On the Security and Degradability of Gaussian Channels

On the security and degradability of Gaussian channels

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

[1]*Research Laboratory of Electronics, MIT, Cambridge MA 02139, USA*
[2]*Department of Computer Science, University of York, York YO10 5DD, UK*
[3]*Department of Mechanical Engineering, MIT, Cambridge MA 02139, USA*

(Dated: February 19, 2013)

We consider the notion of canonical attacks, which are the cryptographic analog of the canonical forms of a one-mode Gaussian channel. Using this notion, we explore the connections between the degradability properties of the channel and its security for quantum key distribution. Finally, we also show some relations between canonical attacks and optimal Gaussian cloners.

I. INTRODUCTION

Today, quantum cryptography is one of the most promising areas in quantum information science. This is particularly true in the framework of continuous variable (CV) systems [1], which are quantum systems characterized by infinite-dimensional Hilbert spaces. The increasing interest in CV quantum cryptography is mainly due to the practical advantages of quantum key distribution (QKD) using Gaussian states [2, 3, 4, 5, 6]. Furthermore, this Gaussian QKD has been also extended to multiple quantum communications [7] and the non-trivial possibility of a quantum direct communication has been also explored [8]. Very recently, a new insight in the theory of quantum channels has been provided by the canonical classification of the one-mode Gaussian channels [9] (see also Refs. [10, 11] and the *compact version* of this classification in Ref. [5]). These channels have been proven to be unitarily equivalent to canonical forms of six different classes [9], whose degradability properties have been also studied [11]. Here, we exploit these concepts in the scenario of quantum cryptography. In particular, we consider the notion of canonical attacks as the cryptographic analog of the canonical forms. By adopting the individual version of these canonical attacks, we explore the connections between the degradability properties of the channel and its security for QKD. Then, we also show when (and in what sense) these attacks can be considered equivalent to individual attacks using optimal Gaussian cloners.

II. QUANTUM COMMUNICATION SCENARIO

The simplest continuous variable system is a single bosonic mode, i.e., a quantum system described by a pair of quadrature operators $\hat{\mathbf{x}}^T := (\hat{q}, \hat{p})$ with $[\hat{q}, \hat{p}] = 2i$. In particular, a single-mode bosonic state ρ with Gaussian statistics is called *Gaussian state* and it is completely characterized by a 2×2 covariance matrix $\mathbf{V}$ plus a displacement vector $\bar{\mathbf{x}} \in \mathbb{R}^2$. Then, a one-mode Gaussian channel is a completely positive trace-preserving (CPT) map $\mathcal{G}(\mathbf{T}, \mathbf{N}, \mathbf{d})$ transforming an input Gaussian state $\rho_a(\mathbf{V}_a, \bar{\mathbf{x}}_a)$ of a sender (Alice) into an output Gaussian state $\rho_b(\mathbf{V}_b, \bar{\mathbf{x}}_b)$ of a receiver (Bob) via the relations $\mathbf{V}_b = \mathbf{T}\mathbf{V}_a\mathbf{T}^T + \mathbf{N}$ and $\bar{\mathbf{x}}_b = \mathbf{T}\bar{\mathbf{x}}_a + \mathbf{d}$. Here, $\mathbf{d} \in \mathbb{R}^2$ and $\mathbf{T}, \mathbf{N}$ are 2×2 real matrices, with $\mathbf{N}^T = \mathbf{N} > 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2$. Up to unitaries on the input and the output, every one-mode Gaussian channel is equivalent to a map $\mathcal{C}$, called the *canonical form*, which is a Gaussian channel with $\mathbf{d} = \mathbf{0}$ and $\mathbf{T}_c, \mathbf{N}_c$ diagonal [9]. According to Ref. [5], the explicit expressions of $\mathbf{T}_c$ and $\mathbf{N}_c$ depend on three symplectic invariants of the channel: the generalized *transmission* $\tau := \det \mathbf{T}$ (ranging from $-\infty$ to $+\infty$), the *rank* $r := [\mathrm{rk}(\mathbf{T})\mathrm{rk}(\mathbf{N})]/2$ (with possible values $r = 0, 1, 2$) and the *temperature* $\bar{n}$ (which is a positive number related to $\det \mathbf{N}$ [5]). These three invariants $\{\tau, r, \bar{n}\}$ completely characterize the two matrices $\mathbf{T}_c, \mathbf{N}_c$ and, therefore, the corresponding canonical form $\mathcal{C} = \mathcal{C}(\tau, r, \bar{n})$. In particular, the first two invariants $\{\tau, r\}$ determine the class of the form [5, 9]. The full classification is explicitly shown in the following table

τ	r	Class	Form	$\mathbf{T}_c$	$\mathbf{N}_c$
0	0	A_1	$\mathcal{C}(0,0,\bar{n})$	$\mathbf{0}$	$(2\bar{n}+1)\mathbf{I}$
0	1	A_2	$\mathcal{C}(0,1,\bar{n})$	$\frac{\mathbf{I}+\mathbf{Z}}{2}$	$(2\bar{n}+1)\mathbf{I}$
1	1	B_1	$\mathcal{C}(1,1,0)$	$\mathbf{I}$	$\frac{\mathbf{I}-\mathbf{Z}}{2}$
1	2	B_2	$\mathcal{C}(1,2,\bar{n})$	$\mathbf{I}$	$\bar{n}\mathbf{I}$
1	0	$B_2(Id)$	$\mathcal{C}(1,0,0)$	$\mathbf{I}$	$\mathbf{0}$
$(0,1)$	2	$C(Att)$	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$
>1	2	$C(Amp)$	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(\tau-1)(2\bar{n}+1)\mathbf{I}$
<0	2	D	$\mathcal{C}(\tau,2,\bar{n})$	$\sqrt{-\tau}\mathbf{Z}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$

In this table, the values of $\{\tau, r\}$ in the first two columns specify a particular class A_1, A_2, B_1, B_2, C and D [12]. Within each class, the possible canonical forms are expressed in the third column, where also the third invariant $\bar{n}$ must be considered. The corresponding expressions of $\mathbf{T}_c, \mathbf{N}_c$ are shown in the last two columns, where $\mathbf{Z} := \mathrm{diag}(1, -1)$, $\mathbf{I} := \mathrm{diag}(1, 1)$ and $\mathbf{0}$ is the zero matrix.

By adopting a Stinespring dilation of the quantum channel, we can describe a canonical form $\mathcal{C}(\tau, r, \bar{n})$ via a symplectic transformation $\mathbf{M}_{ae\tilde{e}}$ mixing the input signal mode $\{a\}$ with two vacuum environmental modes $\{e, \tilde{e}\}$ and yielding the output modes $\{b\}$ for Bob and $\{c, \tilde{c}\}$ for the environment [see Fig. 1(i)]. Such a dilation is known to be unique up to partial isometries. For class B_2, also known as an *additive-noise channel*, the Stinespring dilation corresponds to an optimal Gaussian cloner (OGC) which clones asymmetrically in the clones but symmetrically in the quadratures [13]. Such a machine transforms the input mode $\{a\}$ and the two vacuum modes $\{e, \tilde{e}\}$ into a pair of clone modes $\{b, c\}$ and an anticlone mode $\{\tilde{c}\}$. In particular the reduced state of the output clone $k = b, c$ is given by the modulated state

$$\rho_k = \int d^2\gamma \; G_{\chi_k}(\gamma) \hat{D}(\gamma) \rho_a \hat{D}^\dagger(\gamma) \; , \; G_{\chi_k}(\gamma) := \frac{1}{\pi \chi_k} \exp\left(-\frac{|\gamma|^2}{\chi_k} \right) \; , \tag{1}$$

where $\hat{D}(\gamma)$ is the displacement operator and χ_k is the cloning noise variance satisfying $\chi_b \chi_c = 1$ with $\chi_b = \bar{n}$.

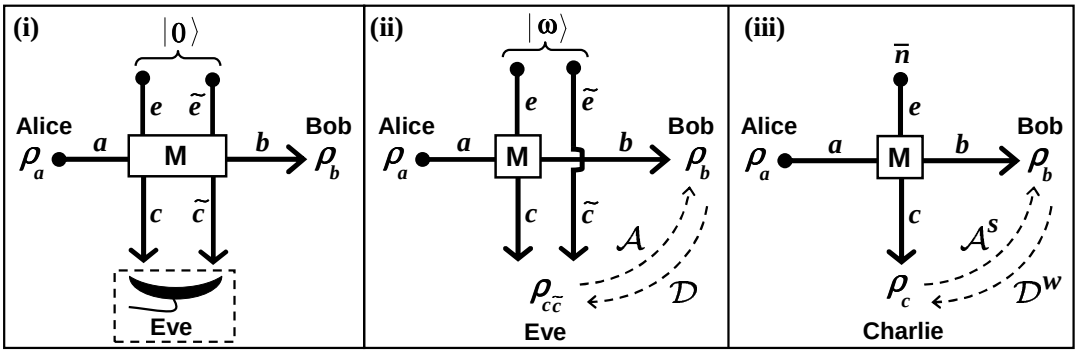

FIG. 1: Inset (i): Stinespring dilation of a canonical form. It describes a canonical attack by including the optimal coherent detection of all the outputs $\{c, \tilde{c}\}$ collected in all the uses of the channel. Both the dilation and the attack are unique up to isometries acting on the environmental modes $\{c, \tilde{c}\}$. Inset (ii): Stinespring dilation of a canonical form of every class but B_2; the form is antidegradable (degradable) if there exists a map $\mathcal{A}$ ($\mathcal{D}$) such that $\rho_b = \mathcal{A}(\rho_{c\tilde{c}})$ [$\rho_{c\tilde{c}} = \mathcal{D}(\rho_b)$]. Inset (iii): Physical representation of a canonical form of every class but B_2; the form is strongly antidegradable (weakly degradable) if there exists a map $\mathcal{A}^s$ ($\mathcal{D}^w$) such that $\rho_b = \mathcal{A}^s(\rho_c)$ [$\rho_c = \mathcal{D}^w(\rho_b)$].

It is important to notice that class B_2 is the unique class where the Stinespring dilation cannot be simplified to a single-mode description [9]. For all the other classes, in fact, we can consider a dilation where the symplectic transformation $\mathbf{M}_{ae\tilde{e}}$ can be decomposed as $\mathbf{M}_{ae} \oplus \mathbf{I}_{\tilde{e}}$, involving the signal mode $\{a\}$ and *only one* mode $\{e\}$ of the two-mode environment $\{e, \tilde{e}\}$ [see Fig. 1(ii)]. This is possible if the environment is prepared in a two-mode squeezed vacuum (TMSV) state $|\omega\rangle_{e\tilde{e}}$, i.e., in a pure Gaussian state with correlation matrix

$$\mathbf{V}_{e\tilde{e}}(\omega) = \begin{pmatrix} \omega \mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega \mathbf{I} \end{pmatrix} \; , \; \omega := 2\bar{n} + 1 \geq 1 \; . \tag{2}$$

Such a dilation $\{\mathbf{M}_{ae} \oplus \mathbf{I}_{\tilde{e}}, |\omega\rangle\}$ is the purification of a single-mode *physical representation* [14] $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$, where $\mathbf{M}_{ae}$ mixes the signal mode $\{a\}$ with a single environmental mode $\{e\}$, prepared in a thermal state $\rho_e(\bar{n})$ with $\bar{n}$ average photons [11]. This physical representation can also be seen as a quantum broadcast channel where the symplectic $\mathbf{M}_{ae}$ relates the output quadratures $\hat{\mathbf{x}}_{out}^T = (\hat{q}_b, \hat{p}_b, \hat{q}_c, \hat{p}_c)$ of two receivers (Bob and Charlie) to the input quadratures $\hat{\mathbf{x}}_{in}^T = (\hat{q}_a, \hat{p}_a, \hat{q}_e, \hat{p}_e)$ of a sender (Alice) and a thermal environment [see Fig. 1(iii)].

An important property of all the canonical forms (except B_2 [15]) is their *degradability* or *antidegradability* [11, 16]. A canonical form is called *strongly antidegradable* if it has a single-mode physical representation $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$

where Charlie can reconstruct Bob's state ρ_b via some CPT map $\mathcal{A}^s$, i.e., $\rho_b = \mathcal{A}^s(\rho_c)$. Notice that the strong antidegradability $\{a\} \to \{c\} \to \{b\}$ is a sufficient but not necessary condition for the (standard) antidegradability $\{a\} \to \{c, \tilde{c}\} \to \{b\}$, where Bob's state is reconstructed by considering all the degrees of freedom of the environment (Eve). In fact, the form is called *antidegradable* if there exists a CPT map $\mathcal{A}$ such that $\rho_b = \mathcal{A}(\rho_{c\tilde{c}})$. In the same way, one can consider the *weak degradability* $\{a\} \to \{b\} \to \{c\}$ which is implied by the (standard) degradability $\{a\} \to \{b\} \to \{c, \tilde{c}\}$. In fact, degradability corresponds to the existence of a map $\mathcal{D}$ such that $\rho_{c\tilde{c}} = \mathcal{D}(\rho_b)$, while weak degradability corresponds to the existence of a map $\mathcal{D}^w$ such that $\rho_c = \mathcal{D}^w(\rho_b)$ for some physical representation. Clearly the weak/strong notions coincide with the standard ones when $\bar{n} = 1$.

From the point of view of practical quantum cryptography, classes C and D are the most important ones. These classes are full-rank ($r = 2$) and represent the unique classes where the invariant τ can take a continuum of values, except for the singular points $\tau = 0$ and $\tau = 1$. Because of this continuity, we call the canonical forms $\mathcal{C}(\tau, 2, \bar{n})$ of classes C and D as *regular*. For these forms, one can consider a single-mode physical representation $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$ with symplectic matrix

$$\mathbf{M}_{ae}(\tau) = \begin{pmatrix} \sqrt{|\tau|} & 0 & \sqrt{|1-\tau|} & 0 \\ 0 & s(\tau)\sqrt{|\tau|} & 0 & s(1-\tau)\sqrt{|1-\tau|} \\ s(\tau-1)\sqrt{|1-\tau|} & 0 & s(\tau)\sqrt{|\tau|} & 0 \\ 0 & -\sqrt{|1-\tau|} & 0 & \sqrt{|\tau|} \end{pmatrix}, \tag{3}$$

where $s(\cdots)$ is the sign function. Notice that Eq. (3) corresponds to a beam splitter for $0 < \tau < 1$ and to an amplifier for $\tau > 1$. A regular canonical form $\mathcal{C}(\tau, 2, \bar{n})$ is strongly antidegradable (weakly degradable) if and only if $\tau \leq 1/2$ ($\tau \geq 1/2$) [11].

III. QUANTUM CRYPTOGRAPHY SCENARIO

In the standard scenario of quantum cryptography, the environment is completely under control of a malicious eavesdropper (Eve). Here, a one-mode channel can be generally seen as the effect of a collective attack, where Eve probes the signals using individual interactions and then performs a coherent detection of all the outputs collected in all the uses of the channel. According to Ref. [5], one can define as a "canonical attack" a collective attack that generates a one-mode Gaussian channel in canonical form. This is actually a particular form of the most general collective Gaussian attack that is completely characterized in Ref. [5]. Up to partial isometries, a canonical attack is described by combining the two-mode Stinespring dilation $\{\mathbf{M}_{ae\tilde{e}}, |0\rangle\}$ of the canonical form with the optimal coherent detection of all the environmental outputs, which are collected in all the uses of the channel [see Fig. 1(i) including Eve]. In the special case of the class B_2, the corresponding B_2 canonical attacks are OGC attacks where both the clone and anticlone are used in the final coherent measurement. In all the other cases, the canonical attacks can be simplified according to Fig. 1(ii) where Eve uses a single-mode symplectic interaction $\mathbf{M}_{ae}$ and the TMSV state specified by Eq. (2). In particular, the *regular canonical attacks* are the ones with $\mathbf{M}_{ae}(\tau)$ given in Eq. (3). These attacks can be associated to a pair $\{\tau, \omega\}$ with $\tau \neq 0, 1$.

In this paper, we consider the individual version of the regular canonical attacks (denoted by $\{\tau, \omega\}_{ind}$), where Eve is restricted to incoherent detections of her outputs (and no isometry is applied). By adopting this kind of attack, we derive the security thresholds of the coherent state protocol of Ref. [3]. In this protocol, Alice prepares a coherent state $\rho_a := |\alpha\rangle\langle\alpha|$ whose amplitude α is Gaussianly modulated with variance μ. Then, Alice sends the state through the channel, whose output is homodyned by Bob. In particular, Bob randomly switches between the detection of $\hat{q}_b$ and $\hat{p}_b$, the effective sequence being classically communicated at the end of the protocol (basis revelation). Here, the optimal attack $\{\tau, \omega\}_{ind}$ is a direct generalization of the delayed-choice entangling cloner attack of Ref. [3, 17] (retrieved in the particular case $0 < \tau < 1$). This means that Eve stores all her outputs in a quantum memory, awaits the basis revelation and, then, performs the correct sequence of $\hat{q}$ and $\hat{p}$ detections on her outputs. This is equivalent to saying that, for each run of the protocol where Bob chooses the $\hat{q}$ quadrature, Eve also detects the $\hat{q}$ quadrature on her modes $\{c, \tilde{c}\}$. In particular, we can assume as first detection one of $\hat{q}_{\tilde{c}}$, which is equivalent to the remote preparation of a $\hat{q}$-squeezed state on the input mode $\{e\}$ with variance $\langle \hat{q}_e^2 \rangle = \omega^{-1}$ [17]. As a consequence, Eve is always able to control the input environment $\{e\}$ in such a way as to enhance her detection of the output mode $\{c\}$ in the same quadrature which is effectively chosen by Bob.

By adopting this optimal attack, let us explicitly derive the security thresholds of the coherent state protocol in the limit of high modulation $\mu \to +\infty$. From Eqs. (2) and (3), we derive the following variance and conditional variance for Bob's output

$$V_B(\mu) = \langle \hat{q}_b^2 \rangle = \langle \hat{p}_b^2 \rangle = |\tau|(\mu + 1) + |1 - \tau|\,\omega \ , \ V_{B|A} = V_B(\mu = 0) \ . \tag{4}$$

Then, we have the following signal-to-noise formula for the classical mutual information

$$I_{AB} := \frac{1}{2}\log\frac{V_B}{V_{B|A}} \overset{\mu\gg 1}{\to} \frac{1}{2}\log\frac{\mu}{\eta(\omega,\tau)} \ , \tag{5}$$

where the total noise $\eta(\omega,\tau) := \Delta + \chi(\omega,\tau)$ is given by the sum of the quantum shot-noise $\Delta = 1$ and the *equivalent noise* of the channel

$$\chi(\omega,\tau) = \left|\frac{1-\tau}{\tau}\right|\omega \ . \tag{6}$$

From the point of view of the classical mutual information of Eq. (5), the regular canonical form $\mathcal{C}(\tau,2,\bar{n})$ is equivalent to a form $\mathcal{C}(1,2,\bar{n})$ of the class B_2 (additive-noise channel), where the input classical signal α with Gaussian modulation μ is subject to the additive Gaussian noises χ and Δ (coming from the channel and the measurement, respectively). In fact, in such a case, we would have

$$V_B = \mu + \Delta + \chi \ , \ V_{B|A} = \Delta + \chi \ , \tag{7}$$

which leads exactly to Eq. (5) for $\mu \to +\infty$. In order to analyze the security thresholds, it is useful to introduce the so-called *excess noise*

$$\varepsilon := \eta(\omega,\tau) - \eta(1,\tau) = \left|\frac{1-\tau}{\tau}\right|(\omega - 1) \tag{8}$$

so that

$$\chi(\varepsilon,\tau) = \left|\frac{1-\tau}{\tau}\right| + \varepsilon \ , \tag{9}$$

i.e., the equivalent noise can be decomposed in pure-τ noise and excess noise $\varepsilon \geq 0$. Roughly speaking, ε quantifies the effect of the input thermal noise (ω) in the equivalent additive description of the quantum channel, which is specified by Eq. (7).

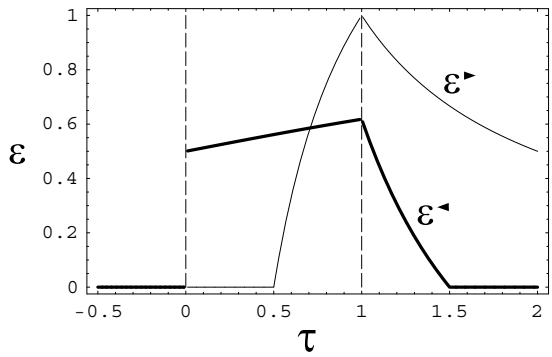

FIG. 2: Security thresholds in DR (thin curve) and RR (thick curve) in the presence of an individual and regular canonical attack $\{\tau,\omega\}_{ind}$ (where $\tau \neq 0,1$). Such thresholds are expressed in terms of maximum-tolerable excess noise ε versus τ. For a given τ, only the positive $\varepsilon's$ below the curves are secure.

In order to derive the security thresholds, let us compute the mutual information I_{AE} (between Alice and Eve) and I_{BE} (between Bob and Eve). It is easy to check that

$$V_E(\mu) = \left\langle \hat{q}_c^2 \right\rangle = \left\langle \hat{p}_c^2 \right\rangle = |1-\tau|\,(\mu+1) + |\tau|\,\omega^{-1} \ , \tag{10}$$

$$V_{E|A} = |1-\tau| + |\tau|\,\omega^{-1} \ , \ V_{B|E} = \left[|\tau|\,(\mu+1)^{-1} + |1-\tau|\,\omega\right]^{-1} \ , \tag{11}$$

and, therefore,

$$I_{AE} := \frac{1}{2}\log\frac{V_E}{V_{E|A}} \overset{\mu\gg 1}{\to} \frac{1}{2}\log\frac{\mu}{1+\chi^{-1}} \ , \ I_{BE} := \frac{1}{2}\log\frac{V_B}{V_{B|E}} \overset{\mu\gg 1}{\to} \frac{1}{2}\log\tau^2\chi\mu \ . \tag{12}$$

Then, we can compute the secret-key rates in direct reconciliation (DR, ▶) and reverse reconciliation (RR, ◀), i.e.,

$$R^{\blacktriangleright} := I_{AB} - I_{AE} \rightarrow \frac{1}{2}\log\frac{1+\chi^{-1}}{1+\chi} \ , \ R^{\blacktriangleleft} := I_{AB} - I_{BE} \rightarrow \frac{1}{2}\log\frac{1}{\tau^2\chi(1+\chi)} \ . \tag{13}$$

From $R^{\blacktriangleright} = 0$ we derive the security threshold $\chi(\varepsilon,\tau) = 1$ or, equivalently, the curve $\varepsilon^{\blacktriangleright} = \varepsilon^{\blacktriangleright}(\tau)$ shown in Fig. 2. From such a figure we clearly see how strong antidegradability (holding for $\tau \leq 1/2$) is a sufficient condition for the insecurity of the channel in DR (since $\varepsilon^{\blacktriangleright} = 0$ for every $\tau \leq 1/2$). However, it is not a necessary condition as shown by the existence of the insecure regions for $\tau \geq 1/2$ and $\varepsilon > \varepsilon^{\blacktriangleright}(\tau)$ (where the channel is insecure but weakly degradable). This is a consequence of the fact that Eve is much more powerful than Charlie, thanks to her active control of the input environment. In fact, even if no strong antidegradability can be found in the range $\tau \geq 1/2$, the channel can be still antidegradable, e.g., within the insecure regions for $\tau \geq 1/2$ and $\varepsilon > \varepsilon^{\blacktriangleright}(\tau)$. We recover a full equivalence between strong antidegradability and insecurity only in the case $\varepsilon = 0$, where the channel does not introduce thermal noise. In such a case, in fact, the strong antidegradability coincides with the standard antidegradability and the security threshold ($\tau = 1/2$) corresponds exactly to the threshold between antidegradability and degradability.

The fact that the strong antidegradability is a sufficient condition for the insecurity in DR is quite obvious. In fact, it implies the antidegradability, where Eve can reconstruct Bob's state and, therefore, retrieve at least the same information of Bob in decoding Alice's signals (i.e., $\exists\mathcal{A}^s \Rightarrow \exists\mathcal{A} \Rightarrow I_{AE} \geq I_{AB}$). However, the situation is completely different in RR, where Alice and Eve try to guess Bob's outcomes. In such a case, even if the channel is strongly antidegradable, Bob's outcomes can be much more correlated to Alice's variables than Eve's ones. In general, the only way for Eve to beat Alice in RR consists in introducing an environment which is squeezed enough to make her correlations prevail. From $R^{\blacktriangleleft} = 0$ we derive the discontinuous [18] security threshold

$$\varepsilon^{\blacktriangleleft} = \varepsilon^{\blacktriangleleft}(\tau) := \frac{\sqrt{4+\tau^2} - |\tau| - 2\,|1-\tau|}{2\,|\tau|} \ , \tag{14}$$

shown in Fig. 2. From Fig. 2 it is clear that, even if the channel is strongly antidegradable, QKD can be secure. This is due to the existence of the secure region for $0 < \tau \leq 1/2$ and $\varepsilon < \varepsilon^{\blacktriangleleft}(\tau)$. Notice that for $\tau > 1$, i.e., for an amplifying channel, reverse reconcilation is outperfomed by direct reconciliation. This is in accordance with the previous results of Ref. [19].

According to the expression of I_{AE} in Eq. (12), the Alice-Eve channel can also be described by an additive-noise channel where the input classical signal α (with variance μ) is modulated by an equivalent channel's noise χ^{-1} and a homodyne detection noise $\Delta = 1$. In fact, we retrieve the same mutual information I_{AE} of Eq. (12) by considering

$$V_E = \mu + \Delta + \chi^{-1} \ , \ V_{E|A} = \Delta + \chi^{-1} \ , \tag{15}$$

and taking the asymptotic limit for $\mu \rightarrow +\infty$. By considering both the Alice-Bob and Alice-Eve channels, one easily checks that the optimal $\{\tau,\omega\}_{ind}$ has therefore an equivalent additive description when direct reconciliation and high modulation are considered. Such an additive description corresponds to an individual OGC attack where Eve clones the input signals with cloning variances $\chi_b = \chi$ and $\chi_c = \chi^{-1}$, stores her clones in a quantum memory and, then, makes the correct homodyne detections after the basis revelation [20]. Such an individual attack is optimal since the saturation of the uncertainty principle $\chi_b\chi_c = 1$ minimizes the information-disturbance trade-off, which can be expressed by the product of the output conditional variances

$$V_{B|A}V_{E|A} = (\Delta+\chi)(\Delta+\chi^{-1}) \ . \tag{16}$$

In direct reconciliation and high modulation, an individual OGC attack with noise χ represents therefore an equivalent additive description of the optimal attack $\{\tau,\omega\}_{ind}$ via Eq. (6). To be precise, there is a whole class of optimal attacks $\{\tau,\omega\}_{ind}$, with different τ and ω but the same $\chi = \chi(\omega,\tau)$, which are equivalent to an individual OGC attack. Notice that this equivalence is true for the "switching" protocol of Ref. [3], but not for the "non-switching" protocol of Ref. [4].

IV. CONCLUSION

In this paper, we have investigated recent notions and properties of the one-mode Gaussian channels in the scenario of quantum cryptography. In particular, we have considered the canonical attacks, which are the cryptographic analog of the canonical forms. We have adopted the individual version of these attacks in order to study the connections between the degradability properties of a Gaussian channel and its security for QKD. We have also explicitly clarified the connections between the various notions of degradability and antidegradability. Finally, we have shown some connections between individual canonical attacks and optimal Gaussian cloners.

V. ACKNOWLEDGMENTS

S.P. was supported by a Marie Curie Fellowship of the European Community. S.L. was supported by the W.M. Keck foundation center for extreme quantum information theory (xQIT).

---

[1] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[2] M. Hillery, Phys. Rev. A **61**, 022309 (2000); T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
[3] F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); F. Grosshans *et al.*, Nature **421**, 238 (2003).
[4] C. Weedbrook *et al.,* Phys. Rev. Lett. **93**, 170504 (2004); A. M. Lance *et al.*, Phys. Rev. Lett. **95**, 180503 (2005).
[5] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[6] S. Pirandola, R. Garcia-Patron, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[7] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nature Physics **4**, 726 (2008).
[8] S. Pirandola *et al.*, Europhys. Lett. **84**, 20013 (2008); S. Pirandola *et al.*, arXiv:0903.0750.
[9] A. S. Holevo, Probl. Inform. Transm. **43**, 1 (2007).
[10] A. Serafini et al., Phys. Rev. A **71**, 012320 (2005).
[11] F. Caruso *et al.*, New Journal of Physics **8**, 310 (2006); F. Caruso and V. Giovannetti, Phys. Rev. A **74**, 062307 (2006).
[12] In particular, class C describes an attenuator for $0 < \tau < 1$ and an amplifier for $\tau > 1$. Class B_2 includes the ideal channel for $r = 0$.
[13] N. J. Cerf *et al.*, Phys. Rev. Lett. **85**, 1754 (2000).
[14] A physical representation is a unitary dilation of the quantum channel where the environmental state ρ_E can be (generally) mixed [11] (see also Ref. [21]). It is *not unique* up to partial isometries, except when it coincides with a Stinespring dilation (i.e., ρ_E is pure).
[15] The class B_2 is the unique class which is neither anti-degradable nor degradable [9].
[16] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[17] F. Grosshans *et al.*, Quant. Inf. and Comp. **3**, 535 (2003).
[18] In Fig. 2 the discontinuity of $\varepsilon^{\blacktriangleleft} = \varepsilon^{\blacktriangleleft}(\tau)$ at $\tau = 0$ is due to the limit $\mu \to +\infty$, taken for every finite and non-zero τ. For every *finite* μ, the curve converges to zero in a continuous way.
[19] R. Filip, Phys. Rev. A **77**, 032347 (2008).
[20] Notice that, in order to be optimal in DR, the individual OGC attack ignores the measurement of the anticlone. It is not known if such a further measurement can be useful in the eavesdropping of the protocol in RR.
[21] A. S. Holevo, Probl. Inform. Transm. **8**, 63 (1972); G. Lindblad, Commun. Math. Phys. **48**, 116 (1976).