Finite-size analysis of a continuous-variable quantum key distribution

Anthony Leverrier, Frédéric Grosshans, Philippe Grangier

Finite-size analysis of a continuous-variable quantum key distribution

Anthony Leverrier,[1,*] Frédéric Grosshans,[2] and Philippe Grangier[3]
[1]*Institut Telecom/Telecom ParisTech, CNRS LTCI, 46 rue Barrault, 75634 Paris Cedex 13, France and ICFO-Institut de Ciencès Fotòniques, E-08860 Castelldefels (Barcelona), Spain*
[2]*Laboratoire de Photonique Quantique et Moléculaire, ENS de Cachan, UMR CNRS 8735, F-94235 Cachan Cedex, France*
[3]*Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, F-91127 Palaiseau Cedex, France*
(Received 4 May 2010; published 28 June 2010)

The goal of this paper is to extend the framework of finite-size analysis recently developed for quantum key distribution to continuous-variable protocols. We do not solve this problem completely here, and we mainly consider the finite-size effects on the parameter estimation procedure. Despite the fact that some questions are left open, we are able to give an estimation of the secret key rate for protocols which do not contain a postselection procedure. As expected, these results are significantly more pessimistic than those obtained in the asymptotic regime. However, we show that recent continuous-variable protocols are able to provide fully secure secret keys in the finite-size scenario, over distances larger than 50 km.

DOI: 10.1103/PhysRevA.81.062343 PACS number(s): 03.67.Dd, 42.50.−p, 89.70.−a

I. INTRODUCTION

Quantum key distribution (QKD) is a cryptographic primitive that allows two distant parties, Alice and Bob, to generate secret keys despite the presence of a potential eavesdropper [1]. When, in 1984, Bennett and Brassard invented the first QKD protocol [2], they could only prove that their protocol had to be secure in some appropriate regime (e.g., in the unrealistic case where Alice and Bob's data are perfectly correlated) but were not able to establish any security proof for a realistic setup at that time. During the last 25 years, security proofs have steadily improved, and today *unconditional security*, that is, security guaranteed in an information-theoretical sense has been established for many QKD protocols [3–6], including continuous-variable (CV) protocols [7]. A caveat, however, is that any theoretical security proof relies on assumptions, which can be more or less explicit. One such assumption can be, for instance, that the physical implementation of the protocol behaves as specified and that no side channels can be exploited by the adversary. This, unfortunately, is, in general, impossible to prove [8] unless one considers *device-independent* quantum cryptography [9,10], which is certainly a fascinating theoretical possibility but highly unpractical. Another assumption which is often made is that one considers the security of a protocol in the asymptotic regime of infinitely many signals exchanged by Alice and Bob. Here, on the positive side, the general framework to address the problem of finite-size effects already exists. The specific formalism was developed in Renner's Ph.D. thesis [6] and subsequently detailed in [11] and applied in [12]. Note also that another analysis compatible with composable security was developed by Hayashi in the case of BB84 with decoy states [13] and later applied to experimental data [14]. On the negative side, the results of these various papers are quite pessimistic and it is not totally unreasonable to think that the security of all QKD implementations realized until now was in fact jeopardized due to the (way) too short length of the blocks exchanged by Alice and Bob!

So far, finite-size analysis has been restricted to discrete-variable protocols, that is, protocols described with a finite-dimensional Hilbert space (see Ref. [15] for an application to QKD using qudit systems). In contrast, CV protocols, where information is encoded in phase space, appear to be a credible alternative to historical protocols like BB84. Indeed, they are relatively easy to implement, requiring only coherent state generation together with homodyne detection [16] and now display very good performances in terms of achievable distance [17–19].

The basic idea of CV QKD is to encode information in phase space. To do so, Alice sends random coherent states to Bob, who decides randomly to measure either one of the quadratures with a homodyne detection. (Note that a variant is for Bob to perform a heterodyne detection, that is, to measure both quadratures simultaneously [20–22].) After this measurement, Alice and Bob share classical variables x (the value of the quadrature of the state sent by Alice) and y (Bob's measurement result), from which they can, in principle, distill a key, once they have exchanged sufficiently many signals. A few protocols of interest have been proven unconditionally secure [7], depending on Alice's modulation, which can be either continuous (Gaussian [16] or eight-dimensional [19], to allow for a very efficient reconciliation procedure) or discrete (binary [23] or quaternary [17,18]). Note that for all such protocols, no postselection of the classical data [24] should be performed, as such a postselection is not compatible with present security proofs.[1]

The goal of the present paper is to give a finite-size analysis for CV QKD protocols. In Sec. II, we rapidly review the

*anthony.leverrier@icfo.es

[1]Remember, indeed, that protocols with a postselection procedure are only proven to be secure against Gaussian attacks. Unfortunately, in a finite-size context, it is impossible to prove rigorously that an attack is indeed Gaussian. One can likely upper-bound the probability that it is not the case, but this is not a trivial task, and it is quite certain that the final secret key rate one could compute would be very low.

framework of [11]. In Sec. III, we describe the outline of a general CV QKD protocol. Then in Sec. IV we discuss the main specificities of CV protocols in the context of finite-size analysis. We proceed in Sec. V with a detailed study of the most important finite-size effect: parameter estimation. Finally, we present the results of this study in Sec. VI and give some perspectives.

II. THE GENERAL FRAMEWORK FOR FINITE-SIZE ANALYSIS

In the following, we note N, the total number of signals exchanged by Alice and Bob during the protocol. We note x and y, the classical data of Alice and Bob, respectively, after they have measured their quantum states, and E refers to the quantum state of the eavesdropper.

The formalism developed in [6] allows for the following generalization of the secret key rate of a discrete-variable QKD protocol which is secure against collective attacks [11]:

$$k = \frac{n}{N}\left(S_{\epsilon_{\mathrm{PE}}}(x|E) - \frac{\mathrm{leak}_{\mathrm{EC}}}{n} - \Delta(n)\right). \tag{1}$$

This key rate has to be compared with the asymptotic key rate K given by

$$K = S(x|E) - H(x|y), \tag{2}$$

and four differences can be noticed.

First, only n signals are used for establishment of the key, of the N signals exchanged. This is due to the fact that $m = N - n$ signals are used for parameter estimation. This leads to the presence of the prefactor n/N in front of the secret key rate. Note that this factor is not very critical: it would become relevant if a QKD protocol were to be implemented and commercialized, as it limits the rate of the protocol, but in practice, it has little effect on the final rate—say a factor of $1/2$ if 50% of the data are used for parameter estimation. Indeed, the real theoretical challenge today is to decide whether a QKD protocol can be used to distill a secret key for some given conditions (of losses and noise). From this point of view, optimizing every possible parameter to maximize the secret key rate seems a little bit premature.

Second, the usual conditional entropy $S(x|E)$ has to be replaced by the expression $S_{\epsilon_{\mathrm{PE}}}(x|E)$, taking into account the finite precision of the parameter estimation. Indeed, whereas the quantum channel can be assumed to be perfectly known in the asymptotic regime, here this can only be achieved with a finite precision related to the probability ϵ_{PE} that the true values of the n_{PE} channel parameters are not inside the confidence region computed from the parameter estimation procedure. Note that there is never unicity of such a confidence region: one is free to optimize his or her choice among all possible regions compatible with the failure probability ϵ_{PE}. This choice can be based on the simplicity of the description of the region (e.g., the Cartesian product of n_{PE} intervals corresponding to each estimated parameter) or on an optimization maximizing the final secret key rate, in which case the confidence region is a very general region in the n_{PE}-dimensional space of the parameter space. Unfortunately, such an optimization is often rather complicated to perform, and in general, one chooses confidence regions with very simple shapes (one is referred to Ref. [25] for a discussion of such considerations in the case of BB84). There also exists a trade-off between the desired level of precision of the parameter estimation (in particular, the number n_{PE} of parameters one considers) and the number m of signals which have to be sacrificed to this end. For instance, it is known that for BB84, in the asymptotic regime, a full tomography of the state increases the secret key rate [26]. This is not necessary true anymore in a finite-size context. In [12], the authors suggest that in the limit where N tends to infinity, the optimal number of samples m used for the parameter estimation should be on the order of $\sqrt{N}$. However, for reasonable values of the block length N, the number of samples needs to be much larger than $\sqrt{N}$, especially in the case of CV protocols.

For BB84, only one parameter needs be estimated in theory: the quantum bit error rate (QBER). In practice, however, depending on the implementation, additional parameters might need to be estimated, especially if weak coherent states are sent instead of true single photons, for instance, in the case where the decoy-state technique [27] is applied. Using Hoeffding's inequality, for instance, one can find a confidence interval (parameterized by ϵ_{PE}) for the QBER such that the true value of the parameter is inside the interval with probability of at least $1 - \epsilon_{\mathrm{PE}}$. In the case where several parameters must be estimated (e.g., in CV QKD protocols), the notion of confidence interval should be replaced by a multidimensional confidence region such that the true value of the parameters lies in the region with a probability of at least $1 - \epsilon_{\mathrm{PE}}$. Then one needs to compute the minimum value of the conditional entropy $S(x|E)$ compatible with the confidence interval: this gives $S_{\epsilon_{\mathrm{PE}}}(x|E)$. Whereas this procedure is relatively straightforward for the QBER (which is a bounded parameter, since $0 \leqslant \mathrm{QBER} \leqslant 1$), we will see in the following that the question is more involved for CV QKD protocols, where one needs to estimate *a priori* unbounded parameters such as the excess noise. In this paper, we consider two parameters to be estimated in CV QKD: the transmission T and the excess noise ξ. In principle, these are not the only parameters to be estimated in a real implementation, as one also needs to know Alice's modulation variance (as well as the electronic noise and the quantum efficiency of the detectors if one considers a scenario where Bob's detection is calibrated), but one can reasonably assume that this parameter is relatively well known, in comparison to T and ξ.

Third, $\mathrm{leak}_{\mathrm{EC}}$ corresponds to the amount of information which needs to be exchanged by Alice and Bob during the reconciliation phase. This quantity is necessarily equal to or larger than the conditional entropy $H(x|y)$, but in practice, it always turns out out be strictly larger than the optimal value. We would like to emphasize that the effect of an imperfect reconciliation, which is parameterized by $\mathrm{leak}_{\mathrm{EC}}$ here, was already taken into account for the study of CV QKD through the so-called *reconciliation efficiency* β. This reconciliation efficiency gives the fraction of $I(x;y)$, the mutual information between Alice's and Bob's data, that the legitimate parties are able to exploit in practice. More precisely, the size of the (identical) bit strings shared by Alice and Bob after the reconciliation procedure is $n\beta I(x;y)$ (the factor n is a reminder that only n couples of data are processed for the key distillation, the rest being used for parameter estimation). This imperfect

reconciliation efficiency for a long time has been the cause of the limited range of CV QKD protocols (and still is for protocols involving a Gaussian modulation). In the case of discrete-variable QKD protocols, leak_{EC} is typically modeled as

$$\text{leak}_{\text{EC}} \approx f_{\text{EC}} H(x|y) + \frac{1}{n}\log_2(2/\epsilon_{\text{EC}}), \tag{3}$$

where $f_{\text{EC}} > 1$ is a parameter characterizing the reconciliation efficiency (in a slightly different way than β for CV reconciliation) and ϵ_{EC} is the probability that the reconciliation fails and that this failure goes undetected by Alice and Bob.[2] In practice, this probability can be made arbitrarily small.

Finally, the parameter $\Delta(n)$ is related to the security of the privacy amplification. Its value is given by

$$\Delta(n) \equiv (2\text{dim}\mathcal{H}_X + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{\text{PA}}), \tag{4}$$

where $\mathcal{H}_X$ is the Hilbert space corresponding to the variable x used in the raw key, $\bar{\epsilon}$ is a *smoothing* parameter, and ϵ_{PA} is the failure probability of the privacy amplification procedure. Both the smoothing parameter $\bar{\epsilon}$ and ϵ_{PA} are intermediate parameters which should be optimized numerically. The first term of $\Delta(n)$, that is, the square-root term, actually corresponds to the speed of convergence of the smooth min-entropy (which is the appropriate measure of the key length) of an independent and identically distributed (i.i.d.) state (remember that we consider collective attacks here) toward the von Neumann entropy. Indeed, only in the asymptotic limit is the smooth min-entropy of an i.i.d. state equal to its von Neumann entropy. The second term is directly linked to the failure probability ϵ_{PA} of the privacy amplification procedure.

Note that if one were to consider general security, it would be necessary to add to Eq. (1) another correction term linked to the use of the exponential version of the de Finetti theorem [28] or to the postselection technique [29], and this would give an even more pessimistic key rate. However, in the case of BB84, for instance, collective attacks are optimal, even in the case of finite-size analysis, and such terms are therefore not required. For CV QKD protocols, it is also conjectured, but not yet proven, that collective attacks are always optimal. Therefore, it makes sense to consider the finite-size analysis when the eavesdropper is restricted to collective attacks. Without the proof of the optimality of collective attacks, one could use the bound derived in [7] for application of an exponential version of the de Finetti theorem for infinite-dimensional Hilbert spaces. However, because this bound, which is not believed to be tight, leads to very pessimistic results, we prefer not to take it into account here and, therefore, limit our analysis to the case of collective attacks.

In the end, one needs to fix an overall security parameter ϵ for the QKD protocol. Indeed, contrary to the more usual asymptotic scenario, no such thing as *perfect security* can exist in a finite-size setting, and one is limited to ϵ security. The (small) parameter ϵ corresponds to the failure probability of the whole protocol, meaning that the protocol is assured to performed as it is supposed to except with a probability of at most ϵ. Again, here we do not consider problems due to an imperfect implementation, which might lead to the existence of side channels that can be used by an eavesdropper. The failure probability ϵ can be computed from the various parameters already described, and in the limit of small parameters, one has

$$\epsilon = \epsilon_{\text{PE}} + \epsilon_{\text{EC}} + \bar{\epsilon} + \epsilon_{\text{PA}}. \tag{5}$$

Note that all parameters $\epsilon_{\text{EC}}, \bar{\epsilon}, \epsilon_{\text{PA}}$, and ϵ_{PA} can independently be fixed at arbitrarily low values (possibly by increasing the total number N of exchanged signals to a rather high value):

1. ϵ_{PE} can be made as low as desired simply by increasing the size of the sample used for parameter estimation (and therefore not used for establishing a key).

2. ϵ_{EC} can be decreased with the following procedure: Alice and Bob simply need to compute a hash of their respective bit strings after the reconciliation and to publicly compare it. This method is very interesting because computing a hash acts like an error amplification: even if the original strings differ for only a few bits out of several millions, their hash will be different with a very high probability. Hence Alice and Bob can check that they share a common bit string while sacrificing only a negligible quantity of data.

3. $\bar{\epsilon}$ and ϵ_{PA} are virtual parameters that can be optimized in the computation. They must simply satisfy both equality (4) and equality (5).

As a consequence, the overall security parameter ϵ can be chosen arbitrarily small, to a value corresponding to Alice and Bob's wishes. Obviously, this comes at the cost of decreasing the final secret key size.

III. OUTLINE OF A CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION PROTOCOL IN A FINITE-SIZE CONTEXT

Traditionally, in the asymptotic regime, one can make the assumption that the quantum channel is perfectly known, before the transmission is even performed. Hence the optimization of the various free parameters can be made before the exchange of data, and the final secret key rate, in principle, can be known in advance (as long as the quantum channel behaves as anticipated).

In the finite-size scenario, the situation is quite different. In particular, one does not know in advance the characteristics of the quantum channel. To be fair, even after the exchange of quantum signals, the quantum channel is only partially known: more precisely, a few relevant parameters (QBER for qubit channels, transmission and excess noise for CV channels) are known to lie inside some confidence regions, except with probability ϵ_{PE}.

Even if Alice and Bob do not know in advance the properties of the quantum channel they will use, they can guess them with a reasonable accuracy, making the assumption that no eavesdropper will actually try to control the quantum channel. Note that this guess is only used to *a priori* optimize various parameters of the protocols and consequently maximize the

[2] In fact, f_{EC} and β are related to each other (for binary variables) through $(f_{\text{EC}} - 1)H(x|y) = (1-\beta)I(x;y)$. Using the fact that $I(x;y) = H(x) - H(x|y) = 1 - H(x;y)$ for symmetric binary variables, one obtains $f_{\text{EC}} = \{1 - \beta[1 - H(x|y)]\}/H(x|y)$.

expected secret key rate, under "normal use" of the quantum channel. If an eavesdropper is present, the guess made by Alice and Bob might not be very good, hence leading to a nonoptimized use of the quantum channel, but the security of the key distribution will not be affected.

For a CV QKD protocol, the secret key rate depends (in the asymptotic limit) on three main physical parameters: Alice's modulation variance V_A, the transmission of the channel T, and the excess noise ξ, which corresponds to the noise on Bob's state in excess compared to the shot noise. The idea is to optimize V_A to maximize the expected secret key rate. To do that, Alice and Bob can guess the values of T and ξ. The transmission can be evaluated quite precisely with $T \approx \eta 10^{-0.02d}$, where η is the known quantum efficiency of Bob's detection and d is the distance in kilometers between Alice and Bob. Here, we assume an optical fiber with losses of 0.2 dB per kilometer. In practice, Alice and Bob generally have a good estimate of the value of the transmission of the quantum channel before they start the QKD protocol. The value of ξ, in contrast, depends on the quality of the setup and turns out to be fairly stable from one experimental run of the QKD protocol to the next. Typically, for state-of-the-art implementations, its value is about 1% of the shot noise [30]. Note that this corresponds to the *expected* value of the excess noise. As we see later, the measured value might differ significantly from the theoretical value due to a high statistical noise.

At the beginning of the protocol, Alice and Bob agree on a particular value of the overall security parameter ϵ. They also agree on a reconciliation protocol, meaning that they know the parameter ϵ_{EC} in advance. Since both $\bar{\epsilon}$ and ϵ_{PA} are virtual parameters that have to be optimized afterward, the rest of the initial (that is, before the quantum distribution) optimization consists in studying the parameter ϵ_{PE}, which quantifies the failure probability of the parameter estimation. This parameter depends on the number $m = N - n$ of samples used for this parameter estimation as well as on some properties of the quantum channels, such as the expected true values of the parameters T and ξ. Therefore, given the expected behavior of the quantum channel, one can infer the value of m required to obtain a particular value of the parameter ϵ_{PE}. This in turn puts a lower bound on the block size N necessary to obtain an ϵ-secure secret key.

At this point, still before the actual start of the QKD protocol, Alice and Bob can optimize the values of the total number N of signals exchanged, the length of the raw key n, and the optimal value for Alice's modulation variance V_A to maximize the expected secret key rate compatible with the overall security parameter ϵ. The values of N, n, and V_A can be considered to be fixed at this stage.

Then Alice and Bob proceed with the quantum exchange part of the QKD protocol: Alice sends N random coherent states (or $N/2$ for protocols with heterodyne detection) according to the modulation characterizing the protocol (with a modulation variance V_A) who measures them with a homodyne (or heterodyne) detection. Bob informs Alice of his measurement choices (that is, for each state, Bob tells Alice whether he measured the X quadrature, the P quadrature, or both) and Alice discards the data that Bob did not measure. They publicly disclose $N - n$ of their correlated data to estimate the true values of the transmission and excess noise of the quantum channel. They can therefore compute the value of $S_{\epsilon_{\mathrm{PE}}}(y|E)$, the conditional von Neumann entropy of Bob's data (which will be used to form the key in a reverse reconciliation procedure) given Eve's quantum state, which is compatible with the estimated parameters except with probability ϵ_{PE}. If this value is compatible with a positive secret key rate, Alice and Bob continue with the reconciliation procedure; otherwise, they abort the protocol. At the end of the reconciliation procedure, Alice and Bob compute the hash of their respective bit strings (for some well-chosen hash function, that is, a randomly chosen hash function from a family such that the equality of both hashes guarantees that the reconciliation procedure worked except with probability ϵ_{EC}).[3] If their strings differ (because their hashes differ), Alice and Bob abort the protocol. (Note, however, that Alice and Bob might try to continue with the protocol by exchanging more classical information to complete the reconciliation procedure.) If their hashes are identical, Alice and Bob compute the final key size compatible with the security parameter ϵ (by optimizing over $\bar{\epsilon}$ and ϵ_{PA}) and perform the privacy amplification; that is, they randomly pick a hash function from a two-universal family of hash functions which outputs a string of length l, with $l = kN$ the size of the ϵ-secure secret key that they can extract from their data.

IV. VARIOUS ISSUES SPECIFIC TO CONTINUOUS VARIABLES

First, we would like to emphasize once again that we are considering only collective attacks here, and not general attacks. This decision was motivated by the fact that the optimality of collective attacks has been proven asymptotically and that it is conjectured that this optimality could hold in a finite-size setting. Moreover, the correction terms computed in [7] are quite large, are likely not tight, and might hide interesting effects (such as the dependence of the key rate on parameter estimation) behind purely technical details such as (temporary?) bounds linked to a particular mathematical proof (exponential version of the de Finetti theorem for infinite-dimensional Hilbert spaces).

A. Dimensionality

The main difference between discrete-variable and CV QKD protocols is obviously the infinite dimensionality of the Hilbert space required to describe CV QKD protocols. This is in general rather problematic when studying the security of CV QKD, but it becomes even more annoying when one considers finite-size effects. In particular, when one is only interested in asymptotic key rates, the dimension problem can be solved by saying that, in the end, everything in the experiment is discrete (even the homodyne detection since the local oscillator has a finite energy). Therefore, one can always theoretically bound the dimension of the relevant Hilbert space by a number large enough and prove that the correction terms due to this large dimension all go to 0 in the asymptotic limit.

[3] We neglect here the (small) number of bits which are revealed through this procedure.

Unfortunately, for a finite-size scenario, such an approach fails, as the convergence toward the asymptotic rate can be heavily slowed for a high dimension. For instance, the finite dimension corresponding to the digitalization is often of the order of $d = 2^{12} = 4096$ if one uses 12-bit analog-to-digital converters. If one compares such a system with a two-dimensional one, Eq. (4) tells us that the same $\Delta(n)$ is attained for an $n \propto d^2$, that is, for a value of n 1.4×10^6 times higher in the high-dimensional case. The magnitude of such factors clearly shows that bounding the dimensionality of the system by a finite value is not enough for ensuring its security in practical circumstances. This dimension should also be as small as possible, and it is important to come up with security proofs that are as dimension independent as possible.

Fortunately, in some CV protocols [17,19,31], the raw key is encoded on bits, and this allows us to take $\dim\mathcal{H}_Y = 2$ for the numerical evaluation of Sec. VI. When this is not possible, one should be able to replace the real dimension of the system by its *effective dimension*, but this remains essentially an open question. Such an effective dimension is generally much smaller than the real dimension and is sufficient to capture the relevant features of the CV system. Different definitions for this effective dimension can be proposed. Generally, however, one defines the effective dimension d_1^{eff} of a mixed system ρ as

$$d_1^{\text{eff}}(\rho) \equiv \frac{1}{\text{tr}\rho^2}, \tag{6}$$

which quantifies the number of states over which ρ is spread [32]. For instance, a totally mixed state over N orthogonal states has $d_1^{\text{eff}} = N$. A more speculative variant would be to remember that according to [33], the proper max-entropy $H_{\max}$ of a state is not given by the Rényi entropy of order 0 (which diverges for any quantum state of a CV system) but by the Rényi entropy of order $1/2$. Therefore one could also define the effective dimension d_2^{eff} as the exponential of this entropy; that is,

$$d_2^{\text{eff}}(\rho) \equiv (\text{tr}\sqrt{\rho})^2. \tag{7}$$

The advantages of the first definition are that it relates to the energy of the state, and that it is automatically bounded, for any (physical) state ρ.

To be rigorous, the preceding effective dimension defined previously will probably be defined under the form of "smooth dimensions," depending on a small parameter ϵ, in a way similar to the smooth entropies introduced in [34], which have allowed us to look at the finite-size effect. In any case, it is intuitively clear that, ultimately, it is such effective dimensions that should appear in security proofs of CV QKD protocols. This question certainly needs to be investigated further. We stress again that such a problem, which is rather benign in the asymptotic limit, plays a crucial role in a finite-size analysis.

B. Ill-defined entropies for continuous variables

Another specificity of the CV QKD is that classical entropies are ill defined for continuous variables: the Shannon entropy has to be replaced by a differential entropy, which is not a practical quantity for analyzing secret key rates. For this reason, the expression

$$S_{\epsilon_{\text{PE}}}(y|E) - \frac{\text{leak}_{\text{EC}}}{n} \tag{8}$$

is inadequate for CV QKD. The solution is to rewrite the different quantities in terms of mutual information instead of relative entropies. Hence, the previous expression can be replaced by

$$\beta I(x:y) - S_{\epsilon_{\text{PE}}}(y:E) \tag{9}$$

in the case of a CV protocol. Here $\beta I(x:y)$ gives the amount of mutual information Alice and Bob were effectively capable of extracting through the reconciliation phase: β is the reconciliation efficiency, which ranges from 0 when no information was extracted to 1 for a perfect reconciliation scheme. While $S_{\epsilon_{\text{PE}}}(y|E)$ is defined as the minimum conditional entropy compatible with the statistics given by the parameter estimation except with probability ϵ_{PE}, $S_{\epsilon_{\text{PE}}}(y:E)$ is naturally defined as the *maximum* of the Holevo information compatible with the statistics except with probability ϵ_{PE}. Hence, in the case of a CV QKD protocol, the secret key rate obtained for a finite-size analysis reads

$$k = \frac{n}{N}[\beta I(x:y) - S_{\epsilon_{\text{PE}}}(y:E) - \Delta(n)]. \tag{10}$$

C. Reconciliation efficiency

Whereas the question of error correction was never a crucial issue for DV protocols where it just implied a small correction term, the same is not true for CV protocols *without postselection*. For these schemes, Alice and Bob need to be able to extract their mutual information very efficiently. The absence of efficient reconciliation protocols working in the low signal-to-noise ratio (SNR) regime was, for a long time, the reason why CV protocols could not distribute secret keys as far as their DV counterparts. To be more precise, a reconciliation protocol is considered efficient if β is larger than roughly 80%. For such efficiencies, the correction term appears quite negligible and has a limited impact on the QKD protocol. For a Gaussian modulation, the best-known protocols achieve efficiencies higher than 80% only for SNRs higher than 1 [31,35,36]. For lower SNRs (relevant to increasing the range of the protocol), no good protocol is known for the reconciliation of correlated Gaussian variables. Fortunately, this problem can be solved in this regime by switching to a discrete modulation where efficient protocols are available for all SNRs lower than 1 [17].

To summarize, both modulation schemes (Gaussian and discrete) are useful, depending on the working distance of the protocol. When working at short distances, a Gaussian modulation should be chosen, whereas a discrete modulation is more adapted to reaching longer distances. In both cases, the effect of imperfect reconciliation can be taken care of by taking $\beta = 0.8$, which is a conservative value consistent with state-of-the-art reconciliation schemes. Note that one can make the best of both worlds (continuous and discrete modulation) by using a specific eight-dimensional continuous modulation (see Ref. [19] for a detailed presentation of such a protocol).

V. PARAMETER ESTIMATION

For discrete-variable QKD protocols, it turns out that the principal finite-size effect, in terms of its consequences on the secret key rate, is the parameter estimation [12]. A similar situation is expected for CV protocols, the main problem being, without any doubt, estimation of the excess noise ξ.

In this section, we study the parameter estimation procedure for CV protocols, without postselection. Quite fortunately, despite being described in an infinite-dimensional Hilbert space, these protocols display only a few parameters that need to be estimated: these are the parameters characterizing the covariance matrix of the state shared by Alice and Bob in the entanglement-based version of the protocol [37]. On the positive side, this covariance matrix can be symmetrized through a technique similar to the one explained in [38], and this symmetrized version is described by only two unknown parameters (in addition to Alice's modulation variance). On the negative side, to be able to estimate the two relevant parameters, it seems that one still has to make the assumption of a Gaussian channel. This does not look as a very constraining assumption, as it is known that Alice and Bob can always assume their state to be Gaussian (see [17]). However, this result has only been established in the asymptotic limit, and one cannot yet rigorously exclude the (improbable) situation where this result does not hold in general.

A non-Gaussian attack that would exploit such a possible loophole would have to be quite subtle. Indeed, the usual security proof stating that Gaussian states are the ones which minimize the secret key rate cannot be used here because the proof implicitly assumes knowledge of the covariance matrix. For a *given* covariance matrix, the state maximizing Eve's information is Gaussian. The only possible loophole would be that because the covariance matrix is not perfectly known in a finite-size scenario, there might exist a non-Gaussian state, compatible with the estimated covariance matrix computed with a Gaussian assumption, that would be better for Eve than the Gaussian state estimated by Alice and Bob. Let us detail things a bit. Let us note $\mathcal{S}^g_{\epsilon_{\mathrm{PE}}}$, the set of states compatible with the results of the parameter estimation, under a Gaussian model, except with probability ϵ_{PE}. Let us note $\mathcal{S}^{ng}_{\epsilon_{\mathrm{PE}}}$, the set of states compatible with the results of the parameter estimation, under a general, non-Gaussian model, except with probability ϵ_{PE}. It is not easy to compare the two sets *a priori*, but one can imagine that they likely get closer and closer as ϵ_{PE} goes to 0 (we typically consider $\epsilon_{\mathrm{PE}} = 10^{-10}$). In the following, because we make the Gaussian assumption, we consider the Gaussian state $\rho^g \in \mathcal{S}^g_{\epsilon_{\mathrm{PE}}}$, which maximizes Eve's information (note that $\mathcal{S}^g_{\epsilon_{\mathrm{PE}}}$ is not composed of Gaussian states only, but we know that the worst case, from Alice and Bob's point of view, is Gaussian). However, it is not yet possible to exclude the existence of a non-Gaussian state $\rho^{ng} \in \mathcal{S}^{ng}_{\epsilon_{\mathrm{PE}}}$ such that the secret key rate obtained for ρ^{ng} is strictly lower than the one obtained for ρ^g. This is, however, quite unlikely.

For this reason, we conjecture that the Gaussian optimality still holds in a nonasymptotic scenario, and in the following, we make the assumption of a Gaussian channel. Again, we insist on the point that even if this conjecture were proven wrong, the bounds computed here would still be quite accurate. Note, however, that this conjecture was recently established in the case of protocols with a Gaussian modulation [39].

Our goal here is to compute $S_{\epsilon_{\mathrm{PE}}}(y:E)$, the maximal value of the Holevo information between Eve's and Bob's classical variable compatible with the statistics except with probability ϵ_{PE}. The nice property of CV protocols without postselection is that $S(y:E)$ can be bounded from above by a function of two parameters only. More precisely, this function depends on the covariance matrix Γ_{AB} of the state ρ_{AB} shared by Alice and Bob in the entanglement-based version of the protocol (see [39–41] for protocols with a Gaussian modulation and [17,18] for protocols with a discrete modulation). One can always assume that Γ_{AB} take the following form:

$$\Gamma = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & (TV_A+1+T\xi)\mathbb{1}_2 \end{pmatrix}, \tag{11}$$

where V_A is the variance of Alice's modulation in the *prepare and measure* scheme, and T and ξ refer to the experimentally estimated effective transmission and excess noise of the channel [38]. The parameter Z is a function of V_A which depends on the modulation scheme. For instance, one has $Z_{\mathrm{Gauss}} = \sqrt{V_A^2 + 2V_A}$ in the case of a Gaussian modulation. For a discrete modulation, Z has a more complicated expression but turns out to be almost equal to Z_{Gauss} for small variances (see [17]): for the two-state protocol, one has

$$Z_2 = V_A \frac{1+e^{-2V_A}}{\sqrt{1-e^{-2V_A}}}, \tag{12}$$

and for the four-state protocol, one has

$$Z_4 = V_A \left(\frac{\lambda_0^{3/2}}{\lambda_1^{1/2}} + \frac{\lambda_1^{3/2}}{\lambda_2^{1/2}} + \frac{\lambda_2^{3/2}}{\lambda_3^{1/2}} + \frac{\lambda_3^{3/2}}{\lambda_0^{1/2}} \right), \tag{13}$$

where

$$\begin{aligned} \lambda_{0,2} &= \tfrac{1}{2} e^{-V_A/2} \left[\cosh(V_A/2) \pm \cos(V_A/2) \right], \\ \lambda_{1,3} &= \tfrac{1}{2} e^{-V_A/2} \left[\sinh(V_A/2) \pm \sin(V_A/2) \right]. \end{aligned} \tag{14}$$

Finally, for the continuous eight-dimensional modulation [19], one has

$$Z_8 = \frac{1}{2} e^{-2V_A} \sum_{k=0}^{\infty} \frac{\sqrt{k+4}}{k!} V_A^{k+\frac{1}{2}}. \tag{15}$$

These various parameters are related through

$$Z_2 < Z_4 < Z_8 < Z_g. \tag{16}$$

To compute $S_{\epsilon_{\mathrm{PE}}}(y:E)$, one simply needs to evaluate $\Gamma_{\epsilon_{\mathrm{PE}}}$, the covariance matrix compatible with the data except with probability ϵ_{PE}, which maximizes the Holevo information between Eve's and Bob's classical data.

The estimation of $\Gamma_{\epsilon_{\mathrm{PE}}}$ is made through the sampling of $m \equiv N - n$ couples of correlated variables $(x_i, y_i)_{i=1\cdots m}$. As we said before, we consider here a normal model for these

variables. Within this model, Alice and Bob's data are linked through the following relation:[4]

$$y = tx + z, \tag{17}$$

which is a normal linear model parametrized by $t = \sqrt{T} \in \mathbb{R}$ and where z follows a centered normal distribution with unknown variance $\sigma^2 = 1 + T\xi$. The random variable x can be either a normal random variable with variance V_A, in the case of the CV QKD protocol with a Gaussian modulation, or an unbiased Bernoulli random variable taking values $\pm\sqrt{V_A}$ in the case of the two- and four-state protocols (and a similar situation occurs for the continuous eight-dimensional modulation). At this point, it is worth considering the dependence of $S(y:E)$ in the variables t and σ^2. One can, in particular, check numerically that the following inequalities hold for any value of the modulation variance V_A and for all modulation schemes considered here:

$$\left.\frac{\partial S(y:E)}{\partial t}\right|_{\sigma^2} < 0 \quad \text{and} \quad \left.\frac{\partial S(y:E)}{\partial \sigma^2}\right|_{t} > 0. \tag{18}$$

This means that one can find the covariance matrix $\Gamma_{\epsilon_{\mathrm{PE}}}$ which minimizes the secret key rate with a probability of at least $1 - \epsilon_{\mathrm{PE}}$:

$$\Gamma_{\epsilon_{\mathrm{PE}}} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & t_{\min} Z \sigma_z \\ t_{\min} Z \sigma_z & \left(t_{\min}^2 V_A + \sigma_{\max}^2\right)\mathbb{1}_2 \end{pmatrix}, \tag{19}$$

where $t_{\min}$ and $\sigma^2_{\max}$ correspond, respectively, to the minimal value of t and the maximal value of σ^2 compatible with the sampled data, except with probability $\epsilon_{\mathrm{PE}}/2$. Note that this means that the confidence region we consider here is simply a two-dimensional rectangle. One could obviously study more complicated regions that might slightly improve the final key rate. However, here we prefer to restrict ourselves to this simpler solution, which has the advantage of displaying the same features as a more complicated model does but without drowning them with overly technical mathematical details.

Maximum-likelihood estimators $\hat{t}$ and $\hat{\sigma}^2$ are known for the normal linear model [42]:

$$\hat{t} = \frac{\sum_{i=1}^m x_i y_i}{\sum_{i=1}^m x_i^2} \quad \text{and} \quad \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^m (y_i - \hat{t}x_i)^2. \tag{20}$$

Moreover, $\hat{t}$ and $\hat{\sigma}^2$ are independent estimators with the following distributions:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^m x_i^2}\right) \quad \text{and} \quad \frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \tag{21}$$

where t and σ^2 are the true values of the parameters. This allows us to compute $t_{\min}$, a lower bound for t, and $\sigma^2_{\max}$, an upper bound for σ^2 in the limit of large m:[5]

$$\begin{aligned} t_{\min} &\approx \hat{t} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}^2}{m V_A}}, \\ \sigma^2_{\max} &\approx \hat{\sigma}^2 + z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{22}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ is such that $1 - \mathrm{erf}(z_{\epsilon_{\mathrm{PE}}/2}/\sqrt{2})/2 = \epsilon_{\mathrm{PE}}/2$ and erf is the error function defined as

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2} dt. \tag{23}$$

In a given experiment, one can simply compute the values of both estimators, $\hat{t}$ and $\hat{\sigma}^2$, and plug them into Eq. (22) to get the values of $t_{\min}$ and $\sigma^2_{\max}$ and, finally, the value of $S_{\epsilon_{\mathrm{PE}}}(y:E)$. To keep analyzing the protocol from a theoretical point of view, we take for $\hat{t}$ and $\hat{\sigma}^2$ their expected values:

$$\begin{aligned} \mathbb{E}[\hat{t}] &= \sqrt{T}, \\ \mathbb{E}[\hat{\sigma}^2] &= 1 + T\xi. \end{aligned} \tag{24}$$

Using these values, one can compute $t_{\min}$ and $\sigma^2_{\max}$:

$$\begin{aligned} t_{\min} &\approx \sqrt{T} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\xi}{m V_A}}, \\ \sigma^2_{\max} &\approx 1 + T\xi + z_{\epsilon_{\mathrm{PE}}/2}\frac{(1+T\xi)\sqrt{2}}{\sqrt{m}}. \end{aligned} \tag{25}$$

Finally, one gets the covariance matrix $\Gamma_{\epsilon_{\mathrm{PE}}}$, which should be used to compute the expected secret key rate $S_{\epsilon_{\mathrm{PE}}}(y:E)$ in the finite case:

$$\mathbb{E}[\Gamma_{\epsilon_{\mathrm{PE}}}] = \begin{pmatrix} \Gamma + 0 & \Delta_Z \sigma_z \\ \Delta_Z \sigma_z & \Delta_B \mathbb{1}_2 \end{pmatrix}, \tag{26}$$

with

$$\begin{aligned} \Delta_Z &= -z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\xi}{m V_A}}, \\ \Delta_B &= \frac{z_{\epsilon_{\mathrm{PE}}/2}}{\sqrt{m}}\left((1+T\xi)\sqrt{2} - 2\sqrt{T V_A}\right) + z^2_{\epsilon_{\mathrm{PE}}/2}\frac{1+T\xi}{m}. \end{aligned}$$

At the first order, for long distances, the main effect is clearly the uncertainty on the excess noise. The *effective* excess noise $\Delta_m\xi$ due to the imprecision of the estimation is given by

$$\Delta_m \xi \approx \frac{z_{\epsilon_{\mathrm{PE}}/2}\sqrt{2}}{T\sqrt{m}}. \tag{27}$$

We display in the next section the effect of the parameter estimation on the secret key rate, but we can already give a hint about the block length that will generally be required

[4]The simplicity of this relation comes from the fact that the state ρ_{AB} and, consequently, the quantum channel are symmetrized.

[5]Indeed, for large m, the χ^2 distribution converges to a normal distribution. The approximation is almost exact in our case, as we consider values of m (much) larger than 10^6.

for a given distance. Indeed, from Eq. (27), one immediately obtains

$$m \approx \frac{2z^2_{\epsilon_{\mathrm{PE}}/2}}{T^2\Delta_m\xi^2}. \tag{28}$$

For $\epsilon_{\mathrm{PE}} = 10^{-10}$, one has $z_{\epsilon_{\mathrm{PE}}/2} \approx 6.5$, and if one requires $\Delta_m\xi \approx 1/100$, which is a typical value for true excess noise [30], then the number of samples required scales as a function of the transmission as

$$m \propto \frac{10^6}{T^2}. \tag{29}$$

For instance, if the distance between Alice and Bob is 50 km, then $T = 10^{-1}$, which means that one expects the block length to be of the order of 10^8, which is barely realistic. If the distance is 100 km, then the block length should be of the order of 10^{10}, which is much more complicated. We see in Sec. VI that the reality is even worse than that.

Before proceeding with the numerical results, we now discuss two technical points linked to the problem of parameter estimation. First, we come back to the assumption made previously that, in a typical experiment, the value of the estimators will roughly correspond to the true value of the parameter. Then we hint on alternative approaches to improve estimation of the parameters for CV QKD protocols, which might be more economical in terms of the number of samples required, but whose mathematical analysis is much more involved.

1. Expected secret key rate or most probable secret key rate

For a given experiment, the secret key rate can be computed and is a function of the observed values of the estimators $\hat{t}$ and $\hat{\sigma}^2$ (but not only). One can write $k_{\mathrm{exp}} = f(\hat{t},\hat{\sigma}^2)$. From a theoretical point of view, that is, without performing the actual experiment, there are two secret key rates that can be computed.

The first possibility, considered, for instance, in [12], is to compute the secret key rate k_1 obtained for the expected values of the parameters:

$$k_1 \equiv f(\mathbb{E}[\hat{t}],\mathbb{E}[\hat{\sigma}^2]). \tag{30}$$

In some sense, this corresponds to what one could call the most probable secret key rate. This interpretation, however, is not correct.

The correct theoretical secret key rate k_2 is given by the expected value of the secret key rate, that is,

$$k_2 \equiv \mathbb{E}[f(\hat{t},\hat{\sigma}^2)]. \tag{31}$$

Obviously, this value is much more difficult to evaluate in general, as one needs to know the probability distributions of both estimators, $\hat{t}$ and $\hat{\sigma}^2$, whereas in the case of k_1, one just needs to know the expected values. Fortunately, we see in Sec. VI that in fact both values are remarkably close, meaning that one can always safely use k_1 as the secret key size.

2. More economical parameter estimation procedures

An interesting characteristic of CV QKD protocols is that it might be possible to perform the parameter estimation without sacrificing any data. This is obviously something impossible in discrete-variable QKD where estimating the QBER requires that Alice and Bob disclose some of their data.

In CV QKD, however, the bit used for the raw key is encoded in only some of Bob's classical data. Let us take the example of the four-state protocol [17]. In this case, Bob's data $\{y_i\}_{1\leqslant i\leqslant N}$ are real numbers and the raw key elements are simply given by the sign of the variables y_i. The absolute value is sent to Alice through the public, authenticated channel, and Alice uses it to perform the reverse reconciliation procedure.

In the parameter estimation procedure that we have described, Alice and Bob would agree on a certain subset of their data and completely disclose their data in this subset. This means that the absolute values of the rest of Bob's data are not used for this parameter estimation, whereas it manifestly contains information concerning the covariance matrix of the state shared by Alice and Bob. One could certainly use this information to improve the accuracy of the parameter estimation or, equivalently, obtain the same accuracy while using fewer samples, therefore increasing the final secret key rate. However, the statistics techniques necessary for this study are beyond the scope of this paper, and we do not address this question more extensively here.

Before concluding this section, we give another possible way to improve on the parameter procedure presented here. For CV QKD protocols, it is clear that the critical parameter to estimate is the excess noise. The transmission, in contrast, is less critical for two reasons: first, it can be estimated more precisely than the excess noise with the same amount of data (in particular, the relative uncertainty for the transmission is smaller than that for the excess noise); and second, the secret key rate is much more sensitive to variations in the excess noise than in the transmission. Therefore, one could use the following method to estimate the transmission and the parameters:

1. The transmission is estimated through the same procedure as before, with m samples.
2. Bob uses the *totality* of his data to compute an estimation of the variance of his data. Then, using the relation $\langle y^2\rangle = 1 + TV_A + T\xi$ and his estimation of T, Bob infers an estimation for the excess noise.

This approach seems better than the one studied above. However, it involves computing two *dependent* estimators, and the probability distributions of the estimators (necessary to compute confidence regions) are not known.

Therefore, in this paper we use a likely suboptimal procedure to perform the parameter estimation, but this procedure allows for the computation of explicit bounds. The question of what is the best parameter estimation procedure in the case of CV QKD is still open and is certainly worth investigating further, as it turns out that the parameter estimation is an important problem if one wants to distribute secret keys over a long distance, while using realistic block lengths.

VI. RESULTS

Before we discuss the results in terms of secret key rate, we start by considering the specific influence of $\Delta(n)$, related to privacy amplification and defined in Eq. (4). We then study the influence of the parameter estimation.

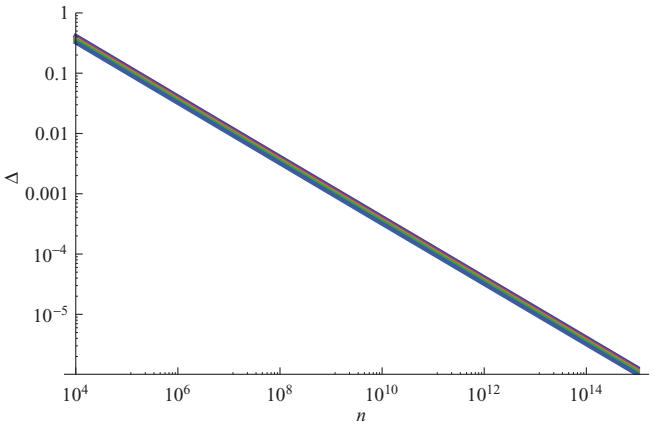

FIG. 1. (Color online) Parameter $\Delta(n)$ as a function of n for various values of $\bar{\epsilon}$ and ϵ_{PA}. From top to bottom, $\bar{\epsilon} = \epsilon_{\mathrm{PA}} = 10^{-6}$, 10^{-7}, 10^{-8}, 10^{-9}, and 10^{-10}.

A. Influence of $\Delta(n)$

In Fig. 1, we plot the value of the parameter $\Delta(n)$ as a function of n, the size of the raw key. Here, we take $\dim\mathcal{H}_Y = 2$, since for all CV protocols we consider, the raw key is encoded on bits [17,19,31]. Among notable features, one sees that the value of $\Delta(n)$ does not critically depend on the parameters $\bar{\epsilon}$ and ϵ_{PA}, which need to be optimized in theory. One can easily see from the curve that, for the plotted domain ($n \geqslant 10^4$), $\Delta(n)$ is essentially determined by the first term in Eq. (4),

$$\delta(n) \simeq 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}}. \tag{32}$$

The important lesson is the large value of $\Delta(n)$, even for (seemingly) quite large sizes of the raw key. In particular, one observes that $\Delta(n)$ is larger than 0.01 for raw key sizes smaller than 10^7. In practice, this means that if the asymptotic secret key rate is below 0.01 bit per channel used, then if one wants to take into account finite-size effects, one has to use block lengths larger than 10 million to be able to claim to have truly distributed a secret key among distance parties.

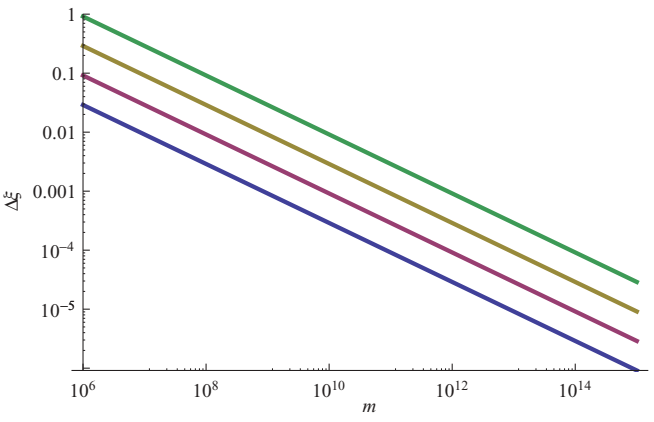

FIG. 2. (Color online) Parameter $\Delta_m\xi$ as a function of m for $\epsilon_{\mathrm{PE}} = 10^{-10}$ (in fact, $\Delta_m\xi$ does not depend too critically on the precise value of ϵ_{PE}, and one obtains very similar plots for $\epsilon_{\mathrm{PE}} = 10^{-5}$, e.g.). From bottom to top, we consider channel losses of 5, 10, 15, and 20 dB. With a perfect homodyne detection (quantum efficiency equal to 1), this is equivalent to distances of 25, 50, 75, and 100 km, respectively.

B. Influence of the parameter estimation

Here we focus on the value of the *effective* excess noise $\Delta_m\xi$ due to the finite precision of the parameter estimation. In Fig. 2, we display this effective excess noise as a function of m, the number of samples used in the parameter estimation. From Fig. 2, it is clear that the parameter estimation has a major impact on the final secret key rate. Indeed, the four-state protocol, for instance, which can achieve remarkably long distances in the asymptotic limit, requires very low values of the excess noise, typically less than 1%, to distribute key over distances close to 100 km. Here, we see that such parameters require sampling of 10 billion couples of correlated data! For this reason, it is doubtful that continuous-variable QKD is very practical over distances much larger than 100 km, at least with the security proofs presently available. Note that a similar situation is also true for discrete-variable protocols.

C. Secret key rate in the finite-size scenario

Here we first consider the secret key rate k_1, which is the one obtained if the estimators $\bar{t}$ and $\bar{\sigma}^2$ are equal to their expected values. We do not proceed to a complete optimization of the various parameters, since it will not fundamentally change the results, and instead take the following values:

$$\begin{aligned} \epsilon_{\mathrm{EC}} = \bar{\epsilon} = \epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}} &= 10^{-10}, \\ \epsilon &\approx 10^{-10}, \\ m = n &= N/2, \\ \beta &= 80\%, \\ \eta &= 0.6. \end{aligned} \tag{33}$$

The choice for ϵ is very conservative, but it turns out that the secret key rate does not depend very critically on ϵ (a similar observation was made in [11]). The choice to use half of the data for the parameter estimation procedure results from the fact that the block size is almost entirely decided by the number of data actually sampled. The reconciliation efficiency of 80% is a conservative value [17,31]. Finally, we consider the quantum efficiency of the homodyne detection to be 60%, which corresponds to a typical experimental parameter [30]. Moreover, we consider the paranoid mode where the electronic noise is null. Remember that two models can be considered when discussing the security of CV QKD: either the electronic noise of Bob's detection is considered regular excess noise (paranoid mode) or it is attributed to Bob's detection (realistic mode). The second case is more natural, but it implies that Bob's detection stage should be calibrated. As a first approximation, the paranoid mode without electronic noise is equivalent (in the asymptotic regime) to the case of a realistic mode where the electronic noise is non-negligible but is not supposed to be caused by the action of an eavesdropper. In the finite-size regime, one can still make the assumption that Bob's detection is very well calibrated and that there is virtually no uncertainty in the value of the electronic noise. As a consequence, to avoid too many technical details, we present here results obtained in the paranoid scenario without

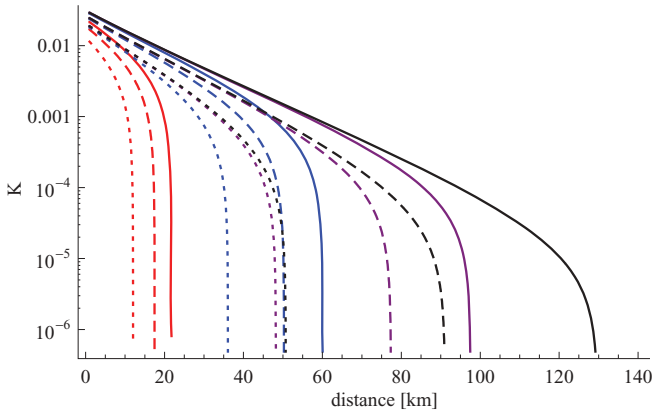

FIG. 3. (Color online) Secret key rate for the four-state protocol. From left to right, curves correspond, respectively, to block lengths of $N = 10^8$, 10^{10}, 10^{12}, and 10^{14}. Full lines, dashed lines, and dotted lines correspond, respectively, to an expected value of the excess noise of 0.001 (optimistic), 0.005 (realistic), and 0.01 (conservative). The secret key rate is null for a block length of 10^6.

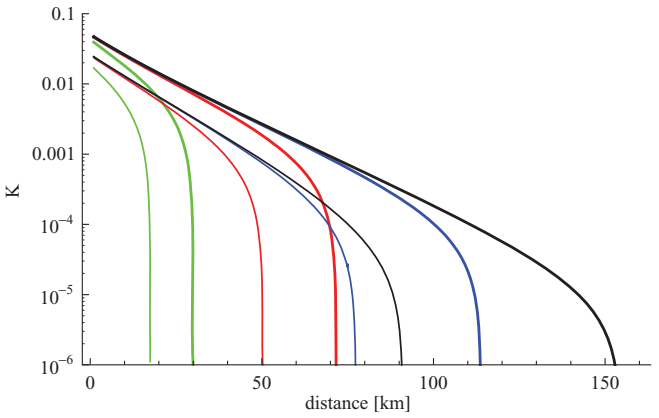

FIG. 4. (Color online) Secret key rate for the four-state (thin curves) and eight-dimension (thick curves) protocols obtained for an expected realistic value of the excess noise of 0.005 and for $\epsilon_{\mathrm{PE}} = 10^{-10}$. From left to right, the block length N is equal to 10^8, 10^{10}, 10^{12}, and 10^{14}. The secret key rate is null for a block length of 10^6. The eight-dimension protocol is better for all curves.

electronic noise. Note that this solution was also chosen in the review by Scarani *et al.* [1].

The secret key rates displayed in Fig. 3 correspond to the key rate one can expect if the estimators give the true value of the parameters. As we argued earlier, a more relevant secret key rate corresponds to the *expected* value computed for the probability distributions of the estimators $\hat{t}$ and $\hat{\sigma}^2$.

As already explained, the most important parameter for the final secret key rate is the excess noise. This means that one should mainly consider the probability distribution of the estimator $\hat{\sigma}^2$. According to Equation (21), one has

$$\frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1). \tag{34}$$

For large m, the χ^2 distribution tends to a normal distribution, which translates into

$$\hat{\sigma}^2 \sim \mathcal{N}\left(\sigma^2, \frac{2\sigma^4}{m}\right), \tag{35}$$

where, as before, σ^2 corresponds to the true value of the parameter. Here we can therefore compute an approximate value of the expected secret key rate k_2 as

$$k_2 = \mathbb{E}[f(\hat{t},\hat{\sigma}^2)] \approx \mathbb{E}[f(t,\hat{\sigma}^2)], \tag{36}$$

since $\hat{t}$ has a probability distribution peaked around the true value of the parameter t and because f does not depend critically on the value of t. Using the normality of the random variable $\hat{\sigma}^2$, one obtains

$$k_2 = \int_{-\infty}^{\infty} \frac{1}{2\sigma^2}\sqrt{\frac{m}{\pi}} \exp\left(-m\frac{(s-\sigma^2)^2}{4\sigma^4}\right) f(t,s)\, ds. \tag{37}$$

It turns out that the behavior of k_2 is numerically indistinguishable from the value of k_1. For this reason, we do not display it here. The main consequence is that one can, in very good approximation, compute the final key rate by considering the expected values of the parameters being estimated. This is rather fortunate, as computing k_2 is much more demanding from a computing point of view than computing k_1.

Finally, in Fig. 4, we display the results for the recently proposed eight-dimension protocol described in detail in Ref. [19], which outperforms the four-state protocol in realistic cases and may also be easier to implement.

VII. PERSPECTIVES

This article has laid down the basis of finite-size analysis of CV QKD protocols, but several problems remain open and should be addressed in further studies. First, a basic tool used in the asymptotic regime is the Gaussian optimality theorem [40,41], which remains valid for collective attacks, even in the case of protocols which do not use a Gaussian modulation, that is, protocols designed to perform well over long distance [17,19]. Whereas using this theorem is completely legitimate in the asymptotic regime [40,41], it is not so clear in a finite-size scenario, where very subtle (and highly improbable) attacks might perform slightly better. Such attacks would have to be based on the idea of fooling Alice and Bob by having them make wrong assumptions in the parameter estimation procedure. This subtle point (given that the blocks have to be very large anyway) deserves further analysis.

Second, and perhaps more importantly, one should prove whether or not collective attacks are optimal in the finite-size setting. If this is the case, then all is for the best, and the bounds derived here are accurate. But if collective attacks are not optimal, then one needs to come up with bounds as tight as possible for coherent attacks. On this subject, it would seem that adapting the postselection technique from [29] to continuous variables (using, e.g., symmetries in phase space as explained in [38]) would lead to much tighter bounds than the one currently available through an exponential version of de Finetti theorem for infinite dimensional Hilbert spaces [7].

Despite the fact that there are still open problems concerning the finite-size analysis of CV QKD, some lessons can already be learned. First, it should be emphasized again

that the problem of the reconciliation efficiency at a low SNR is essentially solved by new protocols using discrete modulation and high-efficiency reconciliation codes, such as the four-state [17] and eight-dimension [19] protocols. Then, as is the case for discrete-variable QKD protocols, the most important remaining finite-size effect is the limited accuracy of the parameter estimation. For CVQKD, the main issue is the value of the channel excess noise, which already has a critical effect for values as small as 1% of the shot noise. Nevertheless, operating windows do exist, provided that both the "real" excess noise is very small, and the block size is very large. In such circumstances, a secure key distribution over distances larger than 50 km seems quite feasible, especially with the eight-dimension protocol [19], as shown in Fig. 4.

ACKNOWLEDGMENTS

The authors acknowledge the hospitality of CQT Singapore during the workshop "Quantum Cryptography with Finite Resources" (4–6 December 2008). This work received financial support from Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05) and SEQURE (ANR-07-SESU-011-01) and from the EU ERC Starting Grant PERCENT.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[5] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[6] R. Renner, Ph.D. thesis, ETH Zurich, 2005, e-print arXiv:quant-ph/0512258.
[7] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[8] V. Scarani and C. Kurtsiefer, e-print arXiv:0906.4547.
[9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[10] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[11] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[12] R. Y. Q. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[13] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[14] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, e-print arXiv:0705.3081.
[15] L. Sheridan and V. Scarani, e-print arXiv:1003.5464.
[16] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[17] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[18] A. Leverrier and P. Grangier, e-print arXiv:1002.4083.
[19] A. Leverrier and P. Grangier, e-print arXiv:1005.0328.
[20] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[21] J. Lodewyck and P. Grangier, Phys. Rev. A **76**, 022332 (2007).
[22] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Phys. Rev. A **76**, 052301 (2007).
[23] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Phys. Rev. A **79**, 012307 (2009).
[24] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[25] Y. Sano, R. Matsumoto, and T. Uyematsu, e-print arXiv:1003.5766.
[26] S. Watanabe, R. Matsumoto, and T. Uyematsu, Phys. Rev. A **78**, 042316 (2008).
[27] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[28] R. Renner, Nature Phys. **3**, 645 (2007).
[29] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[30] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).
[31] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[32] S. Popescu, A. Short, and A. Winter, Nature Phys. **2**, 754 (2006).
[33] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[34] R. Renner and S. Wolf, in *IEEE International Symposium on Information Theory 2004* (2004), p. 233.
[35] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[36] M. Bloch, A. Thangaraj, S. McLaughlin, and J. Merolla, in *IEEE Information Theory Workshop, 2006. ITW'06 Punta del Este* (2006), pp. 116–120.
[37] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[38] A. Leverrier, E. Karpov, P. Grangier, and N. Cerf, New J. Phys. **11**, 115009 (2009).
[39] A. Leverrier and P. Grangier, Phys. Rev. A **81**, 062314 (2010).
[40] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[41] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[42] A. Montfort, *Cours de statistique mathématique* (Economica, London, 1997).