# CHAPTER 1

## Continuous-Variable Quantum Key Distribution

F. Grosshans

*Laboratoire de Photonique Quantique et Moléculaire, UMR CNRS 8537,
Ecole Normale Supérieure de Cachan, 94235 Cachan Cedex, France*

A. Acín

*ICFO - Institut de Ciències Fotòniques, Parc Mediterrani de la Tecnologia,
08860 Castelldefels (Barcelona), Spain*

N. J. Cerf

*Quantum Information and Communication, Ecole Polytechnique, CP 165,
Université Libre de Bruxelles, 1050 Brussels, Belgium*

Quantum key distribution is a technique in which secret key bits are encoded into quantum states which are transmitted over a quantum channel, e.g. an optical link, so that the security is guaranteed by the laws of quantum physics. Most experimental realizations to date have relied on discrete protocols, involving ideally single-photons states (or, in practice, strongly attenuated light pulses) as well as single-photon detectors. In this chapter, we present an overview of the recent continuous-variable quantum cryptosystems, which instead rely on continuously-modulated Gaussian states (e.g. coherent states) and homodyne detection. The series of security proofs of these protocols against increasingly powerful attacks will be reviewed. A particular emphasis will be put on the optimality of Gaussian attacks in this context, which holds provided that the second-order moments of the relevant variables are monitored.

## 1. Introduction

Quantum key distribution (QKD) is the most mature practical application of quantum information sciences today. It's provable security against arbitrarily powerful adversaries – even for parties exchanging a secret key

quantum key distribution ! prepare-and-measure
quantum key distribution ! entanglement-based

using only present day's technology – allowed it to leave the laboratory and become already commercially available [1]. Although essentially all the currently deployed QKD systems are discrete, hence based on single-photon detectors following the original proposal by Bennett and Brassard (BB84)[2], continuous variables (CV) will probably also have a role to play because the detectors they rely on are more technologically developed: while the photon counters used in BB84 seem to be limited to detection rates of a few megahertz in ideal conditions [3], the homodyne or heterodyne detectors used in continuous-variable QKD can easily operate in the gigahertz range. For instance, the use of homodyning allowed the very first proof-of-principle CV-QKD experiment to distribute keys at a rate of 1.7 Mbit/s [4].

The field of CV-QKD is evolving very quickly, due to the relative simplicity of the experimental setups but also certainly thanks to the theoretical knowledge that is inherited from photon counting-based QKD. The security proofs have greatly improved over the last few years, going from the security against simple beamsplitting attacks as analyzed in the early paper by Hillery [5] to the security against very general (collective) attacks in [6,7]. This is certainly not the end of the story, and we are confident that a complete unconditional security proofs for CV-QKD including all experimental imperfection is not very far. A main simplification in this direction may come from the work of Renner [8], indicating that the security against collective attacks actually ensures security against more general coherent attacks. The present chapter aims at providing a broad overview of the various security proofs that have been developed in CV-QKD, in particular for the so-called Gaussian protocols. [9,10,11,4,6,7].

## 2. Generic description of continuous-variable protocols

The objective of a QKD protocol is for two partners, traditionally named Alice and Bob, to agree on a secret random string (the key). This secret key has to be kept unknown to an eavesdropper (Eve) who is assumed to have access to a much more advanced technology than Alice and Bob. If Eve has unlimited resources and is able to do everything but violate the laws of quantum physics (as well as entering Alice's and Bob's lab), one speaks about unconditional security.

QKD protocols can be divided into two main categories, the *prepare-and-measure* (P&M) and *entanglement-based* (E-B) schemes. A P&M protocol generally works as follows: Alice prepares quantum systems (usually light pulses) in some states and sends them to Bob through a quantum channel which is supposed to be controlled by Eve. After Bob has measured the received systems, Alice and Bob share correlated classical information, from which they extract the secret key through classical communication over a public authenticated channel. Of course, Eve is supposed to have interacted as much as she wanted with the quantum systems on their way from Alice to Bob. She also has listened to all communicated messages over the classical channel.

reconciliation
privacy amplification

In an E-B protocol, Alice and Bob initially share an entangled state (which could even have been prepared by Eve) and perform both a measurement on their part of it. Everything else is identical to a P&M scheme. Since Alice's measurement can be viewed as a "preparation through measurement", these protocols are indeed equivalent to P&M schemes [12]. While E-B protocols are more difficult to realize experimentally, they are easier to study theoretically, not only because of the symmetry between Alice and Bob, but also because the "monogamy" of entanglement allows us to study Eve's attack more generally. In this chapter, we will use this point of view, and study the continuous-variable P&M protocols through their E-B counterparts.

The classical communication between Alice and Bob allows them to distill a secret key from their correlated data. It is usually divided into three steps: (i) *Channel evaluation*: Alice and Bob publish a random sample of their measurements and compare them to evaluate the characteristics of the quantum channel (and infer Eve's potential action from it); (ii) *Reconciliation*: they use error correction techniques to correct the transmission errors and agree on a common bit string, partially known by Eve; (iii) *Privacy amplification*: they use a technique based on hash functions to extract, from this common string, a secret key unknown of Eve.

When turning to continuous variables, the above general description of QKD remains valid. But, in addition, CV-QKD can be understood in a restricted or more general manner. In a restricted P&M version of CV-QKD, Bob is using homodyne detection, hence he measures continuous data, but Alice is sending states selected from a finite alphabet, typically made of just a few non-orthogonal states, see e.g. [5,13]. In a fully-continuous P&M version of CV-QKD, as first explored in [9], Alice prepares randomly chosen Gaussian states drawn from an arbitrary continuous (e.g. Gaussian) distribution. The prepared states can be either coherent or squeezed. Bob then measures them with an homodyne or heterodyne detection. Similarly, Bob can keep all his measurements or discard some part of it (postselection). We will limit ourselves here to a Gaussian modulation and full measurement

Gaussian QKD protocols

(no postselection), because the resulting family of protocols is better understood and easier to study. Restricted (or discretely-modulated) protocols with postselection such as [13] seem to be easy to implement and robust to losses, but, to the best of our knowledge, no study has been carried out beyond Gaussian attacks, which are obviously not the optimal attacks in this case.

In what follows, is will be more convenient to consider the E-B version of these fully-continuous Gaussian P&M protocols, as introduced in [14]. In such a protocol, Alice prepares her state by measuring half of a two-mode vacuum squeezed state of parameter $r_A$, which was initially shared with Bob (see Fig. 1). For a coherent-state protocol, this means that Alice measures both quadratures, $X_A$ and $P_A$, by using a beam-splitter of transmittance $T_A = 1/2$ (heterodyne detection). Denote by $x_A$ and $p_A$ the obtained outcome. This effectively projects the second mode onto a coherent state centered on

$$x = \sqrt{2} \tanh\left(\frac{r_A}{2}\right) x_A \quad p = -\sqrt{2} \tanh\left(\frac{r_A}{2}\right) p_A, \tag{1}$$

and modulated according to a Gaussian distribution centered on the origin and of variance $\langle x^2 \rangle = \langle p^2 \rangle = [\cosh(r_A) - 1]/2$. In contrast, if $T_A = 1$ (homodyne detection) and Alice chooses randomly the measured quadrature, she is effectively preparing squeezed states of squeezing parameter $\cosh(r_A)$ which are modulated with a Gaussian distribution of variance $\langle x^2 \rangle = \langle p^2 \rangle = \sinh(r)^2/[2\cosh(r)]$.

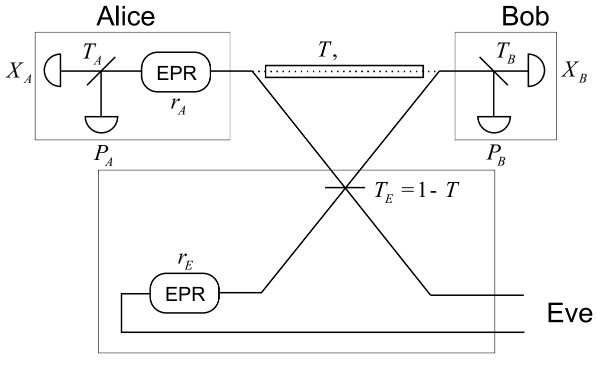

Fig. 1. Entanglement-based protocol under consideration. After Alice's effective preparation by measuring her part of an entangled state, the resulting Gaussian-modulated coherent or squeezed state of light is measured by Bob. Eve replaces the channel of transmittance $T$ and excess noise $\varepsilon$ by an entangling cloner of parameters $r_E$ and $T_E$. The excess noise is defined as the noise that goes beyond the loss-induced noise.

Now, since Alice can arbitrarily delay her measurement, we can interpret this protocol as if Alice was sending half of a two-mode squeezed state to Bob through an insecure channel before performing her measurement. As a result, Alice and Bob would share a noisy entangled state that is mapped into correlated classical data by Gaussian measurements. Both protocols are of course equivalent from Eve's point of view, but the theoretical analysis turns out to be simpler for this E-B scheme. However, the obtained security bounds automatically apply to the corresponding P&M scheme.

excess noise
entangling cloner

## 3. Structure of the security proofs

### 3.1. *Eve's physical attack*

In the E-B scheme, Alice and Bob share a mixed entangled state $\rho_{AB}$. The best situation for Eve is when she can "purify" this state: the global state between Alice, Bob, and Eve is then pure $|\Psi\rangle_{ABE}$, with $\mathrm{tr}_E|\Psi\rangle\langle\Psi| = \rho_{AB}$. If Alice and Bob could perform a full tomography of their state, they could know $\rho_{AB}$ and deduce Eve's state up to an irrelevant transformation. However, this strategy, which is standard in discrete-variable QKD, is not realistic with continuous variables because of the infinite dimensionality of the Hilbert space. Therefore, tomography must be limited to a few parameters, usually the coefficients of the covariance matrix $\gamma_{AB}$ of the state $\rho_{AB}$. Fortunately, if it is Gaussian, the state $\rho_{AB}$ – and Eve's attack – becomes fully characterized by $\gamma_{AB}$. Of course, this is not true in the general case, so it will be crucial, in the security analysis, to show that the Gaussian attack is optimal for a given covariance matrix $\gamma_{AB}$.

It is convenient at this point to introduce Eve's Gaussian attack for a given symmetric Gaussian channel, characterized by its transmission $T$ and excess noise $\varepsilon$, called the "entangling cloner" (see Fig. 1). As proven in [15], Eve can simulate the channel $(T, \varepsilon)$ by combining at a beam-splitter of transmittance $T_E = 1 - T$ the intercepted state together with half of a two-mode squeezed vacuum state. The squeezing parameter $r_E$ has to be chosen such that $(1 - T)\cosh r_E = 1 - T + \varepsilon T$. If the initial covariance matrix between Alice and Bob (*before* transmission) is $\gamma_0$, it becomes *after* transmission $\gamma_{AB} = M^{\mathrm{T}}\gamma_0 M + N$, with $M = \mathrm{diag}(1, 1, \sqrt{T}, \sqrt{T})$ and $N = \mathrm{diag}(0, 0, 1 - T + \varepsilon T, 1 - T + \varepsilon T)$.

### 3.2. *Eve's measurement*

As we have seen, Eve's physical attack allows her to hold a (Gaussian or non-Gaussian) purification of $\rho_{AB}$. This is not enough *per se* to give her

attacks ! individual
attacks ! collective
attacks ! coherent

information about the secret key. She necessarily needs to perform some measurement in order to extract this information. This measurement can be divided into 3 categories of increasing power, namely (1) individual, (2) collective, and (3) coherent attacks.

In individual attacks, Eve makes one ancilla interact with each pulse, individually, and performs a measurement on it. This measurement cannot depend on Alice and Bob's classical communication (except for the possibly disclosed basis choice). Since this measurement outcome is classical, Eve's information is then measured by Shannon (classical) mutual information. A variation of this attack is the "finite-size attack", where the interaction encompasses several pulses. The size of the block, however, has to be much smaller than the length of the codewords used in the key extraction stage, and, even more importantly, the joint measurement of the ancillas cannot depend on the exchanged messages during this key extraction stage.

For collective attacks, the interaction with the ancillas stays individual (or, at least, of a finite size), but the ancillas are stored in a quantum memory and measured only after Alice and Bob have communicated to perform the key extraction stage. At this point, a complex collective measurement is performed on the quantum memory. The information gained by Eve using this strategy is computed using the Von Neumann entropies instead of Shannon entropies, which leads to the Holevo information. This strategy potentially gives Eve more information than an individual attack.

Coherent attacks are, by definition, the most powerful attacks allowed by quantum mechanics: Eve interacts globally with all pulses and then performs a delayed global measurement. This global interaction renders any statistical assumption difficult, since Alice, Bob, and Eve now share a single high-dimensional quantum system. However, the collective attacks, which are currently known to be optimal within a restricted class of explicit attacks, are likely to be fully optimal even against coherent attacks (see [8]) although there is no rigorous proof of it yet for continuous variables.

### 3.3. *Eve's knowledge*

To extract the secret key from their correlated data, Alice and Bob use privacy amplification, which, roughly speaking, allows them to filter out the bits known to Eve. All they need to know to apply privacy amplification is an upper bound $I_E$ on Eve's information. Once this bound is known, they can extract a secret key whose length is at least $I(A:B) - I_E$, where $I(A:B)$ is the mutual information between Alice's and Bob's data.

reconciliation
! direct
reconciliation
! reverse

The expression of $I_E$ of course depends on Eve's strategy, but also on the direction of the classical information flow: if the classical communication is one-way and flows from Alice to Bob in order for him to error correct his data, it means that Alice's data form the secret key so that $I_E$ is the amount of information Eve has gained on Alice's data. This is known as *Direct Reconciliation* (DR). For obvious symmetry reasons, such a strategy cannot succeed when the physical channel is a lossy channel with more than 50% losses. The symmetry between Bob and Eve has to be broken, which can only be done with a feedback, that is, with some classical communication flowing from Bob to Alice. This can be done using one-way backward classical communication (and no forward communication): this is the *Reverse Reconciliation* (RR) scenario, where the secret key is based on Bob's data. In this case $I_E$ represents the amount of information gained by Eve on Bob's data. It is also possible to use two-way classical communication (e.g., in postselection-based protocols [13,16]) but this strategy will not be discussed here.

## 4. Individual attacks

### 4.1. *Preliminaries*

For individual attacks, Eve is assumed (i) to interact individually and in the same way with each quantum state sent over the channel, and (ii) to measure before the error correction and privacy amplification procedures have taken place. These two assumptions are realistic within the present-day technology, even though more general attacks may be imagined. The results shown in this subsection were published (with more details) in [9,10,4] for individual attacks and in [11] for finite-size attacks.

If Eve interacts individually and in the same way with the states, this corresponds, in the entanglement picture, to a situation where Alice, Bob, and Eve share many copies of the state $|\Psi\rangle_{ABE}$, resulting from Eve's interaction on half of a two-mode squeezed state, $|\psi(r_A)\rangle$, and a reference state $|R\rangle_E$, that is,

$$|\Psi\rangle_{ABE} = (\mathbb{1}_A \otimes U_{BE})|\psi(r_A)\rangle_{AB}|R\rangle_E. \qquad (2)$$

After their measurements, Alice and Bob map their shared state into correlated random variables, $A$ and $B$. Eve is also assumed to measure at this point, so she has a random variable $E$ correlated with Alice and Bob's outputs. Therefore, the three parties share correlated Classical-Classical-Classical information (CCC correlations). This results in the diagonal den-

Csisz“'ar-K“”orner bound

sity operator

$$\rho_{ABE} = \sum_{A,B,E} p\,(A,B,E)|A\rangle\langle A| \otimes |B\rangle\langle B| \otimes |E\rangle\langle E|. \tag{3}$$

The process of distilling a secret key out of CCC correlations using one-way communication protocols was studied in [17]. There, it was shown that given a CCC correlation with distribution $p\,(A,B,E)$, the direct one-way secret-key rate satisfies

$$K^{\rightarrow} \geq I(A:B) - I(A:E) = \bar{K}_D. \tag{4}$$

In this formula, it is assumed that the flow of information in the error correction and privacy amplification stages goes from Alice to Bob. Also, $I$ stands for Shannon's mutual between the classical random variables,

$$I(X:Y) = H(X) - H(X|Y), \tag{5}$$

where $H(X)$ denotes a Shannon entropy while $H(X|Y)$ is a Shannon conditional entropy [18].

The maximal information Bob can extract about Alice's variable $A$ from his variable $B$ is equal to the mutual information $I(A:B)$. The same holds for Eve, so her accessible information on Alice's data is given by $I(A:E)$. Therefore, the bound (4) compares the information on Alice's preparation accessible to Bob and Eve. The Csiszár-Körner bound (4), is thus quite intuitive as it reflects Bob's advantage over Eve, but its proof is rather involved!

Very naturally, in the case of reverse reconciliation, the previous bound becomes

$$K^{\leftarrow} \geq I(A:B) - I(B:E) = \bar{K}_R, \tag{6}$$

as it is the advantage of Alice over Eve which is relevant. We are now ready to analyze the rate of key extraction against individual attacks using these simple bounds. In particular, it will analyzed how it depends on the channel parameters, $T$ and $\varepsilon$, for different protocols.

### 4.2. *Secure key rates against individual attacks*

Let us show how to compute the bounds of Eqs. (4) and (6) for the CV-QKD protocols using squeezed or coherent states, and homodyne or heterodyne measurements (a more detailed calculation can be found in [14]). We restrict our considerations to Gaussian attacks, as in Fig. 1. It will be proven in

Section 7 that these attacks minimize all the bounds, so they are maximally pessimistic (i.e., optimal for Eve).

As explained above, the state preparation by Alice can be done by means of a two-mode squeezed vacuum state of squeezing parameter $r_A$ and a beam-splitter of transmittance $T_A$. After propagating through the insecure channel, Alice, Bob, and Eve share a tripartite state, $|\Psi\rangle_{ABE}$. This state depends on Alice's preparation, the channel properties $(T, \varepsilon)$, and Bob's measurement, either homodyne ($T_B = 1$) or heterodyne ($T_B = 1/2$). Since Eve's attack is Gaussian, the state is completely specified by its covariance matrix $\gamma_{ABE}$, while the displacement vector is zero. It is relatively simple to calculate (4) and (6) from $\gamma_{ABE}$. Alice and Bob's mutual information can be found through the Wigner function of their reduced state $\rho_{AB}$. The Wigner function indeed defines the Gaussian probability distribution of the quadrature measurements of Alice and Bob, from which $I(A:B)$ can be obtained. The same reasoning gives $I(A:E)$ (or $I(B:E)$).

Using this formalism, one can compute the key rates that are secure against any Gaussian individual attack for a given protocol (Alice's preparation and Bob's measurement) and channel parameters $(T, \varepsilon)$. Not surprisingly, the obtained key rate turns out to be an increasing function of the modulation in the state preparation, that is, of $r_A$. Moreover, in some particular cases, one obtains relatively simple formulas. For instance, consider the situation where the excess noise $\varepsilon$ in the channel is zero while $r_A$ is large. Then, for the protocols analyzed in [10,4],

$$\bar{K}_D \approx \frac{1}{2}\log\left(\frac{T}{1-T}\right) \qquad \bar{K}_R \approx \frac{1}{2}\log\left(\frac{1}{1-T}\right), \tag{7}$$

for the coherent-state protocol, while for the squeezed-state protocol [9],

$$\bar{K}_D \approx \log\left(\frac{T}{1-T}\right) \qquad \bar{K}_R \approx \log\left(\frac{1}{1-T}\right), \tag{8}$$

that is, they are twice as large as with coherent states. In the case of the protocol where both Alice and Bob perform heterodyne measurements [19], i.e., $T_A = T_B = 1/2$, one has

$$\bar{K}_D \approx \log\left(\frac{T}{1+T}\right) \qquad \bar{K}_R \approx \log\left(\frac{1}{1-T}\right). \tag{9}$$

All these bounds on the secret key rate define security conditions for lossy but noiseless channels, which guarantee provable security against individual attacks. For all direct protocols, we always have the constraint $T > 1/2$, which correspond to 3 dB of losses. In contrast, for all reverse protocol, arbitrary high losses are tolerable, in principle, since the rate is positive for any non-zero value of $T$.

These bounds can also be computed for noisy channels, that is for a non-zero excess noise $\varepsilon$. Direct protocols (with coherent or squeezed states) are secure provided that the total equivalent input noise is smaller than the shot noise. This corresponds to a maximal excess noise $\varepsilon < 2 - 1/T$, which can only be positive for $T < 1/2$. The maximal tolerable excess noise for reverse protocols depends on the allowed squeezing: if Alice can send arbitrarily squeezed states, one has $\varepsilon < 2$, while if she can only send coherent states, $\varepsilon < \frac{1}{2} - \frac{1}{T} + \sqrt{\frac{1}{T^2} + \frac{1}{4}}$, which varies between $\frac{1}{2}$ (for $T \to 0$) and $(\sqrt{5} - 1)/2 \simeq 0.61$ (for $T = 1$). Thus, in the important case of coherent-state protocols, reverse reconciliation is more appropriate for lossy channels with little noise while direct reconciliation has an advantage for noisy channels with few losses.

## 5. Collective attacks

### 5.1. *Preliminaries*

Even though the two restrictions that we have put on Eve in the analysis of individual attacks [(i) interaction with each pulse individually, and (ii) measurement before the classical key distillation procedure] are very realistic, taking into account the present-day technology, they are unsatisfactory from a theoretical point of view. What we want to achieve in quantum cryptography is provable security without imposing any limitation on Eve's technological power. For instance, the second assumption seems to be particularly strong. After having interacted with the states, Eve holds a quantum system that is correlated with Alice's preparation and Bob's measurement results. During the reconciliation process, the honest parties exchange information through the classical public channel in order to increase their correlations. This information is also available to Eve, so it appears quite reasonable that her correlations with Alice's and Bob's data may also increase. Therefore, she can adapt and improve the measurement on her quantum state according to the exchanged messages. The aim of the next two sections is to extend the previous security analysis to such general attacks. We first get rid of assumption (ii) and allow Eve to delay her measurement until the end of the reconciliation process. This corresponds to the case of collective attacks, treated in this section (more details can be found in [6,7,20]). In the next section, we also get rid of assumption (i), providing key rates secure against any attack consistent with quantum mechanics.

Holevo bound

In collective attacks, Eve's interaction remains the same as with individual attacks, so that Eq. (2) stays valid. After their measurements, Alice and Bob map again their shared state $\rho_{AB}$ into correlated random variables, $A$ and $B$. But, in contrast with individual attacks, Eve is not assumed to measure at this point, so she keeps a quantum state that is correlated with Alice and Bob's outputs, $\rho_E^{AB}$. Here, the three parties share correlated Classical-Classical-Quantum information (CCQ correlations). This can be summarized by means of the quantum state

$$\rho_{ABE} = \sum_{A,B} p\,(A,B) |A\rangle\langle A| \otimes |B\rangle\langle B| \otimes \rho_E^{AB}. \tag{10}$$

where the fact that Eve has not performed a measurement translates into the fact that the density operator is not diagonal in E.

The process of distilling a secret key out of CCQ correlations (and, even more generally, out of CQQ correlations) using one-way communication protocols has been studied in [21] (see also [22]). There, it was shown that given a CQQ state

$$\rho_{ABE} = \sum_{A} p\,(A) |A\rangle\langle A| \otimes \rho_{BE}^{A}, \tag{11}$$

the one-way secret key rate satisfies

$$K^{\rightarrow} \geq \chi(A:B) - \chi(A:E). \tag{12}$$

Here, $\chi$ stands for the Holevo bound [23], which gives the accessible classical information encoded into an ensemble of quantum states $\{p\,(x), \rho^x\}$,

$$\chi = S(\rho) - \sum_x p\,(x) S(\rho^x), \tag{13}$$

where $\rho = \sum_x p\,(x)\rho^x$ and $S(\rho) = -\mathrm{tr}(\rho \log \rho)$ denotes the von Neumann entropy. Equation (12) looks is a very intuitive extension of Eq. (4); however, its proof is again rather involved!

Tracing out Eve, Bob is effectively receiving quantum states encoding Alice's classical data, $\rho_B^A = \mathrm{tr}_E \rho_{BE}^A$, with probability $p\,(A)$. The maximal information he can extract is equal to the Holevo bound $\chi(A:B)$, computed for the ensemble $\{p\,(A), \rho_B^A\}$. The Holevo bound can indeed be interpreted very naturally as the quantum mutual information between the internal state of the preparer (Alice) and the state arriving at the receiver (Bob) [24]. The same holds for Eve, her accessible information on Alice's data being given by $\chi(A:E)$. Therefore, the bound (12) compares the information on Alice's preparation accessible to Bob and Eve, generalizing to the CQQ case the well-known Csiszár-Körner bound (4) for CCC correlations.

In any P&M protocol, Bob also holds classical data since he measures his quantum state upon receiving it, as described by Eq. (10). This simply represents a special subset of the more general scenario analyzed in [21], so that the same reasoning holds for CCQ correlations. The Holevo quantity $\chi(A:B)$ then simply coincides with the standard mutual information between Alice and Bob, $I(A:B)$ [24]. Thus, the extractable secret key rate in direct reconciliation satisfies

$$K^{\rightarrow} \geq I(A:B) - \chi(A:E) = \hat{K}_D. \tag{14}$$

In the case of reverse reconciliation, this bound reads,

$$K^{\leftarrow} \geq I(A:B) - \chi(B:E) = \hat{K}_R. \tag{15}$$

### 5.2. *Secure key rates against collective attacks*

Let us analyze how the bounds (14) or (15) depend on the channel parameters, $T$ and $\varepsilon$, for different QKD protocols (using squeezed or coherent states, and heterodyne or homodyne measurements). A more detailed calculation can be found in [20]. We again restrict our considerations to Gaussian attacks, as in Fig. 1, knowing that these attacks minimize all the bounds considered here (see section 7).

The information $I(A:B)$ is calculated exactly as for individual attacks, while the calculation of $\chi(A:E)$ is slightly more involved. After tracing out Bob, one has the Gaussian state $\rho_{AE}$ of covariance matrix $\gamma_{AE}$ and zero displacement vector, completely specifying the correlations between Alice and Eve. This covariance matrix has the form

$$\gamma_{AE} = \begin{pmatrix} \gamma_A & C_{AE} \\ C_{AE}^T & \gamma_E \end{pmatrix}, \tag{16}$$

where $\gamma_A$ ($\gamma_E$) is the covariance matrix of Alice's (Eve's) local state, and $C_{AE}$ characterizes their correlations. Alice's measurement projects her state into a Gaussian state of covariance matrix $\gamma_A^{m_A}$ and displacement vector $\vec{d}_A^{m_A}$, depending on the obtained outcome $m_A$, and on the type of measurement. For instance, $\gamma_A^{m_A} = \mathbb{1}$ for a coherent state protocol. This measurement is also effectively preparing a Gaussian state on Eve's side, with covariance matrix $\gamma_E^{m_A}$ and displacement vector $\vec{d}_E^{m_A}$. These two quantities can be calculated using the Gaussian formalism developed in [25,26], namely

$$\begin{aligned} \gamma_E^{m_A} &= \gamma_E - C_{AE}^T(\gamma_A + \gamma_A^{m_A})^{-1} C_{AE} \\ \vec{d}_E^{m_A} &= C_{AE}^T(\gamma_A + \gamma_A^{m_A})^{-1} d_A^{m_A}. \end{aligned} \tag{17}$$

In all the considered protocols, with squeezed or coherent states, $\gamma_A^{m_A}$ does not depend on the measurement outcome $m_A$, so $\gamma_E^{m_A}$ is also independent of $m_A$, $\gamma_E^{m_A} \equiv \gamma_E^A$. Therefore, $\chi(A:E)$ is simply equal to

$$\chi(A:E) = S(\gamma_E) - S(\gamma_E^A), \tag{18}$$

where we explicitly use the fact that the von Neumann entropy of a Gaussian state only depends on its covariance matrix. The same reasoning can be applied to the calculation of $\chi(B:E)$ for reverse reconciliation.

Using this formalism, one can compute secure key rates against any collective attack, for a given protocol (Alice's preparation and Bob's measurement) and channel parameters. The calculation of the bounds is lengthy but straightforward. In the case where the excess noise $\varepsilon$ in the channel is zero and $r_A$ is large, one obtains simple results. Then, for the coherent-state protocols analyzed in [10,4], one has

$$\hat{K}_D \approx \frac{1}{2}\log\left(\frac{T}{1-T}\right) \qquad \hat{K}_R \approx \frac{1}{2}\log\left(\frac{1}{1-T}\right), \tag{19}$$

while, for squeezed-state protocols [9], one has

$$\hat{K}_D \approx \log\left(\frac{T}{1-T}\right) \qquad \hat{K}_R \approx \log\left(\frac{1}{1-T}\right), \tag{20}$$

In the case of the protocol of [19], where $T_A = T_B = 1/2$, one has

$$\hat{K}_D \approx \log\left(\frac{T}{1+T}\right) - \log e \qquad \hat{K}_R \approx \frac{1}{T}\log\left(\frac{1}{1-T}\right) - \log e. \tag{21}$$

All these bounds on the extractable secret key rate define security conditions for provable security against collective attacks, as summarized in Fig. 2.

| Protocol | Direct | Reverse |
|---|---|---|
| Coherent states | 3 dB | no limit |
| Squeezed states | 3 dB | no limit |
| Heterodyne measurements | 1.4 dB | no limit |

Fig. 2. Critical values of the channel transmission for provable security against collective attacks in the case of zero excess noise and large modulation variance. The coherent-state protocol, squeezed-state protocol, and the protocol with heterodyne measurements are compared.

The previous formalism is also useful to establish the critical value of the excess noise in the line, above which no key distribution is possible, independently of Alice's modulation, see [7]. These values have to be understood as simply testable sufficient conditions for secure key distribution. For squeezed-state protocols, it is always more convenient to employ reverse reconciliation. In contrast, for coherent-state protocols, direct reconciliation turns out to be more resistant against excess noise down to a channel transmission of $\approx 0.65$. Note also that there exist limiting values of the excess noise, $\varepsilon_c$, for which the considered secret key rates are zero, independently of the modulation and the losses. These values can be computed analytically. For coherent states and direct reconciliation, one has that $\varepsilon_c$ is the solution to the equation

$$\frac{1}{1+\varepsilon}\left(\frac{\sqrt{1+\varepsilon}+1}{\sqrt{1+\varepsilon}-1}\right)^{\sqrt{1+\varepsilon}} = e^2, \tag{22}$$

that gives $\varepsilon_c \approx 0.8$, while for reverse reconciliation

$$\varepsilon_c = \frac{1}{2}\left(\sqrt{1+\frac{16}{e^2}}-1\right) \approx 0.39. \tag{23}$$

In the case of squeezed states, the critical excess noise is equal to $2/e \approx 0.7$ for both reconciliation protocols. A similar picture can be obtained for the heterodyne measurement-based protocol of [19].

## 6. Coherent attacks

A first approach to analyze the resistance of CV-QKD against the most general (coherent) attacks consists in exploiting the equivalence between quantum error correcting codes and one-way entanglement purification protocols, exactly as for discrete-variable QKD. This approach was followed in [28] in order to prove that Gaussian-modulated squeezed-state protocols can be made unconditionally secure provided that the squeezing exceeds some threshold $r \approx 0.3$. It was extended in [29] to the case of coherent-state protocols, although the tolerable loss is only of 0.4 dB in this case. These results can be viewed as proofs of principle that unconditional security is achievable with continuous-variable protocols, but unfortunately they do not yield useful secret key rates.

Recently, however, powerful techniques for the analysis of general security proofs of QKD have been presented in [27], which can predict secret key rates. In any QKD scheme, there is a tomographic process that partly characterizes the insecure channel connecting Alice and Bob. It allows the honest parties to evaluate their mutual information, $I(A:B)$. Moreover, it puts a bound on Eve's knowledge: it was shown in [27] that, using the information collected during this process, one can construct a secure reconciliation protocol that allows one to extract

$$\tilde{K} = I(A:B) - \max_{\rho_{AB} \in \mathcal{R}} S(\rho_{AB}), \tag{24}$$

secret bits, where $\mathcal{R}$ is the set of quantum states consistent with the measured probabilities (see [27] for more details). Thus, this quantity represents a lower bound to the achievable key rate, $K \geq \tilde{K}$. For all the QKD schemes analyzed here, the attack minimizing $\tilde{K}$ for fixed first and second moments of $\rho_{AB}$ is Gaussian (see section 7). Unfortunately, this bound does not make any distinction between direct and reverse reconciliation, a relevant issue in continuous-variable QKD protocols.

The calculation of $\tilde{K}$ proceeds along the same lines as above for $\hat{K}_D$ or $\hat{K}_R$. Consider first the coherent-state or squeezed-state protocol. For the case of a lossy but noiseless line, $\varepsilon = 0$, one can numerically see that there exists an optimal squeezing $r_A^{opt}$ which is the same for coherent-state and squeezed-state protocols [7]. A reason for this counter-intuitive result may be that $\tilde{K}$ is known to be a non-tight bound to the optimal key rate [27]. This optimal squeezing, $r_A^{opt} \approx 1.5$, defines a critical value for the tolerable losses of approximately 1.7 and 0.83 dB for squeezed-state and coherent-state protocols, respectively.

As discussed in [27] it is possible to improve the bound (24) by conditioning the privacy amplification process on a classical random variable $W$ (see [27] for more details), decreasing Eve's entropy. For the case of coherent states, Alice and Bob can make public the value of the second measured quadrature, instead of discarding it. This process does not modify Alice and Bob's mutual information but changes Eve's entropy. The obtained critical transmission, $T_c$, is now a decreasing function of the squeezing, as expected. One can see that in the limit of high modulation, $r_A \rightarrow \infty$,

$$T_c = \frac{e^2}{e^2 + 4}. \tag{25}$$

That is, the protocol using coherent states and homodyne measurements is secure up to 1.9 dB of losses.

Finally, let us consider the heterodyne measurement-based protocol of [19] in the case of a lossy line. Recall that the two quadratures measured by Alice contribute to the key. These two homodyne measurements effectively prepare a coherent state that propagates through the insecure channel, and Eve keeps a fraction $1 - T$ of it. Therefore, Eve receives pure coherent attacks ! Gaussian

states, depending on $x_A$ and $p_A$. This implies that $S(\rho_E)$ is actually equal to $\chi(A:E)$, which means that $\tilde{K} = \hat{K}_D$. Thus, a secure key distribution against general attacks is possible up to 1.4 dB of losses (see Fig 2).

## 7. Optimality of Gaussian attacks

### 7.1. *Preliminaries*

The derivation of all the previous bounds on the extractable secret key rates has been done assuming that Eve's optimal attack was Gaussian. The goal of this section is to prove this optimality, that is, to show that for given first and second moments of the measured quadratures by Alice and Bob, the attack minimizing $\bar{K}_D$, $\bar{K}_R$, $\hat{K}_D$, $\hat{K}_R$, and $\tilde{K}$ is Gaussian. A proof of this result has first been given in [11] for finite-size attacks (but assuming that Eve's measurement takes place before the key distillation procedure), and will be presented in [20] for collective and coherent attacks (when Eve's measurement is allowed to depend on the exchanged messages during the key distillation procedure).

The details of the proof are different for finite-size and collective attacks, but the generic idea is the same: Gaussian attacks are the one which induced the less structured (i.e., more entropic) noise on Bob's measurement outcomes for a given covariance matrix. Roughly speaking, since Eve is constrained by quantum mechanics, the more structure she induces on Bob's noise, the less freedom she has on her attack. More rigorously, the amount of information $I_E$ she gains can be upper bounded by an entropic quantity that is calculated from the (experimentally accessible) covariance matrix of the state $\rho_{AB}$ shared by Alice and Bob, and this maximum is attained for a Gaussian attack.

Note that, for all practical purposes, one only needs to bound $I_E$, since $I(A:B)$ will in reality depend on the practical error-correcting codes used by Alice and Bob in the reconciliation stage. Even if these codes would yield a rate that is close to Shannon's limit for a Gaussian channel, the evolution of this rate for an arbitrary non-Gaussian attack would be difficult to predict. Nevertheless, this is not a problem in practical CV-QKD because Alice and Bob can always measure $I(A:B)$ by comparing a sample of their reconciliated keys, so there is no need to predict it.

### 7.2. *Entropy of Gaussian states $\tilde{\rho}$ – general attacks*

Let $\rho \in B(\mathcal{H}^2)$ denote an arbitrary density operator, and $\tilde{\rho}$ the density operator corresponding to a Gaussian state characterized by the same covariance matrix (or second-order moments) and displacement vector (or first-order moments) as $\rho$. Similarly, if $p\,(x)$ is a probability distribution for a random variable $X$, then $\tilde{p}\,(x)$ denotes the Gaussian probability distribution with the same first- and second-order moments as $p\,(x)$. Finally, if $F(x)$ represents any function of a random variable $x$, whose probability distribution is $p\,(x)$, then $F(\tilde{x})$ has to be understood as the same function $F$ applied to the distribution $\tilde{p}\,(x)$. It can be shown that, for any state $\rho$, one has

entropy ! relative
entropy ! conditional

$$S(\tilde{\rho})-S(\rho)=\mathrm{tr}(\rho\log\rho)-\mathrm{tr}(\rho\log\tilde{\rho})+\mathrm{tr}(\rho\log\tilde{\rho})-\mathrm{tr}(\tilde{\rho}\log\tilde{\rho})=S(\rho||\tilde{\rho}) \quad (26)$$

where the first two terms in the r.h.s. of Eq. (26) sum to the quantum relative entropy $S(\rho||\tilde{\rho})$. The sum of the last two term in the r.h.s. of Eq. (26) vanishes because $\log\tilde{\rho}$ is a polynomial of second order in the field operators, so that $\rho$ and $\tilde{\rho}$ have, by definition, to the same expectation values.

As a consequence, since the quantum relative entropy is positive semi-definite [30], the state of maximal entropy for fixed first- and second-order moments is indeed Gaussian. In particular, if Alice and Bob share a state $\rho_{AB}$, they can bound its entropy from its covariance matrix, that is, $S(\rho_{AB})\leq S(\tilde{\rho}_{AB})$. Using similar arguments, it can be seen that the same property holds for classical probability distributions

$$H(\tilde{x})-H(x)=H(x||\tilde{x})\geq 0, \quad (27)$$

where $H(x||\tilde{x})=\sum_x p\,(x)\log[p\,(x)/\tilde{p}\,(x)]$ is the classical relative entropy.

The fact than the states with a maximal entropy are Gaussian combined with the bound (24) gives us immediately the optimal general attack (for this bound): it is a Gaussian attack.

### 7.3. *Conditional entropy of $\tilde{\rho}$ – individual attacks*

The von Neumann conditional entropy [31] is

$$S(A|B)=S(\rho_{AB})-S(\rho_B)=S(\tilde{A}|\tilde{B})-S(\rho_{AB}||\tilde{\rho}_{AB})+S(\rho_B||\tilde{\rho}_B) \quad (28)$$

The relative entropy is a discrimination measure between two states and can only decrease under a physical (*i.e.* trace preserving) map. That is, for any such map, denoted by $\mathcal{T}$, and any two states, $\rho_1$ and $\rho_2$,

$$S(\rho_1||\rho_2)\geq S(\mathcal{T}(\rho_1)||\mathcal{T}(\rho_2)). \quad (29)$$

Tracing out $A$ is a particular instance of such a trace-preserving map, with $\mathcal{T}(\rho_{AB})=\rho_B$ and $\mathcal{T}(\tilde{\rho}_{AB})=\tilde{\rho}_B$. Therefore $S(\rho_B||\tilde{\rho}_B)\leq S(\rho_{AB}||\tilde{\rho}_{AB})$, entropic uncertainty principle

which implies that quantum conditional entropy is also maximized for a Gaussian state

$$S(A|B) \leq S(\tilde{A}|\tilde{B}). \tag{30}$$

Naturally, the same reasoning applies to classical probability distribution, substituting von Neumann conditional entropies with Shannon conditional entropies, and replacing trace-preserving maps by stochastic maps:

$$H(x|y) \leq H(\tilde{x}|\tilde{y}). \tag{31}$$

In order to find the optimal individual attacks, one needs to combine this inequality with the entropic uncertainty principle [32], which states that $H(p_A|p_B) + H(x_A|x_E) \geq 0$ where $x_A$ and $p_A$ are the two quadratures of Alice's state, inferred from Bob's ($p_B$) or Eve's ($x_E$) measurements. Note that $x_A$ and $p_A$ are expressed her in the appropriate units so that the r.h.s. term is 0 (in other units, it would simply be a constant). Thus, Alice and Eve's mutual information can been rewritten as

$$I(A:E) = H(x_A) - H(x_A|x_E) \leq H(x_A) + H(p_A|p_B) \tag{32}$$

which is optimal (maximum) for a Gaussian attack as a consequence of Eqs. (27) and (31). Of course, the same reasoning applies to $I(B:E)$ in the case of reverse reconciliation. This confirms that the attack which minimizes the bounds $\bar{K}_D$ and $\bar{K}_R$ for individual (finite-size) attacks is Gaussian.

### 7.4. *Effect of Alice's measurement – collective attacks*

Let $\rho \in B(\mathcal{H}^2)$ be any physical state and $\rho'$ the result of a measurement on a part of it by projection onto a given basis, say $X$,

$$\rho' = \sum_x |x\rangle\langle x|\rho|x\rangle\langle x| = \sum_x p\,(x)|x\rangle\langle x| \otimes \rho^x. \tag{33}$$

For example, $\rho$ can be thought of as the joint state of the system under investigation and an ancilla, which, after measurement, contains the measurement outcome. It is straightforward to check that [24]

$$S(\rho') = H(x) + \sum_x p\,(x) S(\rho^x), \tag{34}$$

where $H$ denotes the usual Shannon entropy. Now, Eve's gained information on Alice's measurement outcome (after Alice's measurement) that is needed to calculate the bound (14) can be written

$$\chi(A:E) = S(\rho_E) - \sum_{x_A} p\,(x_A) S(\rho_E^{x_A}), \tag{35}$$

see Eq. (13). Since the state of Alice, Bob, and Eve before Alice's measurement $|\Psi\rangle_{ABE}$ is pure, $S(\rho_E) = S(\rho_{AB})$. Similarly, since the state of Bob and Eve conditioned on Alice's measurement outcome $x_A$, i.e. $\langle x_A|\Psi\rangle_{ABE}$, is pure, $S(\rho_E^{x_A}) = S(\rho_B^{x_A})$. Thus

$$\begin{aligned}\chi(A:E) &= S(\rho_{AB}) - \sum_{x_A} p\,(x_A) S(\rho_B^{x_A}) = S(\rho_{AB}) - S(\rho'_B) + H(x_A) \\ &\leq S(\rho_{AB}) - S(\rho_B) + H(x_A) = S(A|B) + H(x_A). \qquad (36)\end{aligned}$$

where we have used Eq. (34) as well as the fact that the transformation $\rho_B \rightarrow \rho'_B$ can only increase the von Neumann entropy [30]. Once again, we see that the above expression is optimal (maximum) for a Gaussian attack as a result of Eqs. (27) and (30). The same reasoning also applies to $\chi(B:E)$ in reverse reconciliation. Note that if the states of Bob and Eve conditional on Alice's measurement are not pure (if Alice sends mixed states in the corresponding P&M protocol), the strong subadditivity of the entropies ensures that $\chi(A:E)$ is upper bounded by the same quantity, which maintains this optimality result. This confirms that the attack which minimizes the bounds $\hat{K}_D$ and $\hat{K}_R$ for collective attacks is Gaussian.

More generally, if Eve's attack is not identical from pulse to pulse, the above reasoning still holds, with multimode Gaussian states instead of single-mode ones. However Alice and Bob will not measure the full covariance matrix, but an averaged one, so they will overlook the pulse-to-pulse correlations. Fortunately, it is straightforward to show that this averaging will make them overestimate Eve's information, so they remain on the safe side. In other words, the optimal attack for a given estimated "single-pulse" covariance matrix remains the Gaussian attack described in Fig. 1.

## 8. Conclusion

We have outlined the main security proofs obtained today for assessing the security of continuous-variable quantum key distribution based on Gaussian-modulated Gaussian states and Gaussian measurements. We have discussed the increasingly difficult analyses of individual, collective, and coherent attacks. We have shown that, for a given estimated covariance matrix of Alice and Bob's quadrature components, the Gaussian attacks are optimal; hence, they provide a tight bound on the attainable secure key rates. We hope that these theoretical progresses will further encourage bringing CV-QKD closer to practice. An interesting recent step in this direction is the all-fibered coherent-state setup working at telecom wavelength (1550 nm) at a rate exceeding 1 Mbit/s that was reported in [33].

## References

1. For a recent review, see N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. C. H. Bennett and G. Brassard, *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*, IEEE, New York, (1984).
3. K. J. Gordon, V. Fernandez, G. S. Bulleri, I. Rech, S. D. Cova and P. D. Townsend, Optics Express **13**, 3015 (2005).
4. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, Nature **421**, 238 (2003).
5. M. Hillery, Phys. Rev. **63**, 022309 (2000).
6. F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
7. M. Navascués and A. Acín, Phys. Rev. Lett. **94**, 020505 (2005).
8. R. Renner, Ph.D. Thesis (ETH Zurich, 2005).
9. N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
10. F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
11. F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
12. C. H. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
13. Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
14. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Quant. Inf. Comp. **3**, 535 (2003).
15. F. Grosshans and Ph. Grangier, arXiv quant-ph/0204127.
16. M. Navascués, J. Baes, J. I. Cirac, M. Lewenstein, A. Sanpera and A. Acın, Phys. Rev. Lett. **94**, 010502 (2005).
17. Csiszár and Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
18. C. E. Shannon, Bell Syst. Tech. J. **27**, 479 and 623 (1948).
19. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
20. M. Navascués, F. Grosshans, and A. Acín, in preparation.
21. I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); Proc. R. Soc. Lond. A, **461**, 207 (2005).
22. R. Renner and R. König, quant-ph/0403133.
23. A. S. Holevo, Probl. Inf. Trans. **9**, 177 (1973).
24. N. J. Cerf and C. Adami, arXiv quant-ph/9611032.
25. G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).
26. J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).
27. M. Christandl, R. Renner, and A. Ekert, arXiv quant-ph/0402131.
28. D. Gottesman and J. Preskill, Phys. Rev. **63**, 022309 (2001).
29. S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
30. A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).
31. N. J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).
32. I. Bialynicki-Birula and J. Mycielski , Commun. Math. Phys. **44**, 129 (1975).
33. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303(R) (2005).