Supplementary Information on the paper "Continuous variable quantum cryptography using two-way quantum communication"

Stefano Pirandola,[1] Stefano Mancini,[2] Seth Lloyd,[1, 3] and Samuel L. Braunstein[4]

[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge MA 02139, USA*
[2] *Dipartimento di Fisica & CNISM, Università di Camerino, Camerino 62032, Italy*
[3] *Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge MA 02139, USA*
[4] *Department of Computer Science, University of York, York YO10 5DD, United Kingdom*

(Dated: May 17, 2008)

In this document, we first review some basic information about Gaussian states. Then, we exhibit the general expressions for the secret-key rates (in both direct and reverse reconciliation) when the various protocols are subject to one-mode Gaussian attacks. In the following sections, we explicitly compute these secret-key rates for all the one-way and two-way protocols. From these quantities we derive the security thresholds shown in the main paper. Finally, in the last section, we give the explicit description of a general two-mode attack and we analyze the conditions for its reducibility. This last analysis shows the security of the hybrid protocols against collective Gaussian attacks.

I. BASICS OF GAUSSIAN STATES

A bosonic system of n modes can be described by a quadrature row-vector $\hat{\mathbf{Y}} := (\hat{Q}_1, \hat{P}_1, \ldots, \hat{Q}_n, \hat{P}_n)$ satisfying $[\hat{Y}_l, \hat{Y}_m] = 2i\Omega_{lm}$ $(1 \leq l, m \leq 2n)$, where

$$\mathbf{\Omega} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{1}$$

defines a symplectic form. A bosonic state ρ is called Gaussian if its statistics is Gaussian [1, 2]. In such a case, the state ρ is fully characterized by its displacement $\langle \hat{\mathbf{Y}} \rangle = \mathrm{Tr}(\hat{\mathbf{Y}}\rho)$ and correlation matrix (CM) $\mathbf{V}$, whose generic element is defined by $V_{lm} := \langle \hat{Y}_l \hat{Y}_m + \hat{Y}_m \hat{Y}_l \rangle/2 - \langle \hat{Y}_l \rangle \langle \hat{Y}_m \rangle$ with diagonal terms $V_{ll} = \langle \hat{Y}_l^2 \rangle - \langle \hat{Y}_l \rangle^2 := V(\hat{Y}_l)$ express the variances of the quadratures. According to Williamson's theorem [3], every CM $\mathbf{V}$ can be put in diagonal form by means of a symplectic transformation, i.e., there exists a matrix $\mathbf{S}$, satisfying $\mathbf{S}^T \mathbf{\Omega} \mathbf{S} = \mathbf{\Omega}$, such that $\mathbf{S}^T \mathbf{V} \mathbf{S} = \mathbf{\Delta}(\nu_1, \nu_1, \cdots, \nu_n, \nu_n)$, where $\mathbf{\Delta}$ denotes a diagonal matrix. The set of real values $\boldsymbol{\nu} := \{\nu_1, \cdots, \nu_n\}$ is called *symplectic eigenspectrum* of the CM and provides compact ways to express fundamental properties of the corresponding Gaussian state. In particular, the Von Neumann entropy $S(\rho) := -\mathrm{Tr}\,(\rho \log \rho)$ of a Gaussian state ρ can be expressed in terms of the symplectic eigenvalues by the formula [4]

$$S(\rho) = \sum_{k=1}^{n} g(\nu_k) \ , \tag{2}$$

where

$$\begin{aligned} g(\nu) &:= \tfrac{\nu+1}{2} \log \tfrac{\nu+1}{2} - \tfrac{\nu-1}{2} \log \tfrac{\nu-1}{2} \\ &\to \log \tfrac{e\nu}{2} + O(\nu^{-1}) \ \text{ for } \nu \gg 1 \ . \end{aligned} \tag{3}$$

Here, the information unit is the *bit* if $\log = \log_2$ or the *nat* if $\log = \ln$.

An example of a Gaussian state is the two-mode squeezed vacuum state [5] (or EPR source) whose CM takes the form

$$\mathbf{V}_{EPR}(V) = \begin{pmatrix} V\mathbf{I} & \sqrt{V^2-1}\mathbf{Z} \\ \sqrt{V^2-1}\mathbf{Z} & V\mathbf{I} \end{pmatrix}, \tag{4}$$

where $\mathbf{Z} := \mathbf{\Delta}(1, -1)$ and $\mathbf{I} := \mathbf{\Delta}(1, 1)$. In Eq. (4) the variance V fully characterizes the EPR source [5]. On the one hand, it quantifies the amount of entanglement which is distributed between Alice and Bob, providing a log-negativity [6] equal to

$$\begin{aligned} E_{\mathcal{N}} &= \max\left\{0, -\tfrac{1}{2}\log(2V^2 - 1 - 2V\sqrt{V^2-1})\right\} \\ &\to \log 2V + O(V^{-2}) \ \text{ for } V \gg 1 \ . \end{aligned} \tag{5}$$

On the other hand, it quantifies the amount of energy which is distributed to the parties, since the reduced thermal states $\rho_A := \mathrm{Tr}_B(\rho)$ and $\rho_B := \mathrm{Tr}_A(\rho)$ have mean excitation numbers equal to $(V-1)/2$.

II. GENERAL EXPRESSIONS FOR THE SECRET-KEY RATES

The various protocols differ for the number of paths (1 or 2) and the decoding method, which can be joint, disjoint, individual or collective. In particular, when decoding is disjoint the relevant secret variable X is $Q \in \mathbb{R}$ (or $P \in \mathbb{R}$, equivalently). When decoding is joint, the relevant secret variable X is $\{Q, P\} \in \mathbb{R}^2$. Under the assumption of one-mode Gaussian attacks, the individual protocols (Hom, Het, Hom^2, Het^2) have the following secret-key rates for DR (▶) and RR (◀) [7, 8]

$$R^{\blacktriangleright} := I(X_A : X_B) - I(X_A : E) \ , \tag{6}$$

$$R^{\blacktriangleleft} := I(X_A : X_B) - I(X_B : E) \ . \tag{7}$$

In these formulae, $I(X_A : X_B) := H(X_B) - H(X_B|X_A)$ is the classical mutual information between Alice and Bob's variables X_A and X_B, with $H(X_B) = (1/2)\log V(X_B)$

and $H(X_B|X_A) = (1/2)\log V(X_B|X_A)$ being the total and conditional Shannon entropies [9]. The term

$$I(X_K : E) := H(E) - H(E|X_K) \tag{8}$$

is the Holevo information [10] between Eve (E) and the honest user $K = A, B$ (i.e., Alice or Bob). Here, $H(E) := S(\rho_E)$ is the Von Neumann entropy of Eve's state ρ_E and $H(E|X_K)$ is the Von Neumann entropy conditioned to the classical communication of X_K. For the collective protocols $(\otimes Hom, \otimes Het, \otimes Hom^2, \otimes Het^2)$ we have instead

$$R^{\blacktriangleright} := I(X_A : B) - I(X_A : E) \ , \tag{9}$$

and

$$R^{\blacktriangleleft} := I(X_A : B) - I(B : E) \ , \tag{10}$$

where $I(X_A : B)$, $I(X_A : E)$ are Holevo informations, and

$$I(B : E) := H(B) + H(E) - H(B, E) \tag{11}$$

is the quantum mutual information between Bob and Eve. By setting $R = 0$ in the above Eqs. (6), (7), (9) and (10) one finds the security thresholds for the corresponding protocols. Notice that the Holevo information of Eq. (8) provides an upper bound to Eve's accessible information. In the case of collective protocols, Alice and Bob are able to reach the Holevo bound $I(X_A : B)$ only asymptotically. This is possible if Alice communicates to Bob the optimal collective measurement to be made compatible with the generated sequence of signal states and the detected noise in the channel. Such a measurement will be an asymptotic projection on the codewords of a random quantum code as foreseen by the Holevo–Schumacher–Westmoreland (HSW) theorem [11, 12]. Though such a measurement is highly complex, it is in principle possible and the study of the collective DR secret-key rate of Eq. (9) does make sense (it is also connected to the notion of private classical capacity of Ref. [13]). On the other hand, the quantum mutual information of Eq. (11) provides a bound which is too large in general, preventing a comparison between the collective protocols in RR.

III. SECRET-KEY RATES OF THE ONE-WAY PROTOCOLS

In the one-way protocols, Alice encodes two independent Gaussian variables Q_A, P_A in the quadratures $\hat{Q}_A, \hat{P}_A$ of a signal mode A, i.e., $\hat{Q}_A = Q_A + \hat{Q}_A|Q_A$ and $\hat{P}_A = P_A + \hat{P}_A|P_A$. Here, the quantum variables $\hat{Q}_A, \hat{P}_A$ have a global modulation V, given by the sum of the classical modulation $V(Q_A) = V(P_A) = V - 1$ and the quantum shot-noise $V(\hat{Q}_A|Q_A) = V(\hat{P}_A|P_A) = 1$. On the other hand, Eve has an EPR source $\mathbf{V}_{EPR}(W)$ which distributes entanglement between modes E and E''. The spy mode E is then mixed with the signal mode A via a beam splitter of transmission T, and the output modes, B and E', are received by Eve and Bob, respectively (see Fig. 1 in the main paper). Let us first consider the case of collective protocols $(\otimes Hom, \otimes Het)$, where Bob performs a coherent detection on all the collected modes B in order to decode $X_A = Q_A$ (for $\otimes Hom$) or $X_A = \{Q_A, P_A\}$ (for $\otimes Het$). For an arbitrary triplet $\{V, W, T\}$, the quadratures of the output modes, B and E', have variances

$$V(\hat{Q}_B) = V(\hat{P}_B) = (1-T)W + TV := b_V \ , \tag{12}$$

$$V(\hat{Q}_{E'}) = V(\hat{P}_{E'}) = (1-T)V + TW := e_V \ , \tag{13}$$

and conditional variances

$$V(\hat{Q}_B|Q_A) = V(\hat{P}_B|P_A) = (1-T)W + T = b_1 \ , \tag{14}$$

$$V(\hat{Q}_{E'}|Q_A) = V(\hat{P}_{E'}|P_A) = (1-T) + TW = e_1 \ . \tag{15}$$

Globally, the CMs of the output states ρ_B (of Bob), $\rho_{E'E''} := \rho_E$ (of Eve) and $\rho_{E'E''B} := \rho_{EB}$ (of Eve and Bob) are given by

$$\mathbf{V}_B(V, V) = \mathbf{\Delta}(b_V, b_V) \ , \tag{16}$$

$$\mathbf{V}_E(V, V) = \begin{pmatrix} \mathbf{\Delta}[e_V, e_V] & \varphi\mathbf{Z} \\ \varphi\mathbf{Z} & W\mathbf{I} \end{pmatrix} \ , \tag{17}$$

and

$$\mathbf{V}_{EB} = \begin{pmatrix} \mathbf{V}_E & \mathbf{F} \\ \mathbf{F}^T & \mathbf{V}_B \end{pmatrix} \ , \ \mathbf{F} := \begin{pmatrix} \mu\mathbf{I} \\ \theta\mathbf{Z} \end{pmatrix} \ , \tag{18}$$

where

$$\varphi := [T(W^2-1)]^{1/2} \ , \ \mu := (W-V)[(1-T)T]^{1/2} \ , \tag{19}$$

and

$$\theta := [(1-T)(W^2-1)]^{1/2} \ . \tag{20}$$

The CMs of Bob (B) and Eve (E), conditioned to Alice's variable X_A, are instead equal to

$$\mathbf{V}_{K|Q_A} = \mathbf{V}_K(1, V) \ , \ \mathbf{V}_{K|Q_A,P_A} = \mathbf{V}_K(1, 1) \ , \tag{21}$$

where $K = B, E$. For $T \neq 0, 1$ and $V \gg 1$, the symplectic spectra of all the previous CMs are given by:

$$\boldsymbol{\nu}_B \rightarrow \{TV\} \ , \tag{22}$$

$$\boldsymbol{\nu}_{B|Q_A} \rightarrow \{\sqrt{b_1 TV}\} \ , \tag{23}$$

$$\boldsymbol{\nu}_{B|Q_A,P_A} \rightarrow \{b_1\} \ , \tag{24}$$

$$\boldsymbol{\nu}_E \rightarrow \{(1-T)V, W\} \ , \tag{25}$$

$$\boldsymbol{\nu}_{E|Q_A} \rightarrow \{\sqrt{e_1(1-T)V}, \sqrt{Wb_1/e_1}\} \ , \tag{26}$$

$$\boldsymbol{\nu}_{E|Q_A,P_A} \rightarrow \{b_1, 1\} \ , \tag{27}$$

$$\boldsymbol{\nu}_{BE} \rightarrow \{V, 1, 1\} \ . \tag{28}$$

By using Eqs. (2) and (3), we then compute all the Von Neumann entropies to be used in the quantities $I(X_A :$

B), $I(X_A : E)$ and $I(B : E)$ of Eqs. (9) and (10). After some algebra we get the following asymptotic rates for the one-way collective protocols

$$R^{\blacktriangleright}[\otimes Het] = \log \tfrac{T}{1-T} - g(W) \ , \tag{29}$$

$$R^{\blacktriangleright}[\otimes Hom] = \tfrac{1}{2} \log \tfrac{Te_1}{(1-T)b_1} + g\left(\sqrt{\tfrac{Wb_1}{e_1}}\right) - g(W) \ , \tag{30}$$

and

$$R^{\blacktriangleleft}[\otimes Het] = \log \tfrac{1}{1-T} - g(W) - g(b_1) \ , \tag{31}$$

while $R^{\blacktriangleleft}[\otimes Hom] \rightarrow -\infty$, because of the too large bound provided by $I(B : E)$ in this case.

Let us now consider the individual one-way protocols (Hom, Het). Bob's output variable is $Q_B = \hat{Q}_B$ for Hom, and

$$\{Q_B, P_B\} = 2^{-1/2}\{\hat{Q}_B + \hat{Q}_0, \hat{P}_B - \hat{P}_0\} \tag{32}$$

for Het (with $\hat{Q}_0, \hat{P}_0$ belonging to the vacuum). From Eqs. (12) and (14), we can calculate the variances $V(X_B)$ and $V(X_B|X_A)$ that provide the non-computed term $I(X_A : X_B)$ in Eq. (6). Then, we get the following asymptotic rates in DR

$$R^{\blacktriangleright}[Hom] = R^{\blacktriangleright}[\otimes Hom] \ , \tag{33}$$

and

$$R^{\blacktriangleright}[Het] = \log \tfrac{2T}{e(1-T)(1+b_1)} + g(b_1) - g(W) \ . \tag{34}$$

In order to derive the RR rates from Eq. (7) we must evaluate

$$I(X_B : E) = H(E) - H(E|X_B) \ , \tag{35}$$

where $H(E|X_B)$ is computed from the spectrum $\boldsymbol{\nu}_{E|X_B}$ of the conditional CM $\mathbf{V}_{E|X_B}$. In RR, Eve's quantum variables

$$\hat{Y}_E := (\hat{Q}_{E'}, \hat{P}_{E'}, \hat{Q}_{E''}, \hat{P}_{E''}) \tag{36}$$

must be conditioned to the Bob's classical variable X_B. This is equivalent to constructing, from X_B, the *optimal* linear estimators $\hat{Y}_E^{(X_B)}$ of $\hat{Y}_E$, in such a way that the residual conditional variables

$$\hat{Y}_E|X_B := \hat{Y}_E - \hat{Y}_E^{(X_B)} \tag{37}$$

have minimal entropy $H(E|X_B)$. For the Hom protocol, Bob's variable $X_B = Q_B$ can be used to estimate the $\hat{Q}$ quadratures only. Then, let Bob estimate $\hat{Y}_E$ by

$$\hat{Y}_E^{(Q_B)} = (q'Q_B, 0, q''Q_B, 0) \ , \tag{38}$$

so that the conditional variables are given by

$$\hat{Y}_E|Q_B = (\hat{Q}_{E'} - q'Q_B, \hat{P}_{E'}, \hat{Q}_{E''} - q''Q_B, \hat{P}_{E''}) \ . \tag{39}$$

For $T \neq 0, 1$ and $V \gg 1$, the optimal estimators are given by

$$q' = -\sqrt{(1-T)/T} \ , \tag{40}$$

and $q'' = 0$. The corresponding conditional spectrum

$$\boldsymbol{\nu}_{E|Q_B} \rightarrow \{\sqrt{VW(1-T)/T}, 1\} \tag{41}$$

minimizes $H(E|Q_B)$ and leads to the asymptotic rate

$$R^{\blacktriangleleft}[Hom] = \tfrac{1}{2} \log \tfrac{W}{(1-T)b_1} - g(W) \ . \tag{42}$$

For the Het protocol, Bob's variable $X_B = \{Q_B, P_B\}$ enables him to estimate both the $\hat{Q}$ and $\hat{P}$ quadrature, by constructing the $\hat{Y}_E$-linear estimator

$$\hat{Y}_E^{(Q_B, P_B)} = (q'Q_B, p'P_B, q''Q_B, p''P_B) \ . \tag{43}$$

For $T \neq 0, 1$ and $V \gg 1$, the optimal choice corresponds to

$$q' = p' = -\sqrt{2(1-T)/T} \ , \tag{44}$$

and $q'' = p'' = 0$, which gives

$$\boldsymbol{\nu}_{E|Q_B, P_B} \rightarrow \{(1 - T + b_1)/T, 1\} \ , \tag{45}$$

and leads to the asymptotic rate

$$R^{\blacktriangleleft}[Het] = \log \tfrac{2T}{e(1-T)(1+b_1)} + g\left(\tfrac{1-T+b_1}{T}\right) - g(W) \ . \tag{46}$$

IV. SECRET-KEY RATES OF THE TWO-WAY PROTOCOLS

In the EPR formulation of the two-way protocols (see Fig. 5 in the main paper), Bob assists the encoding via an EPR source $\mathbf{V}_{EPR}(V)$ that distributes entanglement between mode B_1, which is kept, and mode C_1, which is sent in the channel and undergoes the action of an entangling cloner $(T, W) : C_1 \rightarrow A_1$. On the perturbed mode A_1, Alice performs a Gaussian modulation by adding a stochastic amplitude $\alpha = (Q_A + iP_A)/2$ with $V(Q_A) = V(P_A) = \bar{V}$ and $\langle Q_A P_A \rangle = 0$. The modulated mode A_2 is then sent back through the channel, where it undergoes the action of a second entangling cloner $(T, W) : A_2 \rightarrow B_2$, where the output mode B_2 is finally received by Bob. Let us first consider the collective two-way protocols $(\otimes Hom^2, \otimes Het^2)$, where Bob performs an optimal coherent measurement upon all the collected modes B_1, B_2 in order to decode $X_A = Q_A$ (for $\otimes Hom^2$) or $X_A = \{Q_A, P_A\}$ (for $\otimes Het^2$). For an arbitrary quadruplet $\{\bar{V}, V, W, T\}$, the CMs of the output states $\rho_{B_1 B_2} := \rho_B$ (of Bob) and $\rho_{E_1' E_1'' E_2' E_2''} := \rho_E$ (of Eve) are given by

$$\mathbf{V}_B(\bar{V}, \bar{V}) = \begin{pmatrix} V\mathbf{I} & T\sqrt{V^2 - 1}\mathbf{Z} \\ T\sqrt{V^2 - 1}\mathbf{Z} & \mathbf{\Lambda}_B(\bar{V}, \bar{V}) \end{pmatrix} \ , \tag{47}$$

and

$$\mathbf{V}_E(\bar{V},\bar{V}) = \begin{pmatrix} e_V\mathbf{I} & \varphi\mathbf{Z} & \mu'\mathbf{I} & \mathbf{0} \\ \varphi\mathbf{Z} & W\mathbf{I} & \theta'\mathbf{Z} & \mathbf{0} \\ \mu'\mathbf{I} & \theta'\mathbf{Z} & \mathbf{\Lambda}_E(\bar{V},\bar{V}) & \varphi\mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \varphi\mathbf{Z} & W\mathbf{I} \end{pmatrix} , \quad (48)$$

where

$$\mathbf{\Lambda}_B(\bar{V},\bar{V}) := [T^2V + (1-T^2)W]\mathbf{I} + T\mathbf{\Delta}(\bar{V},\bar{V}) , \quad (49)$$

and

$$\mathbf{\Lambda}_E(\bar{V},\bar{V}) := \gamma\mathbf{I} + (1-T)\mathbf{\Delta}(\bar{V},\bar{V}) , \quad (50)$$

with

$$\mu' := -\sqrt{1-T}\mu \ , \ \theta' := -\sqrt{1-T}\theta , \quad (51)$$

and

$$\gamma := T(1-T)V + (1-T)^2W + TW . \quad (52)$$

The CMs of Bob (B) and Eve (E), conditioned to Alice's variable X_A, are instead equal to

$$\mathbf{V}_{K|Q_A} = \mathbf{V}_K(0,\bar{V}) \ , \ \mathbf{V}_{K|Q_A,P_A} = \mathbf{V}_K(0,0) , \quad (53)$$

for $K = B, E$. Let us consider identical resources between Alice and Bob, i.e., $\bar{V} = V - 1$. Then, for $T \neq 0, 1$ and $V \gg 1$, all the symplectic spectra are given by:

$$\begin{aligned} \boldsymbol{\nu}_B &\rightarrow \{f_1V, f_2V\} , & (54) \\ \boldsymbol{\nu}_{B|Q_A} &\rightarrow \{\varsigma V, \varsigma^{-1}\sqrt{T(1-T^2)WV}\} , & (55) \\ \boldsymbol{\nu}_{B|Q_A,P_A} &\rightarrow \{(1-T^2)V, W\} , & (56) \\ \boldsymbol{\nu}_E &\rightarrow \{h_1V, h_2V, W, W\} , & (57) \\ \boldsymbol{\nu}_{E|Q_A} &\rightarrow \{\upsilon(1-T)V, \tfrac{\sqrt{(1-T^2)WV}}{\upsilon}, W, 1\} , & (58) \\ \boldsymbol{\nu}_{E|Q_A,P_A} &\rightarrow \{(1-T^2)V, W, 1, 1\} , & (59) \end{aligned}$$

where $f_1f_2 = T$, $h_1h_2 = (1-T)^2$ and

$$\varsigma := [1+T^2(T^2+T-2)]^{1/2} \ , \ \upsilon := [1+3T+T^2]^{1/2} . \quad (60)$$

By means of Eqs. (2) and (3), we compute all the Von Neumann entropies to be used in Eq. (9), and we get the asymptotic rates

$$R^{\blacktriangleright}[\otimes Hom^2] = \tfrac{1}{2}\log\tfrac{T}{(1-T)^2} - g(W) , \quad (61)$$

and

$$R^{\blacktriangleright}[\otimes Het^2] = 2R^{\blacktriangleright}[\otimes Hom^2] . \quad (62)$$

Clearly these rates imply the same DR threshold $N^{\blacktriangleright} = N^{\blacktriangleright}(T)$ for $\otimes Hom^2$ and $\otimes Het^2$, as is shown in Fig. 2 in the main paper. The derivation of $R^{\blacktriangleleft}[\otimes Het^2]$ and $R^{\blacktriangleleft}[\otimes Hom^2]$ is here omitted because of the trivial negative divergence caused by $I(B:E)$.

Let us now consider the individual two-way protocols Hom^2 and Het^2 in DR. For the Hom^2 protocol, Bob decodes Q_A by constructing the output variable $Q_B := Q_{B_2} - TQ_{B_1}$ from the measurements of $\hat{Q}_{B_1}$ and $\hat{Q}_{B_2}$. In fact, since $\hat{Q}_{B_1} \rightarrow \hat{Q}_{C_1}$ (for $V \gg 1$) and

$$\hat{Q}_{B_2} = \sqrt{T}Q_A + T\hat{Q}_{C_1} + \sqrt{1-T}(\sqrt{T}\hat{Q}_{E_1} + \hat{Q}_{E_2}) , \quad (63)$$

we asymptotically have

$$Q_B \rightarrow \sqrt{T}Q_A + \delta Q , \quad (64)$$

with

$$\delta Q := \sqrt{1-T}(\sqrt{T}\hat{Q}_{E_1} + \hat{Q}_{E_2}) . \quad (65)$$

From $V(Q_B)$ and $V(Q_B|Q_A)$ we easily compute $I(Q_A : Q_B)$ to be used in Eq. (6). It is then easy to check that the asymptotic DR rate satisfies

$$R^{\blacktriangleright}[Hom^2] = R^{\blacktriangleright}[\otimes Hom^2] . \quad (66)$$

For the Het^2 protocol, Bob measures

$$\begin{cases} \hat{q}_- = 2^{-1/2}(\hat{Q}_{B_1} - \hat{Q}_0) , \\ \hat{p}_+ = 2^{-1/2}(\hat{P}_{B_1} + \hat{P}_0) , \end{cases} \quad (67)$$

from the first heterodyne on B_1, and

$$\begin{cases} \hat{Q}_- = 2^{-1/2}(\hat{Q}_{B_2} - \hat{Q}_{0'}) , \\ \hat{P}_+ = 2^{-1/2}(\hat{P}_{B_2} + \hat{P}_{0'}) , \end{cases} \quad (68)$$

from the second one upon B_2. Then, Bob decodes $\{Q_A, P_A\}$ via the variables

$$\begin{cases} Q_B := Q_- - Tq_- , \\ P_B := P_+ + Tp_+ . \end{cases} \quad (69)$$

In fact, for $T \neq 0, 1$ and $V \gg 1$, we have

$$Q_B \rightarrow \sqrt{T/2}Q_A + \delta Q' \ , \ P_B \rightarrow \sqrt{T/2}P_A + \delta P , \quad (70)$$

with

$$\delta Q' := 2^{-1/2}(\delta Q + T\hat{Q}_0 - \hat{Q}_{0'}) , \quad (71)$$

and

$$\delta P := 2^{-1/2}[\sqrt{1-T}(\sqrt{T}\hat{P}_{E_1} + \hat{P}_{E_2}) + T\hat{P}_0 + \hat{P}_{0'}] . \quad (72)$$

From $V(X_B) = V(Q_B)V(P_B)$ and $V(X_B|X_A) = V(Q_B|Q_A)V(P_B|P_A)$ we then compute $I(X_A : X_B)$ and the consequent asymptotic DR rate

$$R^{\blacktriangleright}[Het^2] = \log\tfrac{2T(1+T)}{e(1-T)[1+T^2+(1-T^2)W]} - g(W) . \quad (73)$$

Let us now consider Hom^2 and Het^2 in RR. In order to derive the corresponding rates from Eq. (7), we must again compute $H(E|X_B)$ from the spectrum of the conditional CM $\mathbf{V}_{E|X_B}$, where Eve's quantum variables

$$\hat{Y}_E := (\hat{Q}_{E_1'}, \hat{P}_{E_1'}, \hat{Q}_{E_1''}, \hat{P}_{E_1''}, \hat{Q}_{E_2'}, \hat{P}_{E_2'}, \hat{Q}_{E_2''}, \hat{P}_{E_2''}) \quad (74)$$

are conditioned to Bob's output variable X_B. Of course, this is again equivalent to finding the optimal linear estimators $\hat{Y}_E^{(X_B)}$ of $\hat{Y}_E$. For the Hom^2 protocol where $X_B = Q_B$, the linear estimators of $\hat{Y}_E$ take the form

$$\hat{Y}_E^{(Q_B)} := (q_1' Q_B, 0, q_1'' Q_B, 0, q_2' Q_B, 0, q_2'' Q_B, 0) \ . \quad (75)$$

For $T \neq 0, 1$ and $V \gg 1$, the optimal ones are given by $q_1' = q_1'' = q_2'' = 0$ and $q_2' = -\sqrt{(1-T)/T}$. The corresponding conditional spectrum is given by

$$\boldsymbol{\nu}_{E|Q_B} \rightarrow \{m_1 V, m_2 \sqrt{V}, W, 1\} \ , \quad (76)$$

with

$$m_1 m_2 = [T^{-1}(1-T)^3(1+T^3)W]^{1/2} \ . \quad (77)$$

This leads to the asymptotic rate

$$R^{\blacktriangleleft}[Hom^2] = \tfrac{1}{2} \log \tfrac{1-T+T^2}{(1-T)^2} - g(W) \ . \quad (78)$$

For the Het^2 protocol, where $X_B = \{Q_B, P_B\}$, we have

$$\hat{Y}_E^{(Q_B,P_B)} := \\ (q_1' Q_B, p_1' P_B, q_1'' Q_B, p_1'' P_B, q_2' Q_B, p_2' P_B, q_2'' Q_B, p_2'' P_B) \ . \quad (79)$$

For $T \neq 0, 1$ and $V \gg 1$, the optimal estimators are given by

$$q_2' = p_2' = -\sqrt{2(1-T)/T} \ , \quad (80)$$

and

$$q_1' = p_1' = q_1'' = p_1'' = q_2'' = p_2'' = 0 \ . \quad (81)$$

The corresponding conditional spectrum is given by

$$\boldsymbol{\nu}_{E|Q_B,P_B} \rightarrow \{n_1, n_2, n_3, (1-T^2)V\} \ ,$$

where

$$n_1 n_2 n_3 = \frac{[1 + T^3 + (1-T)(1+T^2)W]W}{T(1+T)} \ . \quad (82)$$

This spectrum leads to the final asymptotic rate

$$R^{\blacktriangleleft}[Het^2] = \log \tfrac{2T(1+T)}{e(1-T)[1+T^2+(1-T^2)W]} \\ + \sum_{i=1}^{3} g(n_i) - 2g(W) \ . \quad (83)$$

V. STRUCTURE OF TWO-MODE ATTACKS

Let us describe the effects of a general two-mode attack when Alice and Bob adopt the hybrid protocol. In the hybrid protocol, Bob sends a modulated pure state $|\varphi\rangle_B$, which is coherent for $Het^{1,2}$ and squeezed for $Hom^{1,2}$. Then, Alice modulates this state by α in the ON configuration, while she detects $|\varphi\rangle_B$ and re-sends a new $|\varphi'\rangle_A$ in the OFF configuration. In general, in a two-mode attack, Eve can use a countable set of ancillas which can always be partitioned in three blocks $\mathbf{E} = \{E_1, F, E_2\}$ (see Fig. 1). However, such an attack can always be reduced to the cascade form of Fig. 2. This is a trivial consequence of the logical structure of the protocol, where the backward path (labelled by 2) is always subsequent to the forward path (labelled by 1) and, therefore, a first unitary interaction $\hat{U}$ can condition a second one $\hat{V}$, but the contrary is not possible. In the first unitary $\hat{U}$, two blocks of ancillas E_1 and F interact with the forward path (1). One output E_1 is sent to the final coherent detection while the other one F is taken as input for the second unitary $\hat{V}$. Such a unitary makes the backward path (2) interact with F (coming from $\hat{U}$) and another block of fresh ancillas E_2. The corresponding outputs of F and E_2 are then sent to the final coherent detection. Note that such a description contains all the possible quantum and/or classical correlations that Eve can create between the forward and backward paths

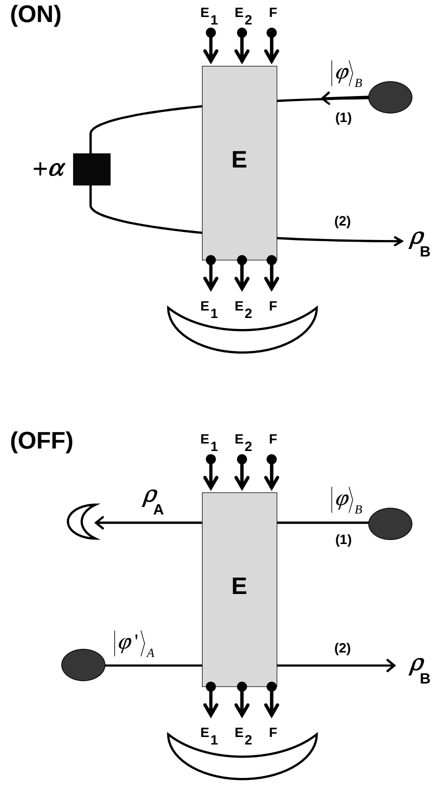

FIG. 1: General two-mode attack against a hybrid protocol (displayed in both the ON and OFF configuration). The two paths of the quantum communication interact with a supply of ancillas that can always be divided into three blocks E_1, E_2 and F.

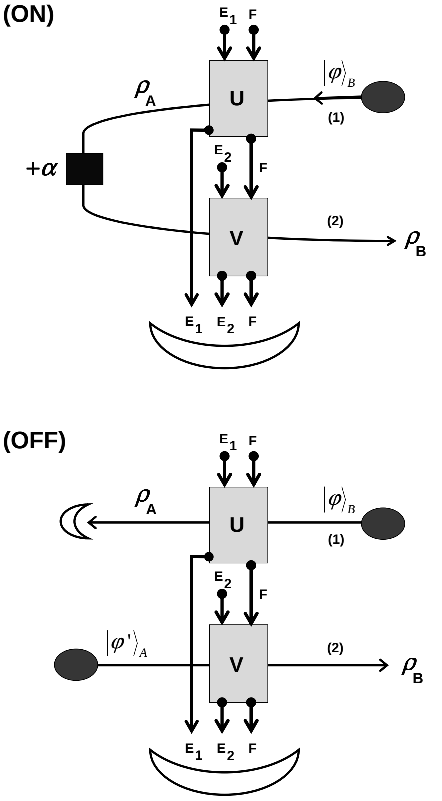

FIG. 2: Cascade form of the two-mode attack. In the first unitary $\hat{U}$, two blocks of ancillas E_1 and F interact with the forward path (labelled by 1). One output E_1 is sent to the final coherent detection while the other one F is taken as input for the second unitary $\hat{V}$. Such a unitary makes the backward path (labelled by 2) interact with F (coming from $\hat{U}$) and another block of fresh ancillas E_2. The corresponding outputs of F and E_2 are then sent to the final coherent detection.

(both Gaussian and non-Gaussian).

In the OFF configuration, the first channel $\mathcal{E}_1 : |\varphi\rangle_B \langle\varphi| \rightarrow \rho_A$ is described by the Stinespring dilation [14]

$$\mathcal{E}_1(|\varphi\rangle_B \langle\varphi|) = \mathrm{Tr}_{E_1F}\left[\hat{U}_{BE_1F}\left(|\varphi\rangle_B \langle\varphi| \right.\right. \\ \left.\left. \otimes |0\rangle_{E_1} \langle 0| \otimes |0\rangle_F \langle 0|\right) \hat{U}^{\dagger}_{BE_1F}\right] , \quad (84)$$

while the second channel $\mathcal{E}_2 : |\varphi'\rangle_A \langle\varphi'| \rightarrow \rho_B$ can be expressed by the physical representation [15]

$$\mathcal{E}_2(|\varphi'\rangle_A \langle\varphi'|) = \mathrm{Tr}_{E_2F}\left[\hat{V}_{AE_2F}\left(|\varphi'\rangle_A \langle\varphi'| \right.\right. \\ \left.\left. \otimes\rho_F \otimes |0\rangle_{E_2} \langle 0|\right) \hat{V}^{\dagger}_{AE_2F}\right] , \quad (85)$$

where

$$\rho_F = \mathrm{Tr}_{BE_1}\left[\hat{U}_{BE_1F}\left(|\varphi\rangle_B \langle\varphi| \right.\right. \\ \left.\left. \otimes |0\rangle_{E_1} \langle 0| \otimes |0\rangle_F \langle 0|\right) \hat{U}^{\dagger}_{BE_1F}\right] \quad (86)$$

is the (generally mixed) state coming from the attack of the first channel. In the ON configuration, the global map $\mathcal{E}^2 : |\varphi\rangle_B \langle\varphi| \rightarrow \rho_B$ is equal to

$$\mathcal{E}^2(|\varphi\rangle_B \langle\varphi|) = \mathrm{Tr}_{\mathbf{E}}\left[\hat{V}_{B\mathbf{E}}\left(|\varphi\rangle_B \langle\varphi| \otimes |0\rangle_{\mathbf{E}} \langle 0|\right) \hat{V}^{\dagger}_{B\mathbf{E}}\right] , \quad (87)$$

where $|0\rangle_{\mathbf{E}} \langle 0| := |0\rangle_{E_1} \langle 0| \otimes |0\rangle_{E_2} \langle 0| \otimes |0\rangle_F \langle 0|$ and

$$\hat{V}_{B\mathbf{E}} := \hat{V}_{BE_2F}\hat{D}_B(\alpha)\hat{U}_{BE_1F} \ . \quad (88)$$

Notice that the Stinespring dilation of Eq. (87) is *unique* up to a local unitary transformation $\hat{U}_{\mathbf{E}}$ acting on the output ancilla modes. In our description of the attack (see Fig. 2) such a local unitary is included in the optimization of the final coherent detection.

From Eq. (88), it is clear that Eve's attack is void of *quantum correlations* if

$$\hat{V}_{BE_2F} = \hat{V}_{BE_2} \otimes \hat{V}_F \ , \quad (89)$$

or

$$\hat{U}_{BE_1F} = \hat{U}_{BE_1} \otimes \hat{U}_F \ . \quad (90)$$

In such a case in fact the two unitaries $\hat{U}$ and $\hat{V}$ are no longer coupled by the F ancillas. Let us assume one of the incoherence conditions of Eq. (89) and (90). Then, we can group the ancillas into two disjoint blocks $\mathbf{E}_1 = \{E_1, F\}$ and $\mathbf{E}_2 = \{E_2\}$ if Eq. (89) holds, or $\mathbf{E}_1 = \{E_1\}$ and $\mathbf{E}_2 = \{E_2, F\}$ if Eq. (90) holds. In both cases the one-mode channels of Eqs. (84) and (85) are expressed by the Stinespring dilations

$$\mathcal{E}_1(|\varphi\rangle_B \langle\varphi|) = \mathrm{Tr}_{\mathbf{E}_1}\left[\hat{U}_{B\mathbf{E}_1}\left(|\varphi\rangle_B \langle\varphi| \otimes |0\rangle_{\mathbf{E}_1} \langle 0|\right) \hat{U}^{\dagger}_{B\mathbf{E}_1}\right] , \quad (91)$$

and

$$\mathcal{E}_2(|\varphi'\rangle_A \langle\varphi'|) = \mathrm{Tr}_{\mathbf{E}_2}\left[\hat{V}_{A\mathbf{E}_2}\left(|\varphi'\rangle_A \langle\varphi'| \right.\right. \\ \left.\left. \otimes |0\rangle_{\mathbf{E}_2} \langle 0|\right) \hat{V}^{\dagger}_{A\mathbf{E}_2}\right] , \quad (92)$$

while the two-mode channel $\mathcal{E}^2$ is expressed by Eq. (87) with

$$\hat{V}_{B\mathbf{E}} := \hat{V}_{B\mathbf{E}_2}\hat{D}_B(\alpha)\hat{U}_{B\mathbf{E}_1} \ . \quad (93)$$

Now, one can easily check that Eq. (93) is equivalent to the decomposability condition

$$\mathcal{E}^2 = \mathcal{E}_2 \circ \mathcal{E}_\alpha \circ \mathcal{E}_1 \ . \quad (94)$$

This can be easily verified by inserting Eqs. (91) and (92) into the right hand side of Eq. (94) and resorting to the uniqueness property of the Stinespring dilation.

Once the presence of quantum correlations between the paths has been excluded, every residual classical correlation can be excluded by symmetrizing the forward and backward channels, i.e., by setting $\mathcal{E}_1 = \mathcal{E}_2$, which is equivalent to relating the two unitaries $\hat{U}$ and $\hat{V}$ by a partial isometry. In conclusion, the verification of the condition $\mathcal{E}^2 = \mathcal{E} \circ \mathcal{E}_\alpha \circ \mathcal{E}$ by Alice and Bob explicitly excludes every sort of quantum/classical correlation between the two paths of the quantum communication. Moreover, such a verification is relatively easy in case of Gaussian attacks, since the corresponding Gaussian channels can be completely reconstructed from the analysis of the first two statistical moments.

[1] Eisert, J. & Plenio, M. B. Introduction to the basics of entanglement theory in continuous-variable systems. *Int. J. Quant. Inf.* **1**, 479–506 (2003).

[2] Ferraro, A., Olivares, S. & Paris, M. G. A. Gaussian states in quantum information (Bibliopolis, Napoli, 2005).

[3] Williamson, J. On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems. *Am. J. Math.* **58**, 141-163 (1936).

[4] Holevo, A. S., Sohma, M. & Hirota, O. Capacity of quantum Gaussian channels. *Phys. Rev. A* **59**, 1820–1828 (1999).

[5] Walls, D. F. & Milburn, G. J. Quantum Optics (Springer, 1994).

[6] Vidal, G. & Werner, R. F. Computable measure of entanglement. *Phys. Rev. A* **65**, 032314 (2002).

[7] Devetak, I & Winter, A. Relating Quantum Privacy and Quantum Coherence: An Operational Approach. *Phys. Rev. Lett.* **93**, 080501 (2004);

[8] Devetak, I & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461**, 207-235 (2005).

[9] Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 623–656 (1948).

[10] Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Inf. Transm.* **9**, 177-183 (1973).

[11] Holevo, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**, 269-273 (1998).

[12] Schumacher, B. & Westmoreland, M. D. Sending classical information via noisy quantum channels. *Phys. Rev. A*, **56**, 131-138 (1997).

[13] Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Th.* **51**, 44–55 (2005).

[14] Stinespring, W. F. Positive functions on C*-algebras. *Proc. Am. Math. Soc.* **6**, 211-216 (1955).

[15] Holevo, A. S. On the mathematical theory of quantum communication channels. *Probl. Inform. Transm.* **8**, 47-56 (1972).