Analysis of imperfections in practical continuous-variable quantum key distribution

Paul Jouguet,[1,2] Sébastien Kunz-Jacques,[2] Eleni Diamanti,[1] and Anthony Leverrier[3]

[1]*Telecom ParisTech, Laboratoire Traitement et Communication de l'Information, Centre National de la Recherche Scientifique,*
46 Rue Barrault, 75634 Paris Cedex 13, France
[2]*SeQureNet, 23 Avenue d'Italie, 75013 Paris, France*
[3]*Institute for Theoretical Physics, Eidgenssische Technische Hochschule Zurich, 8093 Zurich, Switzerland*

As quantum key distribution becomes a mature technology, it appears clearly that some assumptions made in the security proofs cannot be justified in practical implementations. This might open the door to possible side-channel attacks. We examine several discrepancies between theoretical models and experimental setups in the case of continuous-variable quantum key distribution. We study in particular the impact of an imperfect modulation on the security of Gaussian protocols and show that approximating the theoretical Gaussian modulation with a discrete one is sufficient in practice. We also address the issue of properly calibrating the detection setup and in particular the value of the shot noise. Finally, we consider the influence of phase noise in the preparation stage of the protocol and argue that taking this noise into account can improve the secret key rate because this source of noise is not controlled by the eavesdropper.

PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a cryptographic primitive allowing two distant parties, Alice and Bob, to distill secret keys in an untrusted environment controlled by an eavesdropper, Eve [1]. Among quantum information technologies, QKD is one of the most advanced and reaches already commercial applications. The main argument in favor of QKD is its provable security based on the laws of quantum mechanics; it is therefore particularly important to make sure that the security proofs derived for theoretical protocols can be applied to real-world implementations. This is unfortunately never really the case because the security proofs usually assume idealized implementations, which do not take into account all possible experimental imperfections. This opens the door to potential security loopholes [2] that might be successfully exploited by an attacker. Such side-channel attacks have already been demonstrated against commercial QKD systems [3,4].

There are basically two ways around side-channel attacks. A drastic solution consists in deciding that the systems held by Alice and Bob should not be trusted: this is the device-independent paradigm, based on the violation of a Bell inequality [5]. While appealing in theory, this paradigm does not offer a practical solution since violating a Bell inequality in a loophole-free fashion has not been achieved until now. A more practical way to address side-channel attacks aims at refining the theoretical models used for security proofs in order to include various sources of experimental imperfections. This involves, for instance, developing better models for the state preparation, including the light source, the modulation, and the noise, and for the detection including the quantum efficiency and the calibration of the noise.

In this paper, we follow the second approach in the case of continuous-variable (CV) QKD protocols. The main specificity of these protocols is that they use a homodyne detection instead of single-photon counters, which makes them attractive from a practical perspective. Moreover, they are compatible with wavelength division multiplexing [6], which is an important advantage when it comes to integrating QKD in real-world telecommunication networks. CVQKD protocols are proven secure against coherent attacks [7–9] and, asymptotically, the secret key rate is given by the Devetak-Winter formula [10,11] corresponding to collective attacks [12,13]. At the theoretical level, CVQKD protocols therefore present the same level of security as those based on photon counting, such as BB84 [14].

Here, we focus on Gaussian prepare-and-measure CVQKD protocols, which have already been demonstrated experimentally [15–22] (see [23] for a recent review of all CVQKD protocols). In particular, we consider the GG02 protocol [24] where Alice generates coherent states with a Gaussian modulation and sends them to Bob, who performs a homodyne measurement for a randomly chosen quadrature. By repeating this process a large number of times, Alice and Bob obtain correlated classical data, from which they can extract identical strings through the process of reconciliation [25] and then obtain a secret key using privacy amplification.

We study three kinds of imperfections that occur in all implementations of this protocol and see how they affect its security and the secret key rate. The first imperfection concerns the modulation, which, in practice, can only approach the theoretical Gaussian modulation. Indeed, a Gaussian distribution is not only continuous but unbounded and therefore cannot be exactly achieved since, for instance, an infinite amount of randomness would be required. We show that the impact on security is not significant when the Gaussian distribution is replaced by a bounded, discrete approximation. However, deviations from a perfect discretized distribution degrade the security. The second source of imperfection comes from finite-size effects and in particular from the calibration of the detection setup. While a first study in this direction has already considered statistical estimation of the transmittance and excess noise of the channel [26], it assumed that the quantum efficiency and the electronic noise of the detection, and more importantly the shot-noise level, were all perfectly calibrated. Here, we consider these effects in detail and examine their impact on the secret key rate and distance. Finally, we study the effect of phase noise in the preparation process of the

protocol. This noise is unavoidable but one can safely assume that it is not controlled by the eavesdropper. We therefore show that, by calibrating it properly, one can increase the secret key rate of the protocol.

The three kinds of imperfections are discussed in Secs. II–IV of the paper, respectively.

II. SECURITY OF GAUSSIAN PROTOCOLS WITH AN IMPERFECT MODULATION

We first consider an issue present in all implementations of CVQKD with a Gaussian modulation, namely, that it is impossible to use an exact Gaussian modulation in practice. In the ideal scenario for the prepare-and-measure protocol, for each signal to be sent, Alice is supposed to draw two random normal variables $q, p \sim \mathcal{N}(0, V_A)$ and to prepare the coherent state $|q + ip\rangle$ centered on the point (q, p) in phase space. Unfortunately, in practice, ignoring phase noise, the coherent state really prepared by Alice is centered on (q', p') instead, where (q', p') is a point on a finite grid, approximating the ideal value of (q, p). This is unavoidable for several reasons. First, the analog-to-digital converters that drive the physical modulators used in practice produce discrete voltages; they typically have a bit depth of 10 like in [20]. Second, intensity modulators only work in some finite range of values, whereas the Gaussian distribution is unbounded. Another hardware constraint is the throughput of the physical random number generators (for example Quantis, from ID Quantique, is limited to 16 Mbits/s). But there are also software limitations: one does not want to use too much randomness in order to draw the Gaussian variables q and p out of the uniform variables provided by the physical random number generator because this requires computational power. For these reasons, it is useful to know how well the Gaussian modulation needs to be approximated in order to get a reasonably good level of security.

Intuitively, the presence of shot noise hides the small imperfections of the modulation and the security should not be compromised provided that the grid of (q', p') is sufficiently fine-grained compared to the value of the shot noise. Figure 1
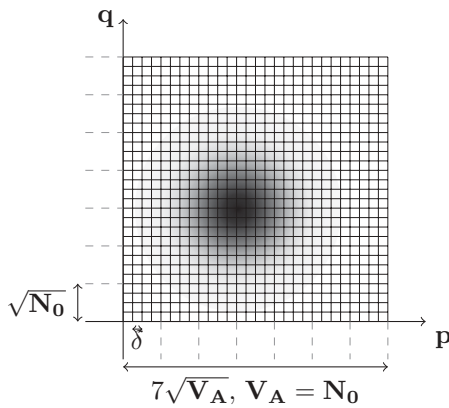

FIG. 1. Discretization grid used to approximate a Gaussian modulation in phase space. The modulation variance V_A is chosen to be equal to the shot noise N_0. The distribution is truncated to seven standard deviations and discretized in steps of 1/4 of shot-noise units. A coherent state of variance N_0 covers a large part of the grid, which results in hiding the small imperfections of the discretized modulation.

illustrates how fine the grid needs to be compared to the shot noise.

In order to analyze the security of the practical protocol, it is convenient to look at the situation from Bob and Eve's points of view. In the theoretical protocol, the state sent by Alice to Bob should be a thermal state from Eve's perspective, that is, a Gaussian mixture of coherent states. If Eve cannot distinguish the state sent in practice from a thermal state, then clearly the security of the protocol is not compromised by the approximated modulation. More precisely, if the trace distance between the ideal state and the actual state is bounded by ϵ_{prep}, and if the usual protocol (with perfect state preparation) is ϵ secure, then the true protocol is $(\epsilon + \epsilon_{\text{prep}})$ secure. Therefore, one simply needs to ensure that ϵ_{prep} can be made quite small, that is, on the order of 10^{-10} in a realistic implementation.

A. The quality of a Gaussian modulation

Let us write $\rho = \rho_{\text{th}} = \sum_{n=0}^{\infty} \frac{\bar{x}^n}{(\bar{x}+1)^{n+1}} |n\rangle\langle n|$ for the ideal thermal state and $\sigma = \sum_k \omega_k |\alpha_k\rangle\langle\alpha_k|$ for the state used in practice. Here ω_k corresponds to the probability of preparing the coherent state $|\alpha_k\rangle$.

We will compute the trace distance $||\rho - \sigma||_1$ between the two states, for two discretizations σ, either with a Cartesian or a polar grid. For both discretizations, we will use the gentle measurement lemma [27,28]:

Lemma 1: Gentle measurement. Let ρ be a state and Π be a projector. Then

$$||\rho - \Pi\rho\Pi|| \leqslant 2\sqrt{1 - \text{tr}(\Pi\rho\Pi)}. \quad (1)$$

Let us take $\Pi = |0\rangle\langle 0| + |1\rangle\langle 1| + \cdots + |Q-1\rangle\langle Q-1|$. The triangle inequality gives

$$||\rho - \sigma|| \leqslant ||\rho - \Pi\rho\Pi|| + ||\Pi\rho\Pi - \Pi\sigma\Pi|| + ||\Pi\sigma\Pi - \sigma||$$

$$\leqslant \sum_{n=Q}^{\infty} \langle n|\rho|n\rangle + \left|\sum_{n,m=0}^{Q-1} \langle n|\rho|m\rangle - \langle n|\sigma|m\rangle\right|$$
$$+ 2\sqrt{1 - \text{tr}(\Pi\sigma\Pi)}$$

$$\leqslant \sum_{n=Q}^{\infty} \frac{\bar{x}^n}{(\bar{x}+1)^{n+1}} + \sum_{n=0}^{Q-1} \left|\frac{\bar{x}^n}{(\bar{x}+1)^{n+1}} - \langle n|\sigma|n\rangle\right|$$

$$+ 2\sum_{0\leqslant n<m<Q} |\langle n|\sigma|m\rangle| + 2\sqrt{1 - \sum_{n=0}^{Q-1} \langle n|\sigma|n\rangle}$$

$$\leqslant \left(\frac{\bar{x}}{\bar{x}+1}\right)^Q + \Delta_{\text{diag}} + 2\Delta_{\text{nondiag}} + 2\sqrt{R_\sigma}, \quad (2)$$

with $\Delta_{\text{diag}} := \sum_{0\leqslant n<Q} |\frac{\bar{x}^n}{(\bar{x}+1)^{n+1}} - \langle n|\sigma|n\rangle|$, $\Delta_{\text{nondiag}} := \sum_{0\leqslant n<m<Q} |\langle n|\sigma|m\rangle|$, and $R_\sigma := 1 - \sum_{0\leqslant n<Q} \langle n|\sigma|n\rangle$. These three quantities can be estimated from the terms $\langle n|\sigma|m\rangle$, $0 \leqslant n, m < Q$.

Notice that $R_\rho := (\frac{\bar{x}}{\bar{x}+1})^Q$ does not depend on the actual approximation used, but only on the mean photon number $\bar{x}$ of the ideal thermal state. When using a Gaussian modulation of variance V_A (in shot-noise units), one has $\bar{x} = 2V_A$. This means that larger values of V_A require larger values of Q in order to obtain a good bound in Eq. (2). A typical range for V_A is [1,20]. For $V_A = 20$ and $\epsilon_{\text{prep}} = 10^{-10}$, one needs to

have $Q \approx 1000$ to ensure that $R_\rho \leqslant \epsilon_{\text{prep}}$. Furthermore one also needs $R_\sigma \leqslant \epsilon_{\text{prep}}^2$, which puts additional constraints on Q.

B. Cartesian approximation

Here, we consider an approximation of the form

$$\sigma = \sum_{k=-N}^{N} \sum_{l=-N}^{N} \omega_k \, \omega_l \, |\alpha_{kl}\rangle \, \langle\alpha_{kl}|, \tag{3}$$

where $\omega_k = \frac{\gamma_k}{\sum_k \gamma_k}$, $\gamma_k = e^{-q_k^2/(2V)}$, $q_k = p_k = \frac{A}{N}k$, $\alpha_{kl} = q_k + ip_k$, and A and N are two parameters to be optimized. The $|\alpha_{kl}\rangle$ are coherent states: $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$.

Therefore,

$$\langle n|\sigma|m\rangle = \sum_{k,l=-N}^{N} \omega_k \omega_l \langle n|\alpha_{kl}\rangle \langle\alpha_{kl}|m\rangle$$

$$= \sum_{k,l=-N}^{N} \omega_k \omega_l \, e^{-|\alpha_{kl}|^2} \frac{\alpha_{kl}^n \, \alpha_{kl}^{*\,m}}{\sqrt{n!m!}}.$$

From this expression, Δ_{diag}, Δ_{nondiag}, and R_σ can be evaluated numerically for any choice of $\bar{x} = 2V_A, Q, A$, and N. Once A is chosen, N is typically set so that $\delta = A/N$, the discretization step, has some predetermined value. Given V_A, let us show that a low $\epsilon_{\text{prep}} = ||\rho - \sigma||$ can be obtained with reasonable values of A and N. Assume $V_A = 20$, a rather large value corresponding to a Gaussian modulation of standard deviation $\sqrt{20}$; use (see Fig. 1) (1) $A = 7\sqrt{V_A}$, meaning that the actual Gaussian distribution is truncated to seven standard deviations, and (2) $N = \lceil 4A \rceil$, meaning that the distribution is discretized in steps of $1/4$ of shot-noise units. These choices can be used in practice: for $V_A = 20$, they require $2 \times \lceil 4 \times 7 \times \sqrt{V_A} \rceil + 1 = 253$ discretization steps, that is, an 8-bit discretization grid. The entropy of the corresponding pair of discretized Gaussian values is $2 \times 6.2 = 12.4$ bits. Source coding techniques enable us to use on average no more than this randomness quantity when drawing them in practice.

For $Q = 2000$ (chosen to get a sufficiently low value of R_σ), a numerical evaluation yields

$$\Delta_{\text{diag}} \leqslant 1.02 \times 10^{-11}, \tag{4}$$

$$\Delta_{\text{nondiag}} \leqslant 1.04 \times 10^{-11}, \tag{5}$$

$$R_\sigma \leqslant 1.09 \times 10^{-24}, \tag{6}$$

from which we deduce

$$||\rho - \sigma|| \leqslant 3.31 \times 10^{-11}. \tag{7}$$

In the above discretization scheme, the mass lost because of the distribution cutoff is evenly distributed among the remaining coherent states. Let us give a similar result for a slightly different cutoff scheme where the lost mass is added to $\omega_{\pm N}$ only: $\omega_k = \frac{A}{N} \frac{1}{\sqrt{2\pi V}} e^{-q_k^2/(2V)}$ for $-N + 1 \leqslant i \leqslant N - 1$, and $\omega_{-N} = \omega_N = (1 - \sum_{i=-N+1}^{N-1} \omega_k)/2$. For this scheme with the same parameters as before, we find

$$||\rho - \sigma|| \leqslant 2.98 \times 10^{-11}. \tag{8}$$

C. Polar approximation

The actual modulation devices implement a polar modulation because phase and intensity are modulated separately. It is therefore natural to investigate the discretization required in polar coordinates to obtain a good approximation of a thermal state.

Let us assume that the polar coordinates are discretized uniformly on $[0, R] \times [0, 2\pi]$. Let us note the discretized values as

$$r_k = \left(k + \frac{1}{2}\right) \frac{R}{K}, \quad k \in [\![0, K - 1]\!], \tag{9}$$

$$\theta_l = \left(l + \frac{1}{2}\right) \frac{2\pi}{L}, \quad l \in [\![0, L - 1]\!]. \tag{10}$$

We consider then an approximation of the form

$$\sigma = \frac{1}{L} \sum_k \omega_k \sum_l |\alpha_{kl}\rangle \, \langle\alpha_{kl}|, \tag{11}$$

where $\omega_k = \frac{\gamma_k}{\sum_k \gamma_k}$, $\gamma_k = r_k e^{-r_k^2/(2V)}$ and $|\alpha_{kl}\rangle = e^{-r_k^2/2} \sum_{n=0}^{\infty} \frac{r_k^n e^{in\theta_l}}{\sqrt{n!}} |n\rangle$. Therefore,

$$\langle n|\sigma|m\rangle = \frac{1}{L} \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \omega_k \langle n|\alpha_{kl}\rangle \langle\alpha_{kl}|m\rangle \tag{12}$$

$$= \frac{1}{L} \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \omega_k \, e^{-r_k^2} r_k^{n+m} \frac{e^{i(n-m)2\pi l/L}}{\sqrt{n!m!}} \tag{13}$$

$$= U_{nm,L} \sum_{k=0}^{K-1} \omega_k \frac{e^{-r_k^2} r_k^{n+m}}{\sqrt{n!m!}}, \tag{14}$$

with $U_{nm,L} = 1$ if L divides $n - m$, and $U_{nm,L} = 0$ otherwise.

Unfortunately, this polar discretization requires a finer discretization than the Cartesian one for the same approximation quality. For instance, with $V_A = 20$ as before, using $Q = L = 2000$ [thus eliminating the term Δ_{nondiag} altogether in Eq. (2)] and $R = 7\sqrt{V_A}$, a 17-bit discretization of the amplitude is required to obtain $|\langle 0|\rho|0\rangle - \langle 0|\sigma|0\rangle| \leqslant 10^{-10}$. Drawing values corresponding to this discretization uses 11 bits for the angle and 15.5 bits for the modulus on average. This situation can be improved by using, instead of regularly spaced r_k, points placed according to the Gauss quadratures method, especially the Gauss-Hermite variant: a 9-bit amplitude discretization entropy is found to be sufficient for $\epsilon_{\text{prep}} \leqslant 10^{-10}$. This is still slightly worse than the Cartesian grid, but could be improved further by making the angle discretization depend on the amplitude, as less points are needed in the vicinity of the origin.

D. Robustness of bounds

An important question related to the discretization is the robustness of the bounds given in the previous sections when the discretization grid is disturbed by some small systematic error term. This can happen, for instance, because of calibration errors or because of complex discretization effects due to the experimental setup. For example, an amplitude modulator generally produces an amplitude $A = \cos(cV + \phi)$,

where V is the voltage applied to it; since V is discrete, the modulated amplitude values are projected to a set that is the image of the discrete set of attainable voltages by the functional realized by the modulator. To model the effect of these errors, we added a small disturbance with Gaussian distribution of standard deviation σ_{error} to each point of the Cartesian grid and numerically computed the resulting ϵ_{prep}. With parameters as in Sec. II B, we get $||\rho - \sigma|| \approx 0.1 \times \sigma_{\mathrm{error}}$. This shows that obtaining $\epsilon_{\mathrm{prep}} \leqslant 10^{-10}$ in practice may be difficult; it is more realistic to expect $\epsilon_{\mathrm{prep}} \approx 10^{-4}$ or 10^{-5}.

It is true that the proof techniques used today force us to include ϵ_{prep} in the final security parameter of the key, but it is plausible that this is too pessimistic. Indeed, it is known that protocols with a non-Gaussian modulation are secure against all attacks corresponding to a linear channel between Alice and Bob [29]. This gives a hint that approximations of the order of 10^{-4} or 10^{-5} might be sufficient in practice.

III. IMPERFECT CALIBRATION OF THE DETECTION SETUP

We consider now finite-size effects related to the detection setup. We note that a proper calibration of Alice and Bob's devices is crucial to prove the security of the final key [30]. Our goal is to improve and expand the analysis of Ref. [26] concerning finite-size effects in CVQKD.[1] In particular, the values of the quantum efficiency and the electronic noise of Bob's homodyne detection (HD) can only be estimated up to some finite precision. These inaccuracies must be taken into account when computing a secret key rate compatible with a realistic scenario (where these sources of noise are not assumed to be controlled by Eve) while considering finite-size effects. In the same way, the modulation variance on Alice's side and the excess noise on Bob's side both need to be estimated, in shot-noise units, when computing the secret key rate. This implies that any imperfect precision on the estimation of the shot noise has an impact on the secret key rate.

The effect of a noisy HD has already been taken into account in the security proofs [17,20]. The efficiency of the detection is modeled by a beamsplitter of transmittance η and the electronic noise is modeled by a thermal noise of variance N_{el} added at the second input of the beamsplitter. That is, before Bob's HD, the state received by Bob is mixed with a thermal state of variance N_{el} on a beamsplitter of transmittance η. The variance of the electronic noise of the HD, v_{el}, is linked to N_{el} by $v_{\mathrm{el}} = (1 - \eta)(N_{\mathrm{el}} - 1)$. Interestingly, the final key rate depends only on one parameter, namely, the added noise referred to the input of the measurement device, denoted as $\chi_{\mathrm{hom}} = \frac{1-\eta}{\eta}N_{\mathrm{el}} = \frac{1+v_{\mathrm{el}}}{\eta} - 1$. Therefore, all the combinations of the parameters (η, v_{el}) that give the same χ_{hom} have the same impact on the secret key rate.

In [20], these parameters were supposed to be calibrated in a secure laboratory, which implies that no attacker can interfere with the calibration procedure. Since this calibration is not performed during a QKD run, the statistical noise due to the finite number of samples used for the estimation can be made arbitrarily small. However, both parameters are still known imperfectly because of the finite precision of the measurement apparatuses. Here we consider an imperfect knowledge of these parameters and its effect on the secret key rate.

In order to calibrate a fiber-based HD, like the one used in [20], one should in fact estimate three quantities: (1) the interferometer mode matching η_{mod} with precision $\Delta\eta_{\mathrm{mod}}$, (2) the efficiency of the photodiodes η_{phot} with precision $\Delta\eta_{\mathrm{phot}}$, and (3) the fiber-optic transmittance η_{opt} with precision $\Delta\eta_{\mathrm{opt}}$. Then, the HD efficiency reads[2] $\eta = \eta_{\mathrm{mod}}^2\eta_{\mathrm{phot}}\eta_{\mathrm{opt}}$ and the overall uncertainty is

$$\Delta\eta = \eta\left(2\frac{\Delta\eta_{\mathrm{mod}}}{\eta_{\mathrm{mod}}} + \frac{\Delta\eta_{\mathrm{phot}}}{\eta_{\mathrm{phot}}} + \frac{\Delta\eta_{\mathrm{opt}}}{\eta_{\mathrm{opt}}}\right). \qquad (15)$$

The interferometer mode matching efficiency η_{mod} is close to 99%, while a typical value for η_{phot} is 80% with the *p-i-n* photodiodes used in [20]. The fiber-optic transmittance is usually low (around 80% for fiber-based HD since losses are usually applied on one arm of the interferometer to compensate for an unbalanced beamsplitter).

As far as v_{el} is concerned, this is estimated as the variance of the HD electronic noise, i.e., the detection output variance when no optical signal enters the detection device. This noise is mainly due to the thermal noise introduced by the load resistance at the entrance of the amplifier circuit (the intrinsic noise of the photodiodes is typically negligible). A straightforward way to determine v_{el} is to measure it directly as the variance of the HD output when no light enters the homodyne detection. Alternatively, one can plot the relationship between the power of a light source entering one branch of the beamsplitter of a balanced shot-noise limited HD and the variance of the HD output, when the other entrance of the HD is disconnected. This relationship should be linear, the Y intercept being the variance of the electronic noise. Experimentally, the latter method leads to less accurate values of the electronic noise. However, even with the direct method v_{el} can only be known up to a precision Δv_{el}.

The different uncertainties mentioned above can be evaluated depending on the measurement procedure and the precision of the measurement devices. In a practical CVQKD setup, Alice and Bob estimate the quantities required to compute the secret key rate through the sampling of $m = N - n$ pairs of correlated variables $(x_i, y_i)_{i=1...m}$, where N is the total number of quantum signals sent through the quantum channel and n is the number of signals used for the key establishment.

---

[1]Note that finite-size effects are also considered in [8], where an entropic uncertainty relation is used to prove the security of an entanglement-based CVQKD protocol. Unfortunately, the bounds derived there are too pessimistic to be used in realistic experimental conditions.

[2]Note that η_{mod} is derived from a measurement of the visibility of the interference fringes on one arm of the HD when the local oscillator (LO) interferes with another classical signal of the same intensity. It is therefore the experimentally useful quantity to characterize mode mismatching in the interferometer and is used as a reference for modeling the equivalent beamsplitter transmittance.

More precisely, the parameter estimation is performed in two steps. First, after the state distribution and measurements, Alice and Bob need to roughly estimate the signal-to-noise ratio of their classical data in order to choose the proper error correcting code for the reconciliation [25]. This typically requires $m = O(\sqrt{N})$. Then, after the (reverse) reconciliation, Alice knows both her raw string and the one received by Bob. In practice, Alice and Bob would publicly compare a small hash of their final string to make sure that the reconciliation procedure succeeded. The size of these strings is N and the parameter estimation can be performed *on the whole string*. The results of this estimation will be used to compute a tight bound on Eve's information about Bob's string.

Since for CVQKD it is sufficient to estimate the covariance matrix of the state shared by Alice and Bob, the only parameters that need to be estimated are the variance on Alice's and Bob's sides, respectively, $\langle x^2 \rangle$ and $\langle y^2 \rangle$, and the covariance between Alice and Bob $\langle xy \rangle$ (assuming here that x and y are centered variables, that is, that $\langle x \rangle = \langle y \rangle = 0$). These values are linked to the key rate parameters through

$$\langle x^2 \rangle = V_A, \tag{16}$$

$$\langle y^2 \rangle = \eta T V_A + N_0 + \eta T \xi + v_{\text{el}}, \tag{17}$$

$$\langle xy \rangle = \sqrt{\eta T} V_A, \tag{18}$$

where T is the quantum channel transmittance, V_A is the modulation variance, ξ is the excess noise, and N_0 is the shot noise (all expressed in their respective units and not in shot-noise units as it is usually assumed).

Since η and v_{el} are calibrated beforehand, one has four unknown parameters (V_A, N_0, T, ξ) and only three equations. However, by forcing a quantum channel with zero transmittance, we get one more equation:

$$\langle y_0^2 \rangle = N_0 + v_{\text{el}}. \tag{19}$$

This can be done in Bob's laboratory by measuring the vacuum.

In order to compute confidence intervals for these parameters, we consider here a normal model for Alice and Bob's correlated variables $(x_i, y_i)_{i=1...N}$:

$$y = tx + z, \tag{20}$$

where $t = \sqrt{\eta T} \in \mathbb{R}$ and where z follows a centered normal distribution with unknown variance $\sigma^2 = N_0 + \eta T \xi + v_{\text{el}}$. Note that this normal model is an assumption justified in practice but not by *current* proof techniques, which show that the Gaussian assumption is valid once the covariance matrix is known [12,13]. Exploiting symmetries of the protocol in phase space might be a way to rigorously justify this assumption [31,32]. The random variable x is a normal random variable with variance V_A in the case of a Gaussian modulation. Another set of Bob's data $(y_{0i})_{i=1...N'}$ can be used to measure the noise when no signal is exchanged (one can take N' to be on the order of N):

$$y_0 = z_0, \tag{21}$$

where z_0 follows a centered normal distribution with unknown variance $\sigma_0^2 = N_0 + v_{\text{el}}$. Similarly to the analysis in [26], maximum-likelihood estimators $\hat{t}$, $\hat{\sigma}^2$, and $\hat{\sigma_0}^2$ are known for

the normal linear model:

$$\hat{t} = \frac{\sum_{i=1}^{N} x_i y_i}{\sum_{i=1}^{N} x_i^2}, \tag{22}$$

$$\hat{\sigma}^2 = \frac{1}{N} \sum_{i=1}^{N} (y_i - \hat{t} x_i)^2, \tag{23}$$

$$\hat{\sigma_0}^2 = \frac{1}{N'} \sum_{i=1}^{N'} y_{0i}^2, \tag{24}$$

$$\hat{V}_A = \frac{1}{N} \sum_{i=1}^{N} x_i^2. \tag{25}$$

The estimators $\hat{t}$, $\hat{\sigma}^2$, $\hat{\sigma_0}^2$, and $\hat{V}_A$ are independent estimators whose distributions are

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^{N} x_i^2}\right), \tag{26}$$

$$\frac{N\hat{\sigma}^2}{\sigma^2}, \frac{N'\hat{\sigma_0}^2}{\sigma_0^2}, \frac{N\hat{V}_A}{V_A} \sim \chi^2(m-1), \tag{27}$$

where t, σ^2, σ_0^2, and V_A are the true values of the parameters. In the limit of large N, N', one can compute confidence intervals for these parameters:

$$t \in [\hat{t} - \Delta T, \hat{t} + \Delta T], \tag{28}$$

$$\sigma^2 \in [\hat{\sigma}^2 - \Delta \sigma^2, \hat{\sigma}^2 + \Delta \sigma^2], \tag{29}$$

$$\sigma_0^2 \in \left[\hat{\sigma_0}^2 - \Delta \sigma_0^2, \hat{\sigma_0}^2 + \Delta \sigma_0^2\right], \tag{30}$$

$$V_A \in [\hat{V}_A - \Delta V_A, \hat{V}_A + \Delta V_A], \tag{31}$$

where $\Delta T = z_{\epsilon_{\text{PE}}/2} \sqrt{\frac{\hat{\sigma}^2}{N V_A}}$, $\Delta \sigma^2 = z_{\epsilon_{\text{PE}}/2} \frac{\hat{\sigma}^2 \sqrt{2}}{\sqrt{N}}$, $\Delta \sigma_0^2 = z_{\epsilon_{\text{PE}}/2} \frac{\hat{\sigma_0}^2 \sqrt{2}}{\sqrt{N'}}$, $\Delta V_A = z_{\epsilon_{\text{PE}}/2} \frac{\hat{V}_A \sqrt{2}}{\sqrt{N}}$, and $z_{\epsilon_{\text{PE}}/2}$ is such that $1 - \text{erf}(z_{\epsilon_{\text{PE}}/2}/\sqrt{2})/2 = \epsilon_{\text{PE}}/2$ (ϵ_{PE}, typically 10^{-10}, is the probability that the estimated parameters do not belong to the confidence region computed from the parameter estimation procedure). Here we have used the error function $\text{erf}(x)$, defined as

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt. \tag{32}$$

One can then estimate $T = \frac{\hat{t}^2}{\eta}$ and $\xi = \frac{\sigma^2 - \sigma_0^2}{\hat{t}^2}$ using the previous estimators and their confidence intervals. As regards the shot noise, it is known with a precision that depends both on the number of samples used to compute the estimator $\hat{\sigma_0}^2$ and on $\Delta_{v_{el}}$.

Once the parameters and their respective confidence intervals have been determined, one can in particular express in shot-noise units all the quantities needed to compute $S_{\epsilon_{\text{PE}}}(y : E)$, the maximal value of the Holevo information between Eve and Bob's classical data compatible with the statistics except with probability ϵ_{PE}. Thus, the secret key rate for collective attacks including all the finite-size effects and calibration
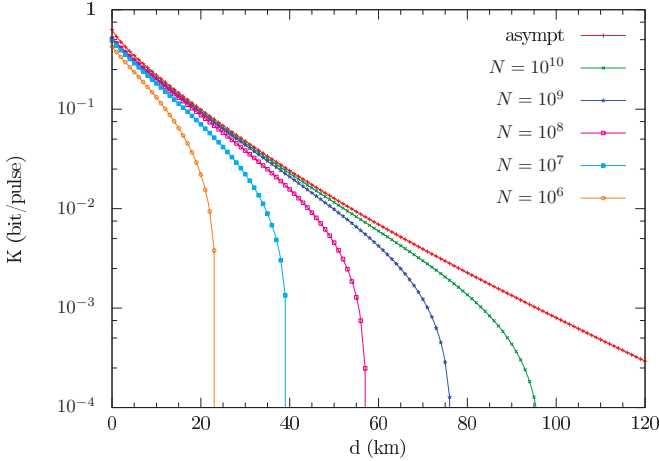
FIG. 2. (Color online) Secret key rate for collective attacks including finite-size effects and calibration imperfections with respect to the distance for different values of the number of samples. The transmittance T and distance d are linked with the expression $T = 10^{-\alpha d/10}$, where α is the loss coefficient of the optical fiber. $V_A = 2.5$, $\xi = 0.01$, $\eta = 0.6$, $v_{el} = 0.01$, $\alpha = 0.2$ dB/km, $\beta = 95\%$, $\Delta\eta = 0.1\eta$, $\Delta v_{el} = 0.1 v_{el}$, $\epsilon_{PE} = 10^{-10}$, $N =$ asympt, 10^{10}, 10^9, 10^8, 10^7, 10^6 from top to bottom.

imperfections discussed previously can be computed as

$$K_{\text{finite}} = \frac{n}{N}[\beta I(x : y) - S_{\epsilon_{PE}}(y : E) - \Delta(n)], \qquad (33)$$

where $\beta I(x : y)$ is 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) and $\Delta(n)$ is related to the security of the privacy amplification [26,33].

Figure 2 gives the secret key rate for various values of the number of samples $N = N'$. It appears that, even taking pessimistic confidence intervals for η and v_{el}, for example, with $\Delta\eta = 0.1\eta$ and $\Delta v_{el} = 0.1 v_{el}$, the impact on the secret key rate is not significant. However, a high precision on the shot noise is required for long distances since $\eta T \xi$ must be known with a high precision as already observed in [26]. It is worth noting that even using 10^6 samples leads to a positive secret key rate for the Gaussian protocol unlike discrete modulation protocols, for which at least 10^8 samples are required [26].

IV. IMPROVED KEY RATE WITH PHASE NOISE CALIBRATION

In order to obtain precise statements about the security of a given quantum key distribution (QKD) protocol, it is useful to carefully characterize the equipment of Alice and Bob. For CVQKD, this issue has already been addressed extensively for the detection stage. In particular, as was discussed in the previous section, in a calibrated device scenario, the detection model includes a finite quantum efficiency and a given level of electronic noise. Interestingly, both these imperfections act as sources of noise that can be trusted, in the sense that they are not controlled by Eve. This corresponds to the so-called

realistic model, as opposed to the paranoid model where the eavesdropper is supposed to control all sources of noise. The realistic model allows one to derive a secret key rate that is actually better than the one obtained without this modeling for the imperfections of Bob's detection.

Concerning the preparation phase of the Gaussian CVQKD protocol that we are considering, recent work has addressed the issue of imperfections in Alice's state preparation. In particular, [34–36] studied the situation where Alice in fact prepares thermal states instead of coherent states. In fact, it is even possible to achieve CVQKD in the microwave regime where the preparation of pure coherent states is impossible [37,38]. One remark about these works is that they consider a specific kind of imperfection that can be efficiently dealt with experimentally (at least in the optical regime). Indeed, if Alice really prepares thermal states instead of coherent states, one simple solution is to increase the variance of modulation and then to strongly attenuate the resulting state in order to obtain something very close to a coherent state. For this reason, the problem of preparing thermal states instead of coherent states is not really an issue in a practical scenario.

A more relevant issue concerns non-Gaussian sources of noise. In particular, there always is some phase noise on the state prepared by Alice. A typical value for the variance of this noise is $10^{-4} N_0$ per photon in the pulse [39]. One cannot suppress this noise by increasing the variance of the modulation and then attenuating the state, as mentioned above. Studying this noise is therefore of particular theoretical interest and of importance for actual experiments.

An important property of this noise is that it leaves the global state $\rho_{B_0} = \text{tr}_A \rho_{AB_0}$ sent by Alice in the quantum channel (and therefore seen by Eve) invariant. This is different from the thermal noise considered in [35,36], which increases the variance of ρ_{B_0}. In particular, this means that this noise can be modeled as an imperfect measurement for Alice in the entanglement-based equivalent protocol. In that picture, Alice prepares two-mode squeezed vacuum states, sends one mode to Bob, and measures the other one with a heterodyne detection. When modeling the noise, one can keep the preparation of two-mode squeezed vacuum states, and only Alice's detection will be noisy. This simply means that the *classical* data that she gets are noisy (with some phase noise). Therefore, the only consequence of this noise is that it degrades the mutual information shared between Alice and Bob, but it cannot increase Eve's information about Bob's measurement outcome, which is of interest in a reverse reconciliation scheme.

More specifically, in this case, the secret key rate against collective attacks is $K_{\text{asympt}} = \beta I(x : y) - \chi(y : E)$, where $\beta I(x : y)$ is defined as in the previous section and $\chi(y : E)$ is an upper bound on Eve's information on Bob's measurement outcomes. Because one can model phase noise as a local noise acting on Alice's system, it can only decrease the quantity $I(x : y)$ but cannot help the eavesdropper by increasing $\chi(y : E)$. In such a scenario, one can expect that the phase noise can be removed from the excess noise when computing Eve's information, leading to a realistic model for the preparation stage, similarly to the detection stage. This should lead to better secret key rates in practice.

A. Model for the phase noise

The phase noise can be modeled as applying a phase rotation $U(\theta) = \exp(i\theta a^\dagger a)$ on Alice's mode with a random phase θ characterized by some probability distribution $p(\theta)$. This means that when Alice tries to prepare some coherent state $|\alpha\rangle$ in the prepare-and-measure protocol she actually prepares a state with a noisy phase: $\rho_\alpha = \int U(\theta)|\alpha\rangle\langle\alpha|U(\theta)^\dagger p(\theta)\mathrm{d}\theta$. Let us assume that Alice initially prepares an ideal two-mode squeezed vacuum state with a variance V_A. This state ρ_{ideal} has the following covariance matrix (for a displacement vector $[q_A, p_A, q_B, p_B]^T$):

$$\Gamma_{\mathrm{ideal}} = \begin{bmatrix} V_A \mathbb{1}_2 & W\sigma_z \\ W\sigma_z & V_A \mathbb{1}_2 \end{bmatrix}, \tag{34}$$

where $W := \sqrt{V_A^2 - 1}$ and $\sigma_z = \mathrm{diag}(1, -1)$.

Applying a local phase shift $U(\theta)$ on Alice's mode gives a state with a covariance matrix $\Gamma(\theta)$ given by

$$\Gamma(\theta) = \begin{bmatrix} V_A & & W\cos\theta & W\sin\theta \\ & V_A & W\sin\theta & -W\cos\theta \\ W\cos\theta & W\sin\theta & V_A & \\ W\sin\theta & -W\cos\theta & & V_A \end{bmatrix}. \tag{35}$$

Finally, the state affected by the phase noise is a classical mixture of states with random phase shifts $\rho = \int (U_A(\theta) \otimes \mathbb{1}_B)\rho_{\mathrm{ideal}}(U_A(\theta)^\dagger \otimes \mathbb{1}_B)p(\theta)\mathrm{d}\theta$, and its covariance matrix is

$$\Gamma_{\mathrm{phase\,noise}} = \begin{bmatrix} V_A \mathbb{1}_2 & \sqrt{\kappa} W\sigma_z \\ \sqrt{\kappa} W\sigma_z & V_A \mathbb{1}_2 \end{bmatrix}, \tag{36}$$

where we assumed that the distribution θ is symmetric, and more precisely that $\int p(\theta)\sin\theta \mathrm{d}\theta = 0$, and introduced $\kappa := (\int p(\theta)\cos\theta \mathrm{d}\theta)^2 = (E[\cos\theta])^2$, where $E[X]$ is the expectation of the random variable X.

The interesting point is that from both Bob's and Eve's points of view it does not change anything whether a random phase shift is applied. In particular, the value of $\chi(y:E)$ quantifying the information that Eve can acquire about the raw key in a *reverse reconciliation* scenario does not depend on the value of the phase noise. Note that this statement would not be true in a direct reconciliation scenario, where the raw key would correspond to Alice's noisy data.

Let us suppose that the quantum channel between Alice and Bob is characterized by its transmittance T and excess noise ξ. The covariance matrix Γ_{AB} of the bipartite state shared by Alice and Bob after the quantum channel is then given by

$$\Gamma_{AB} = \begin{bmatrix} V_A \mathbb{1}_2 & \sqrt{\kappa T} W\sigma_z \\ \sqrt{\kappa T} W\sigma_z & (T(V_A - 1) + 1 + T\xi)\mathbb{1}_2 \end{bmatrix}. \tag{37}$$

If they were not taking phase noise into account (that is, if κ was equal to 1), Alice and Bob would estimate a transmittance T' and an excess noise ξ' such that

$$T' = T\kappa \tag{38}$$
$$T'(V_A - 1) + 1 + T'\xi' = T(V_A - 1) + 1 + T\xi,$$

that is,

$$T = T'/\kappa \tag{39}$$
$$\xi = \xi' - (1 - \kappa)(V_A - 1).$$

If the phase noise parameter κ is known, one can estimate the covariance matrix as usual, hence obtaining values (T', ξ'), and use the formula above to deduce the parameters (T, ξ) that can be used instead to compute Eve's information $\chi(y:E)$.

For this technique to work, it is necessary to be able to measure $\kappa = (E[\cos\theta])^2$ experimentally. This is discussed in the next section.

B. Experimental evaluation of the phase noise

The evaluation of the phase noise can be performed with a phase sensitive apparatus which allows us to compute an estimate of the noise between a signal whose quadratures are modulated following a chosen sequence and the outputs of some chosen quadrature measurements. A homodyne or heterodyne detection can be used for this purpose.

Similarly to what is done on Bob's side when the homodyne detection efficiency and the variance of the electronic noise are calibrated, it is necessary to assume that the calibration of the phase noise is performed in a safe place, i.e., that Eve cannot interfere with Alice's apparatus during the phase noise measurement. The measurement can also be performed during a run of the protocol but one still needs to assume that Eve cannot interfere with Alice's device. This is crucial since overestimating the phase noise would lead to an overestimation of the secret key rate.

Here, we are interested in the phase noise in the prepare-and-measure version of the protocol. The procedure to estimate it goes as follows: Alice modulates as usual with a bivariate Gaussian distribution and she measures either one of the quadratures with a homodyne detection. Computing the variance of her measurement outcomes allows us here to infer the quantity κ introduced above. Let us denote by ϕ the random variable corresponding to the angle between the modulated state and the measured quadrature and by B the random variable corresponding to the noise. This means for
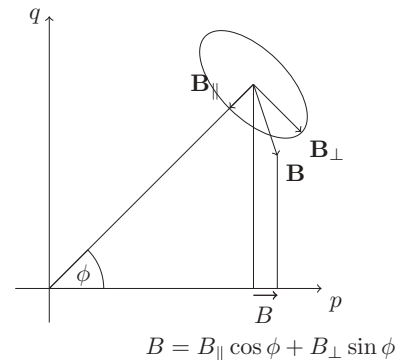

$$B = B_\parallel \cos\phi + B_\perp \sin\phi$$

FIG. 3. Experimental evaluation of the phase noise. The noise **B** before Bob's measurement can be decomposed into the sum of a component orthogonal to the signal $\mathbf{B}_\perp$ and a component parallel to the signal $\mathbf{B}_\parallel$. The result of Bob's q-quadrature measurement is $A\cos\phi + B$ where Alice prepared the state centered in $Ae^{i\phi}$ with $A \geqslant 0$.
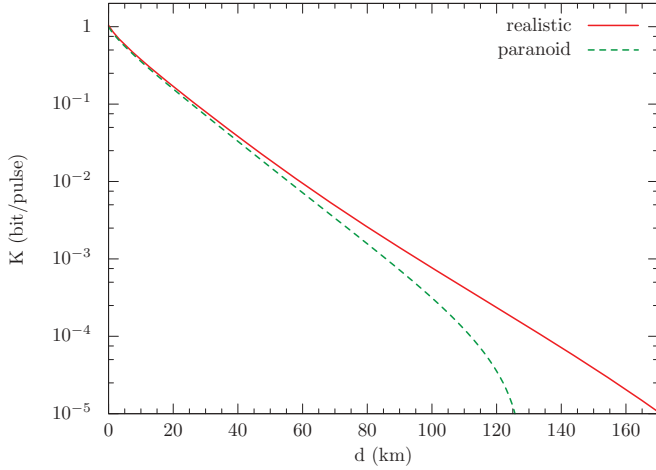
FIG. 4. (Color online) Secret key rate for collective attacks in the asymptotic regime. The plot at the top is obtained in the so-called realistic model where the phase noise is calibrated and is considered as a local noise useless to the eavesdropper. The plot at the bottom corresponds to the so-called paranoid model where all the sources of noise are attributed to the eavesdropper. The transmittance T and distance d are linked with the expression $T = 10^{-\alpha d/10}$, where α is the loss coefficient of the optical fiber. $V_A = 2.5$, $\xi = 0.025$, $\alpha = 0.2$ dB/km, $\beta = 95\%$, $E_1 = 3 \times 10^{-3}$.

example that Alice prepared the state centered in $Ae^{i\phi}$ (with $A \geqslant 0$) and that the outcome of her q-quadrature measurement was $A \cos \phi + B$. This noise B can be decomposed into the sum of a component orthogonal to the signal and a component parallel to the signal:

$$B = B_{\parallel} \cos \phi + B_{\perp} \sin \phi, \qquad (40)$$

where we assume that $B_{\parallel}$ and $B_{\perp}$ are independent of ϕ. Figure 3 gives an illustration of this decomposition. We can easily build estimators of $B_{\parallel}$ and $B_{\perp}$ (in the following, $E[X]$ and $V[X]$ refer, respectively, to the expectation and variance of the random variable X):

$$V[B \cos \phi] = V[B_{\parallel} \cos^2 \phi] + V[B_{\perp} \cos \phi \sin \phi] \qquad (41)$$

$$= V[B_{\parallel}]E[\cos^4 \phi] + V[B_{\perp}]E[\cos^2 \phi \sin^2 \phi] \qquad (42)$$

$$= 3/8 V[B_{\parallel}] + 1/8 V[B_{\perp}], \qquad (43)$$

$$V[B \sin \phi] = 1/8 V[B_{\perp}] + 3/8 V[B_{\parallel}]. \qquad (44)$$

Since both $V[B \cos \phi]$ and $V[B \sin \phi]$ can be measured experimentally, one therefore has access to the values of $V[B_{\perp}]$ and $V[B_{\parallel}]$. Here, we assume that the only sources of noise are the shot noise and the phase noise. We assume that $B_{\perp}$ can be fully described by the shot noise and the phase noise:

$$V[B_{\perp}] = N_0 + V[A \sin \theta] = N_0 + E[\sin^2 \theta]E[A^2], \qquad (45)$$

$$E[\sin^2 \theta] = \frac{V[B_{\perp}] - N_0}{E[A^2]} = E_1, \qquad (46)$$

where A is the amplitude of the modulated signal and where we used $E[\sin \theta] = 0$. The assumption of a small phase noise, i.e., small values of θ, gives

$$E[\cos \theta] = E[1 - \theta^2/2] \qquad (47)$$

$$= 1 - \tfrac{1}{2}E_1. \qquad (48)$$

Figure 4 compares the so-called realistic and paranoid models. We consider a pessimistic scenario where the excess noise on Alice's side is about 2.5% of the shot noise (the detector quantum efficiency and electronic noise are not taken into account here, for clarity). For a modulation variance $V_A = 2.5$, we measured experimentally $E_1 = 3 \times 10^{-3}$ with a system similar to the one described in [20]. This leads to a realistic value of the excess noise $\xi_{\text{real}} = 1.75\%$. The result on the secret key rate for collective attacks is an increase in achievable distance of about 40 km.

V. CONCLUSION

In this work, we have analyzed several types of imperfections that appear in practical implementations of Gaussian continuous-variable QKD protocols. In particular, we studied a realistic approximate Gaussian modulation in the state preparation at Alice's site, the calibration of detection characteristics estimated with a finite precision at Bob's site, and the presence of intrinsic phase noise in the prepared states. In all cases, we provided a precise model of the imperfection and used this model to examine its effect on the security and performance of the protocol. These effects are more or less significant in practice: it is clear, for instance, that taking into account the phase noise in the security proof of a realistic scenario provides an important advantage in terms of secret key rate, while carefully approximating the ideal Gaussian modulation with respect to the shot-noise values can minimize the impact of this imperfection. Finally, as expected, finite-size effects at all stages of the protocol should always be considered when calculating practical secret key rates.

This analysis demonstrates the importance of refining security proofs of QKD protocols to consider practical imperfections. In particular for CVQKD protocols, where potential side channels have not been yet widely studied, it provides specific ways to bypass attacks based on improperly modeled devices and procedures.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] V. Scarani and C. Kurtsiefer, arXiv:0906.4547v2 [quant-ph] (2012).

[3] F. Xu, B. Qi, and H. Lo, New J. Phys. **12**, 113026 (2010).

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] B. Qi, W. Zhu, L. Qian, and H. Lo, New J. Phys. **12**, 103042 (2010).

[7] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[8] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, arXiv:1112.2179v2 [quant-ph] (2011).

[9] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, arXiv:1208.4920v1 [quant-ph] (2012).

[10] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[11] M. Berta, F. Furrer, and V. Scholz, arXiv:1107.5460v1 [quant-ph] (2011).

[12] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[13] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[14] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[15] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[16] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[17] J. Lodewyck *et al.*, Phys. Rev. A **76**, 042305 (2007).

[18] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).

[19] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303 (2007).

[20] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[21] T. Symul, V. Sharma, T. Ralph, and P. Lam, in *Optical Fiber Communication Conference* (Optical Society of America, San Diego, CA, 2010).

[22] L. Madsen, V. Usenko, M. Lassen, R. Filip, and U. Andersen, arXiv:1110.5522v1 [quant-ph] (2011).

[23] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[24] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[25] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[26] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[27] A. Winter, in *IEEE Transactions on Information Theory* (IEEE Press, Piscataway, NJ, 1999), Vol. 45, pp. 2481–2485.

[28] T. Ogawa and H. Nagaoka, in *Proceedings of IEEE International Symposium on Information Theory* (IEEE Press, Lausanne, Switzerland, 2002), p. 73.

[29] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[30] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[31] A. Leverrier, E. Karpov, P. Grangier, and N. Cerf, New J. Phys. **11**, 115009 (2009).

[32] A. Leverrier and P. Grangier, Phys. Rev. A **81**, 062314 (2010).

[33] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[34] R. Filip, Phys. Rev. A **77**, 022310 (2008).

[35] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).

[36] Y. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).

[37] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[38] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).

[39] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303 (2005).