{V_B + 1}{V_{B|\alpha, \alpha'} + 1}. \quad (\text{A5})$$

Taking the limit of large modulation ($\mu \gg 1$), one gets the asymptotic expression of the mutual information, given in Eq. (13) of the main text; i.e.,

$$I_{AB} = 2 \log_2 \frac{\tau(\mu+1) + (1-\tau)\omega + 1}{1 + \tau + (1-\tau)\omega} \xrightarrow{\mu \rightarrow \infty} 2 \log_2 \frac{\tau\mu}{1 + \tau + (1-\tau)\omega}. \quad (\text{A6})$$

3. Computation of the Holevo bound

The EB representation and dilation of the two-mode channel allows us to describe the joint Alice-Bob-Eve output state as pure. Noting that this quantum state is always processed by rank-1 measurements, one has that the purity is also preserved on the conditional state after detection. The eavesdropper is assumed to control the quantum memory storing her ancillary modes; she is computationally unbounded, but the parties exchange an infinite number of signals, $N \gg 1$. In this regime Eve’s accessible information I_E on Bob’s variables is bounded by the Holevo quantity χ . It can be obtained from the von Neumann entropy of the Alice-Bob total state $S(\rho_{aa'BB'})$, and the conditional von Neumann entropy $S(\rho_{aa'|\beta\beta'})$. The Holevo bound is then given by

$$\chi = S(\rho_{aa'BB'}) - S(\rho_{aa'|\beta\beta'}). \quad (\text{A7})$$

We need to derive the function χ in terms of the relevant parameters of the protocol τ , ω , g , and g' . We then compute the symplectic spectrum of the total CM given by Eq. (A3), from the absolute value of the eigenvalues of the matrix $\mathbf{M} = i\Omega\mathbf{V}$, where $\Omega = \bigoplus_{k=1}^4 \omega$ is the 8×8 (four modes) symplectic form [15]. For large μ , one obtains the following expressions:

$$v_+ = \sqrt{(\omega+g)(\omega+g')}, \quad (\text{A8})$$

$$v_- = \sqrt{(\omega-g)(\omega-g')}, \quad (\text{A9})$$

$$v_1 = v_2 = (1-\tau)\mu, \quad (\text{A10})$$

which, together with Eq. (8) and Eq. (21), are used to calculate the total von Neumann entropy $S(\rho_{aa'BB'}) = S_{AB}$ given in Eq. (22).

Now, the conditional CM \mathbf{V}_C , providing the conditional von Neumann entropy, is obtained via heterodyning Bob’s modes B and B' . We apply the formula for heterodyne detection [43] to the total CM \mathbf{V} . After some algebra, \mathbf{V}_C can be written in the following form:

$$\mathbf{V}_C = \frac{1}{(\Lambda+1)^2 - g^2(1-\tau)^2} \begin{pmatrix} k & & \tilde{k} & \\ & k' & & \tilde{k}' \\ \tilde{k} & & k & \\ & \tilde{k}' & & k' \end{pmatrix}, \quad (\text{A11})$$

with the matrix entries defined as

$$k := (\mu+1)[g^2(1-\tau)^2 + (\Lambda+1)\tilde{\Lambda}] + (\Lambda+1)\tau, \quad (\text{A12})$$

$$\tilde{k} := -g(1-\tau)\tau\mu(\mu+2), \quad (\text{A13})$$

$$\tilde{\Lambda} := \Lambda - \tau, \quad (\text{A14})$$

$$k' := (\mu+1)[g'^2(1-\tau)^2 + (\Lambda+1)\tilde{\Lambda}] + (\Lambda+1)\tau, \quad (\text{A15})$$

$$\tilde{k}' := -g'(1-\tau)\tau\mu(\mu+2). \quad (\text{A16})$$

For large μ , the symplectic spectrum of the conditional CM \mathbf{V}_C is given by Eq. (23). Note that this spectrum does not depend on the modulation μ , and for $g = g' = 0$ we recover the conditional eigenvalues of Ref. [17].

Now, from Eq. (23), we derive the conditional von Neumann entropy $S(\rho_{aa'|\beta\beta'}) = S_{A|\beta\beta'}$, given in Eq. (26). Combining the computed entropies, we obtain the Holevo bound in Eq. (27). Finally, including the mutual information of Eq. (A6), we derive the asymptotic key rate

$$R_{\text{Block}} = \log_2 \frac{4}{e^2} \frac{\tau^2}{(1-\tau)^2 [1+\tau + (1-\tau)\omega]^2} + \sum_{k=\pm} [h(\bar{v}_k) - h(v_k)]. \quad (\text{A17})$$

More precisely, for channel use, we find

$$R = \frac{R_{\text{Block}}}{2}, \quad (\text{A18})$$

as given in Eq. (28).

4. Study of the critical point

From the first-order derivatives $\partial_g R$ and $\partial_{g'} R$, and solving the equation $\nabla R = 0$, one finds a single critical point P_0 for any τ and ω ; this is given by the origin ($g = g' = 0$) of the correlation plane (g, g'), bounded by the constraints given by Eq. (5). We then take the second-order derivative $\partial^2 R$, with respect to g and g' , and build the (symmetric) Hessian matrix

$$H = \begin{pmatrix} \partial_g^2 R & \partial_{gg'}^2 R \\ \partial_{g'g}^2 R & \partial_{g'}^2 R \end{pmatrix}. \quad (\text{A19})$$

From the positive definiteness of this matrix, evaluated in the critical point P_0 , one has that P_0 is an absolute minimum. We then study the sign, in P_0 , of the determinant of the Hessian matrix (A19).

After some algebra one can write it in the simplified form

$$\det H = \frac{D_1 - D_2}{\tau[\bar{\lambda} + \tau]\bar{\lambda}\omega(\omega^2 - 1)}, \quad (\text{A20})$$

where we have defined

$$f(x) := \frac{1}{\log_2 e} \log_2 \frac{1+x}{1-x} \quad (> 0 \text{ for } 0 < x < 1), \quad (\text{A21})$$

$$D_1 := \tau \left[f(\omega^{-1}) + 2 \log_2 \frac{\bar{\lambda} + \tau}{(1-\tau)\sqrt{\omega^2 - 1}} \right], \quad (\text{A22})$$

$$D_2 := \omega \left[f(\tau\bar{\lambda}^{-1}) + \tau^2 \log_2 \frac{\bar{\lambda} + \tau}{\bar{\lambda} + \tau - 2} \right], \quad (\text{A23})$$

$$\bar{\lambda} := 1 + \omega(1 - \tau). \quad (\text{A24})$$

One can check that $f(\tau\bar{\lambda}^{-1}) \geq 0$, and $D_1 > D_2$ for any $0 \leq \tau \leq 1$ and $\omega \geq 1$. Indeed, being both quantities τ and ω positive, as well as $\bar{\lambda}$, we have

$$\det H > 0 \quad \text{for any } \tau \text{ and } \omega. \quad (\text{A25})$$

We then proceed with the study of the second-order derivative $\partial_g^2 R$ at the critical point P_0 . This is the first principal

minor of the Hessian matrix of Eq. (A19). It is easy to check the following chain of inequalities:

$$\begin{aligned} \partial_g^2 R &= \frac{1}{(\tau + \bar{\lambda})(\omega^2 - 1)} + \frac{f(\omega^{-1})}{4\omega} + \frac{(1-\tau)^2}{4\tau\bar{\lambda}} f(\tau\bar{\lambda}^{-1}) \\ &> \frac{1}{(\tau + \bar{\lambda})(\omega^2 - 1)} + \frac{f(\omega^{-1})}{4\omega} \\ &> \frac{1}{(\tau + \bar{\lambda})(\omega^2 - 1)} > 0, \quad \forall \omega > 1 \text{ and } 0 \leq \tau \leq 1. \end{aligned} \quad (\text{A26})$$

Therefore, the extremal point P_0 is an absolute minimum for the key rate of the no-switching protocol.

By contrast, we notice that the study described above is only valid for the pairs (g, g') for which it is possible to define the derivatives, i.e., those lying within the domain bounded by the constraints of Eq. (5). In order to complete our analysis we check that also the points at the boundary of the domain, described by Eq. (5), give a key rate which is larger than that one obtained for $g = g' = 0$. We have studied numerically these cases, computing the rate for the pairs (g, g') fulfilling the condition $\omega|g + g'| = \omega^2 + gg' - 1$. In Fig. 2 we show an example of this computation, corresponding to the case of a transmissivity $\tau \simeq 0.44$ and thermal noise $\omega = 1.3$, in shot-noise unit (SNU). We see that the rate for single-mode collective attack (red spot) lies well below the blue points, which describe the key rate for the boundary two-mode attacks. The colored region gives the values of the key rate for any nonzero correlations g, g' .

Clearly, similar results are obtained for any other value of $0 \leq \tau \leq 1$ and $\omega \geq 1$, with the area describing two-mode attacks vanishing into a point as $\omega \rightarrow 1$. In that case, the only possible attack is single mode and, according to Eq. (5), we have $g, g' \rightarrow 0$.

APPENDIX B: SWITCHING PROTOCOL

In this section, we analyze the key rate and its critical point for the switching protocol. We arrive at the same conclusion obtained for the no-switching protocol. In this case Bob performs homodyne detections on the received signals modes, by randomly switching the quadratures measured. Within each block c_j , Bob can decide to apply the same homodyne detection on both modes B, B' , or measure on two distinct bases (\hat{q} and \hat{p}). Here we assume the former case. When Bob detects both his modes in quadrature \hat{q} , we have

$$\begin{aligned} \mathbf{V}_C^q &= \mu \mathbf{I} - \frac{\tau(\mu^2 - 1)}{\bar{\Lambda}[g^2(1-\tau)^2 - \bar{\Lambda}^2]} \\ &\times \begin{pmatrix} 2g^2(1-\tau)^2 - \bar{\Lambda}^2 & & g(1-\tau)\bar{\Lambda} \\ & 1 & \\ g(1-\tau)\bar{\Lambda} & & \bar{\Lambda}^2 \\ & & & 1 \end{pmatrix}, \end{aligned} \quad (\text{B1})$$

where $\tilde{\Lambda} = \tau\mu + (1 - \tau)\omega = \Lambda - \tau$. When Bob detects both his modes in quadrature \hat{p} , we obtain

$$\mathbf{V}_C^p = \mu \mathbf{I} - \frac{\tau(\mu^2 - 1)}{\tilde{\Lambda}[g'^2(1 - \tau)^2 - \tilde{\Lambda}^2]} \times \begin{pmatrix} 1 & & & \\ & 2g'^2(1 - \tau)^2 - \tilde{\Lambda}^2 & & \\ & & 1 & \\ & g'(1 - \tau)\tilde{\Lambda} & & \tilde{\Lambda}^2 \end{pmatrix}. \quad (\text{B2})$$

In the first case (\hat{q} detection), for large μ , we obtain the following symplectic spectrum

$$\tilde{v}_{\pm} = \sqrt{\frac{(1 - \tau)(\omega \pm g)\mu}{\tau}}, \quad (\text{B3})$$

which depends on the correlation parameter g . In the second case (\hat{p} detection), we have the following symplectic eigenvalues:

$$\tilde{v}'_{\pm} = \sqrt{\frac{(1 - \tau)(\omega \pm g')\mu}{\tau}}, \quad (\text{B4})$$

depending on correlation parameter g' . From Eqs. (B3) and (B4), we compute two distinct conditional von Neumann entropies,

$$S_{E|\beta_q\beta'_q} = h(\tilde{v}_+) + h(\tilde{v}_-) \\ \stackrel{\mu \rightarrow \infty}{\approx} \log_2 \frac{e^2}{4} \frac{1 - \tau}{\tau} \sqrt{(\omega + g)(\omega - g)}\mu \quad (\text{B5})$$

and

$$S_{E|\beta_p\beta'_p} = h(\tilde{v}'_+) + h(\tilde{v}'_-) \\ \stackrel{\mu \rightarrow \infty}{\approx} \log_2 \frac{e^2}{4} \frac{1 - \tau}{\tau} \sqrt{(\omega + g')(\omega - g')}\mu. \quad (\text{B6})$$

To the conditional von Neumann entropy, we average over these two cases, getting the expression

$$S_{E|\beta\beta'} = \frac{S_{E|\beta_q\beta'_q} + S_{E|\beta_p\beta'_p}}{2} \\ = \log_2 \frac{e^2}{4} \frac{1 - \tau}{\tau} \sqrt{v_- v_+} \mu. \quad (\text{B7})$$

1. Key rate for the switching protocol

Using the total von Neumann entropy of Eq. (22), the conditional entropy of Eq. (B7), and the asymptotic expression of the mutual information for the switching protocol,

$$I_{AB} \rightarrow 2 \log_2 \frac{\tau\mu}{\tau + (1 - \tau)\omega}, \quad (\text{B8})$$

we compute the following expression of the key rate against Gaussian two-mode coherent attacks:

$$\tilde{R} = \frac{1}{2} \log_2 \frac{\sqrt{v_- v_+}}{(1 - \tau)[\tau + (1 - \tau)\omega]} - \frac{h(v_+) + h(v_-)}{2}, \quad (\text{B9})$$

from which we can recover the standard case of single-mode collective attack setting $g = g' = 0$.

For the sake of completeness, here we also discuss the case where Bob applies different homodyne detections (one in \hat{q} , the other in \hat{p}), within each two-mode block. In this case one finds a lower key rate because measurements have the effect of decorrelating modes B and B' . As a result, any dependency on g, g' is canceled from the conditional CM, and for $\mu \gg 1$ one finds the following doubly degenerate eigenvalues:

$$\tilde{v}_{1,2} = \sqrt{\frac{(1 - \tau)\omega\mu}{\tau}}. \quad (\text{B10})$$

After some algebra we obtain the following nonoptimal key rate

$$\bar{R} = \frac{1}{2} \log_2 \frac{\omega}{(1 - \tau)[\tau + (1 - \tau)\omega]} - \frac{h(v_+) + h(v_-)}{2}, \quad (\text{B11})$$

which is not interesting from a practical point of view, because the parties can always choose to group instances of the protocol with the same quadrature homodyned.

2. Study of the critical point for the switching protocol

We then compute the first derivatives of the rate in Eq. (B9), with respect to the correlations parameters g and g' , obtaining the following:

$$\partial_g \tilde{R} = \frac{\zeta}{4} \left[f(v_-^{-1}) + \frac{g}{(\omega + g)v_-} - \frac{v_+ v_- f(v_+^{-1})}{(\omega + g)(\omega - g')} \right], \quad (\text{B12})$$

$$\partial_{g'} \tilde{R} = \frac{\zeta'}{4} \left[f(v_-^{-1}) + \frac{g'}{(\omega + g')v_-} - \frac{v_+ v_- f(v_+^{-1})}{(\omega + g')(\omega - g)} \right], \quad (\text{B13})$$

where the function $f(\cdot)$ has been defined in Eq. (A21), and the symplectic eigenvalues v_{\pm} are given in Eqs. (A8) and (A9), while we defined ζ and ζ' as follows:

$$\zeta := \frac{v_-}{2(\omega - g')}, \quad \zeta' := \frac{v_-}{2(\omega - g)}. \quad (\text{B14})$$

Note that these derivatives are properly defined within the constraints of Eq. (5) that identify a sector of the (g, g') plane for which the conditions $v_- > 1$ and $v_+ > 1$ must hold. In fact, the situation for which one has $v_{\pm} = 1$ can only be obtained in P_0 , i.e., if the attack is collective. Solving the system of equations $\nabla R = 0$ one finds that P_0 is a critical point, and that it is also unique for any $\omega \geq 1$ and g and g' fulfilling Eq. (5).

3. Positive definiteness of the Hessian matrix

The second-order derivatives with respect to g , evaluated in P_0 , is given by

$$\partial_g^2 \tilde{R} = -\frac{\omega^2 + g^2}{4(\omega^2 - g^2)^2} + \frac{1}{8} \left[\frac{\kappa_+}{v_+^2 - 1} - \frac{\kappa_-}{v_-^2 - 1} \right] \\ + \frac{1}{8} \left[\frac{\sqrt{\kappa_+} f(v_+^{-1})}{\omega + g} - \frac{\sqrt{\kappa_-} f(v_-^{-1})}{\omega - g} \right], \quad (\text{B15})$$

with the coefficients κ_{\pm} defined as follows:

$$\kappa_{+} := \frac{\omega + g'}{\omega + g}, \quad \kappa_{-} := \frac{\omega - g'}{\omega - g}. \quad (\text{B16})$$

The derivative with respect to g' and the mixed derivatives are given by the expressions

$$\begin{aligned} \partial_{g'}^2 \tilde{R} &= -\frac{\omega^2 + g'^2}{4(\omega^2 - g'^2)^2} + \frac{1}{8} \left[\frac{\kappa_{+}^{-1}}{v_{+}^2 - 1} - \frac{\kappa_{-}^{-1}}{v_{-}^2 - 1} \right] \\ &\quad + \frac{1}{8} \left[\frac{f(v_{+}^{-1})}{\sqrt{\kappa_{+}(\omega + g')}} - \frac{f(v_{-}^{-1})}{\sqrt{\kappa_{-}(\omega - g')}} \right], \end{aligned} \quad (\text{B17})$$

$$\begin{aligned} \partial_{g',g}^2 \tilde{R} &= \partial_{g',g}^2 \tilde{R} \\ &= \frac{1}{8} \left[\frac{1}{v_{+}^2 - 1} - \frac{1}{v_{-}^2 - 1} + \frac{f(v_{+}^{-1})}{v_{+}} - \frac{f(v_{-}^{-1})}{v_{-}} \right], \end{aligned} \quad (\text{B18})$$

which, evaluated in P_0 , give

$$\partial_{g'}^2 \tilde{R} = \partial_{g'}^2 \tilde{R} = \frac{1}{4} \left(\frac{1}{\omega^2(\omega^2 - 1)} + \omega^{-1} f(\omega^{-1}) \right), \quad (\text{B19})$$

$$\partial_{g',g}^2 \tilde{R} = \partial_{g',g}^2 \tilde{R} = \frac{1}{4} \left(\frac{1}{\omega^2 - 1} - \omega^{-1} f(\omega^{-1}) \right). \quad (\text{B20})$$

We then compute the determinant of the Hessian in P_0 , obtaining the following expression:

$$\begin{aligned} \det H &= \partial_{g'}^2 \tilde{R} \times \partial_{g'}^2 \tilde{R} - (\partial_{g',g}^2 \tilde{R})^2 \\ &= \frac{(\omega^2 + 1)(2\omega f(\omega^{-1}) - 1)}{16\omega^4(\omega^2 - 1)}, \end{aligned} \quad (\text{B21})$$

which is always positive because

$$f(\omega^{-1}) > \frac{1}{\omega} \quad \text{for } \omega \geq 1. \quad (\text{B22})$$

We have also checked that $\det H > 0$ in the limit of $\omega \rightarrow 1^+$. Finally, we have verified that the second-order derivative of Eq. (B19) is positive in P_0 . In fact, for $\omega > 1$, one always has

$$\frac{1}{4} \left(\frac{1}{\omega^2(\omega^2 - 1)} + \omega^{-1} f(\omega^{-1}) \right) > 0. \quad (\text{B23})$$

Therefore, P_0 is a point of absolute minimum for the key rate of Eq. (B9), so that Eq. (29) is also verified for the switching protocol.

-
- [1] H. J. Kimble, *Nature (London)* **453**, 1023 (2008).
[2] S. Pirandola and S. L. Braunstein, *Nature (London)* **532**, 169 (2016).
[3] S. Pirandola *et al.*, *Nat. Photon.* **9**, 641 (2015).
[4] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, *Nat. Phys.* **11**, 713 (2015).
[5] G. Kurizki *et al.*, *Proc. Natl. Acad. Sci. USA* **112**, 3866 (2015).
[6] N. Gisin *et al.*, *Rev. Mod. Phys.* **74**, 145 (2002).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
[8] E. Diamanti and A. Leverrier, *Entropy* **17**, 6072 (2015).
[9] B. Schneier, *Applied Cryptography* (John Wiley & Sons, New York, 1996).
[10] C. Shannon, *Bell Syst. Tech. J.* **28**, 656 (1949).
[11] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[12] S. Pirandola, *Sci. Rep.* **4**, 6956 (2014).
[13] W. Wootters and W. Zurek, *Nature (London)* **299**, 802 (1982).
[14] S. L. Braunstein and P. van Loock, *Rev. Mod. Phys.* **77**, 513 (2005).
[15] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
[16] F. Grosshans *et al.*, *Nature (London)* **421**, 238 (2003).
[17] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
[18] P. Jouguet *et al.*, *Nat. Photon.* **7**, 378 (2013).
[19] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, *Phys. Rev. Lett.* **105**, 110501 (2010).
[20] V. C. Usenko and R. Filip, *Phys. Rev. A* **81**, 022318 (2010).
[21] C. Weedbrook, S. Pirandola, and T. C. Ralph, *Phys. Rev. A* **86**, 022318 (2012).
[22] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nat. Phys.* **4**, 726 (2008).
[23] C. Weedbrook, C. Ottaviani, and S. Pirandola, *Phys. Rev. A* **89**, 012309 (2014).
[24] C. Ottaviani, S. Mancini, and S. Pirandola, *Phys. Rev. A* **92**, 062323 (2015).
[25] C. Ottaviani and S. Pirandola, *Sci. Rep.* **6**, 22225 (2016).
[26] Y. Zhang, Z. Li, Y. Zhao, S. Yu, and H. Guo, *J. Phys. B* **50**, 035501 (2017).
[27] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *Nat. Photon.* **9**, 397 (2015).
[28] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, *Phys. Rev. A* **91**, 022320 (2015).
[29] S. Pirandola, C. Ottaviani, C. S. Jacobsen, G. Spedalieri, S. L. Braunstein, S. Lloyd, T. Gehring, and U. L. Andersen, *Nat. Photon.* **9**, 773 (2015).
[30] Z. Li, Y. C. Zhang, F. Xu, X. Peng, and H. Guo, *Phys. Rev. A* **89**, 052301 (2014).
[31] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
[32] G. Spedalieri, C. Ottaviani, S. L. Braunstein, T. Gehring, C. S. Jacobsen, U. L. Andersen, and S. Pirandola, *Proc. SPIE* **9648**, 96480Z (2015).
[33] R. Renner, *Nat. Phys.* **3**, 645 (2007).
[34] R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, 110504 (2009).
[35] I. Devetak and A. Winter, *Proc. R. Soc. London A* **461**, 207 (2005).

- [36] M. M. Wolf, G. Giedke, and J. I. Cirac, *Phys. Rev. Lett.* **96**, 080502 (2006).
- [37] S. Pirandola, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **101**, 200504 (2008).
- [38] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, *Proc. SPIE* **9996**, 999609 (2016).
- [39] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Quantum Inf. Comput.* **3**, 535 (2003).
- [40] S. Pirandola, *New J. Phys.* **15**, 113046 (2013).
- [41] A. Leverrier, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [42] G. Ruggeri and S. Mancini, *Phys. Lett. A* **362**, 340 (2007).
- [43] G. Spedalieri, C. Ottaviani, and S. Pirandola, *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).