Secure coherent-state quantum key distribution protocols with efficient reconciliation

G. Van Assche,[1,*] S. Iblisdir,[1,2] and N. J. Cerf[1]
[1]*QuIC, Ecole Polytechnique, Université Libre de Bruxelles, CP 165/59, 1050 Brussels, Belgium*
[2]*GAP-Optique, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211 Genève, Switzerland*
(Received 8 October 2004; published 4 May 2005)

We study the equivalence of a realistic quantum key distribution protocol using coherent states and homodyne detection with a formal entanglement purification protocol. Maximally entangled qubit pairs that one can extract in the formal protocol correspond to secret key bits in the realistic protocol. More specifically, we define a qubit encoding scheme that allows the formal protocol to produce more than one entangled qubit pair per entangled oscillator pair or, equivalently for the realistic protocol, more than one secret key bit per coherent state. The entanglement parameters are estimated using quantum tomography. We analyze the properties of the encoding scheme and investigate the resulting secret key rate in the important case of the attenuation channel.

DOI: 10.1103/PhysRevA.71.052304 PACS number(s): 03.67.Dd, 89.70.+c

I. INTRODUCTION

The quantum key distribution (QKD), also called quantum cryptography, allows two parties, Alice and Bob, to share a secret key that can be used for encrypting messages using a classical cipher—e.g., the one-time pad. The main interest of such a key distribution scheme is that any eavesdropping is, in principle, detectable because the laws of quantum mechanics imply that measuring a quantum state generally disturbs it.

The resources required by QKD comprise a source of nonorthogonal quantum states on Alice's side, a quantum channel conveying these states to Bob, a measuring apparatus on Bob's side, and a (public) authenticated classical channel between Alice and Bob. In addition to being used to generate a secret key, the quantum channel is subject to probing by the legitimate parties, so as to determine how many secret bits can be generated.

Most interest in the QKD has been devoted to protocols involving (an approximation to) a single-photon source on Alice's side and a single-photon detector on Bob's side (see [1] and the references therein). However, protocols involving quantum continuous variables have been considered with an increasing interest (see e.g., [2–12].) Of special importance are Gaussian-modulated coherent-state protocols [13,14]. The quantum source at Alice's side randomly generates coherent states of a light mode with Gaussian-distributed quadratures, and Bob's measurements are homodyne measurements. These protocols seem to allow for facilitated implementations and higher secret-key generation rates than the protocols involving single-photon sources [14].

Consequently, there is an increasing interest in studying the security of coherent-state protocols under general classes of attacks. Individual Gaussian attacks are considered in [13,14] and are found to be optimal in the more general class of finite-width non-Gaussian incoherent attacks [15]. Individually probed collective attacks are also considered in [16,17]. The recent techniques of [18,19] do not make any assumptions on the eavesdropper's technology and are also considered in [16,17] for coherent-state protocols, although giving lower secret key rates.

In this paper, we study the security of a prepare-and-measure QKD protocol [13,14] by establishing its equivalence to an entanglement purification (EP) protocol, which produces maximally entangled qubit pairs. A maximally entangled qubit pair is by definition completely factored from its environment, and thus the values obtained by measuring each side are fully correlated and secret. The equivalent prepare-and-measure QKD protocol also enjoys this property. This particular technique thus allows one to relieve from any assumptions on the eavesdropper's strategy and was used in [20] to assess the security of the Bennett-Brassard 1984 (BB84) protocol and extended in [5] for a squeezed-state protocol. More recently, this technique was extended to the case of coherent-state protocols [21].

To show the equivalence between a QKD protocol and of an EP protocol, one has to explicitly take into account the secret key distillation—that is, the techniques used to make Alice's and Bob's keys equal (reconciliation) and fully secret (privacy amplification). In [20], the EP protocol uses Calderbank-Shor-Steane (CSS) quantum codes [22,23], which are equivalent in the QKD to reconciliation with syndromes of binary linear codes and privacy amplification by multiplication with a parity-check matrix. In contrast to the BB84 protocol, the modulation of coherent states in the protocol we consider here is *continuous*, therefore producing continuous key elements from which to extract a secret key. Reconciliation of a Gaussian-distributed key was studied in [24], and a generic protocol called sliced error correction was designed so as to distill a *binary* key.

In contrast to [21], the EP protocol investigated here is constructed in such a way that it is equivalent to a QKD protocol with sliced error correction for reconciliation. The advantage is the higher secret key rate and the better resistance to attenuation that one can achieve. In particular, more than one maximally entangled pair (or secret key bit) can be produced per coherent state. Furthermore, thanks to its generality, the asymptotic efficiency of the EP protocol inherits to some extent the asymptotic efficiency of the classical reconciliation protocol.

*Electronic address: gvanassc@ulb.ac.be

The paper is organized as follows. First, in Sec. II, we sketch the formal EP protocol and its equivalent QKD protocol that are used throughout the paper. Then, in Sec. III, we show how the channel can be probed so as to determine the number of secret key bits that Alice and Bob can generate. The encoding of qubits—that is, the generalization of sliced error correction to EP—is described in Sec. IV. Then, Sec. V deals with the important particular case of an attenuation channel. Finally, the asymptotic properties of the qubit encoding scheme are detailed in Sec. VI.

II. FROM ENTANGLEMENT PURIFICATION TO SECRET KEY DISTILLATION

After we review the case of EP using CSS codes and its equivalence to the BB84 protocol, we give a high-level description of a QKD protocol based on EP. We consider this protocol as formal; that is, we do not expect a physical implementation of it. Instead, we propose a prepare-and-measure QKD protocol, derived from the formal one, which also encompasses error correction and privacy amplification.

A. Binary CSS codes

In the case of the BB84 protocol, the CSS codes can readily be used to establish the equivalence between an EP protocol and a QKD protocol [20]. Since we will use CSS codes as an ingredient for the EP and QKD protocols below, let us briefly review their properties.

Starting from the Einstein-Podolski-Rosen (EPR) state

$$|\phi^+\rangle = 2^{-1/2}(|00\rangle + |11\rangle),$$

Alice keeps half of the state and sends the other half to Bob. His part may undergo a bit error ($|\phi^+\rangle \to |\psi^+\rangle$), phase error ($|\phi^+\rangle \to |\phi^-\rangle$), or both errors ($|\phi^+\rangle \to |\psi^-\rangle$), with $|\phi^-\rangle = 2^{-1/2}(|00\rangle - |11\rangle)$ and $|\psi^\pm\rangle = 2^{-1/2}(|01\rangle \pm |10\rangle)$. Given that not too many such errors occur, Alice and Bob can obtain, from many instances of such a transmitted state, a smaller number of EPR pairs using only local operations and classical communications (LOCC's). One way to do this is to use CSS codes.

Let C_1 and C_2 be two binary error correcting codes of n bits (i.e., C_1 and C_2 are vector spaces of $\mathbf{F}_2^n$) with parity check matrices H_1 and H_2, respectively. They are chosen such that $\{0\} \subset C_2 \subset C_1 \subset \mathbf{F}_2^n$. A CSS code is a k-dimensional subspace of $\mathcal{H}^n$, the Hilbert space of n qubits, with $k = \dim C_1 - \dim C_2$ [22,23]. The code C_1 allows one to correct bit errors, while $C_2^\perp$ (the dual code of C_2) allows one to correct phase errors—one important property of the CSS codes is to be able to correct bit errors and phase errors independently.

For entanglement purification, Alice and Bob must compare their syndromes, both for bit errors and phase errors. The relative syndrome determines the correction that Bob must apply to align his qubits to Alice's. Translating this into the BB84 protocol, one can show [20] that the relative syndrome for bit errors in the EP protocol is equal to the relative syndrome for bit errors that Alice and Bob would have reconciled in the BB84 protocol. So, reconciliation can be done using the C_1 code. Phase errors of the EP protocol do not have such a direct equivalent in the BB84 protocol: The prepare-and-measure protocol works as if Alice measured her part of the state in the $\{|0\rangle, |1\rangle\}$ basis, thereby discarding information on the phase. However, one does not really need to correct the phase errors in the BB84 protocol. Instead, if $C_2^\perp$ would be able to correct them in the EP protocol, the syndrome of C_2 in C_1 of Alice and Bob's bit string turns out to be a valid secret key in the prepare-and-measure protocol. Stated otherwise, H_1 determines the syndrome Alice has to send to Bob to perform reconciliation, while H_2 determines the way the final key is computed for privacy amplification.

Overall, the number of secret key bits is thus $k = \dim C_1 - \dim C_2$, provided that C_1 ($C_2^\perp$) is small enough to correct all the bit (phase) errors. When considering asymptotically large block sizes, the CSS codes can produce

$$k = rn \to n[1 - h(e^b) - h(e^p)] = Rn,$$

EPR pairs or secret key bits, with e^b (e^p) the bit (phase) error rate and $h(p) = -p \log_2 p - (1-p)\log_2(1-p)$ [20]. Here, $r = k/n$ indicates the rate obtained for a particular code and $R = 1 - h(e^b) - h(e^p)$ is the asymptotically achievable rate.

We conclude this section by noting that the bit error rate e^b determines the number of bits revealed by reconciliation [asymptotically $h(e^b)$], whereas the phase error rate e^p determines the number of bits discarded by privacy amplification due to eavesdropping [asymptotically $h(e^p)$].

B. Quantum key distribution based on entanglement purification

In the BB84 protocol, the modulation of qubits can be transposed as if Alice prepares a $|\phi^+\rangle$ state and measures her part. In the case of the QKD protocol with Gaussian-modulated coherent states, the formal state that Alice prepares is of course different, as it must reduce to the proper modulation when Alice measures her part. We define the formal state as

$$|\Psi\rangle = \int \mathrm{d}x\mathrm{d}p g(x,p)|x\rangle_{\mathsf{a}_1} \otimes |p\rangle_{\mathsf{a}_2} \otimes |x+ip\rangle_{\mathsf{b}}, \qquad (1)$$

where $g(x,p)$ denotes a bivariate Gaussian distribution $g(x,p) = \sqrt{G_1(x)G_2(p)}$. The kets $|x\rangle$, $|p\rangle$, $|x+ip\rangle$ are shorthand notation for, respectively, a **x**-quadrature eigenstate with eigenvalue x, a **p**-quadrature eigenstate with eigenvalue p, and a coherent state whose **x** mean value equals x and whose **p** mean value equals p. The subscripts a_1, a_2 (b) denote that the system is lying on Alice's side (Bob's side).

The state (1) does not have a direct physical meaning. In particular, the systems a_1 and a_2 must be understood as classical pointers—e.g., resulting from the (formal) homodyne measurement of an EPR state as studied in [25].

In the entanglement purification picture, the b part of the system is sent to Bob (and possibly attacked by Eve) and the a part stays at Alice's station. If Alice measures **x** in a_1 and **p** in a_2, the state is projected as if Alice sent Bob a coherent state centered on $x+ip$.

Let us now describe the EP protocol, which reduces to the prepare-and-measure QKD protocol described further.

(i) Alice creates $l+n$ copies of the state $|\Psi\rangle$, of which she sends the b part to Bob.

(ii) Bob acknowledges reception of the states.

(iii) Out of the $l+n$ states, n will serve for estimation purposes. These states are chosen randomly and uniformly by Alice, who informs Bob about their positions.

(iv) For the remaining l states, Alice and Bob perform entanglement purification, so as to produce rl $(0\leqslant r\leqslant 1)$ states very close to $|\phi^+\rangle$. Measured in the computational bases, the produced states yield rl secret bits on both Alice's and Bob's sides.

The details of the EP procedure, which uses CSS codes as an ingredient, are given in Sec. IV, while the estimation is detailed in Sec. III.

C. Prepare-and-measure quantum key distribution

By virtually measuring the a part of the state $|\Psi\rangle$, the protocol above reduces to the following one.

(i) Alice modulates $l+n$ coherent states $|x+ip\rangle$ that she sends to Bob. The choice of the values of x and p follow the distribution $|g(x,p)|^2=G_1(x)G_2(p)$.

(ii) Bob acknowledges reception of the states.

(iii) Out of the $l+n$ states, n will serve for estimation purposes. These states are chosen randomly and uniformly by Alice, who informs Bob about their positions.

(iv) For the remaining l states, Bob measures $\mathbf{x}$. Alice and Bob perform secret key distillation (reconciliation and privacy amplification), so as to produce rl secret bits.

The reconciliation and privacy amplification procedures are based on classical error correcting codes, which derive from the CSS codes used in the formal EP protocol.

III. ERROR RATES ESTIMATION USING TOMOGRAPHY

In QKD protocols derived from EP, an important step is to show how one can infer the bit and phase error rates of the samples that compose the key. A fraction of the samples sent by Alice to Bob are sacrificed so as to serve as test samples. By randomly choosing them within the stream of data, they are statistically representative of the whole stream.

In [5,20], one can simply make measurements and directly count the number of bit and phase errors from the results. This is possible since Bob's apparatus can measure both bit and phase values. In [21], however, it is not possible to measure directly phase errors. Yet some data postprocessing can be applied on measurements so as to infer the number of phase errors in the stream of data. In this section, we wish to show that we can extend this to more general (and more efficient) encodings of qubits (in the EP picture) or bits (in the derived QKD protocol).

The encoding of bits will be described in a further section. For the moment, the qubit pair system, which Alice and Bob will process using CSS codes, is not explicitly described. However, it is sufficient to describe the CSS codes in terms of the Pauli bit-flip and phase-flip operators of Alice's qubit system in a_1—namely, $\mathbf{Z}_\mathsf{s}$ (phase flip) and $\mathbf{X}_\mathsf{s}$ (bit flip)—and of the Pauli operators in Bob's qubit system in b—namely, $\mathbf{Z}_\mathsf{e}$ and $\mathbf{X}_\mathsf{e}$. (The subscripts s and e stand for slice and estimator, respectively, to follow the convention of the following sections.) The bit errors are assumed to be easy to determine; that is, $\mathbf{Z}_\mathsf{s}$ has a diagonal expansion in $|x\rangle_{\mathsf{a}_1}\langle x|$, and $\mathbf{Z}_\mathsf{e}$ can directly be determined by a single homodyne measurement on b. This ensures, in the derived prepare-and-measure QKD protocol, that Alice knows the bit value she sent and Bob can determine the received bit value. A measurement of the observable $\mathbf{X}_\mathsf{s}\mathbf{I}_{\mathsf{a}_2}\mathbf{X}_\mathsf{e}$ associated with the phase error rate, however, cannot be implemented by a single homodyne measurement on b. Therefore, we have to invoke quantum tomography with a quorum of operators [26] to get an estimate of the phase error rate.

A. Estimating phase errors in the average state

In the EP picture, let $\rho^{(n)}$ be the state of the n samples used for estimation of the phase error rate (i.e., n instances of the $\mathsf{a}_1\mathsf{a}_2\mathsf{b}$ system). To count the number of phase errors in a set of n samples, one needs to measure $\mathbf{O}=\mathbf{X}_\mathsf{s}\mathbf{I}_{\mathsf{a}_2}\mathbf{X}_\mathsf{e}$ on the n samples and sum the results (with $\mathbf{I}_{\mathsf{a}_2}$ the identity in the system a_2). This is equivalent to measuring $\mathbf{O}^{(n)}=\Sigma_i \mathbf{I}_{\mathsf{a}_1\mathsf{a}_2\mathsf{b}}^{\otimes i-1}\otimes\mathbf{X}_\mathsf{s}\mathbf{I}_{\mathsf{a}_2}\mathbf{X}_\mathsf{e}\otimes\mathbf{I}_{\mathsf{a}_1\mathsf{a}_2\mathsf{b}}^{\otimes n-i}$. If the true phase error probability in the $n+l$ samples is e^p, the error variance is $\sigma_1^2=2e^p(1-e^p)/n$, and thus the probability of making an estimation error of more than Δ is [5,20] asymptotically $\exp[-\Delta^2 n/4e^p(1-e^p)]$. It is easy to see that

$$\mathrm{Tr}(\mathbf{O}^{(n)}\rho^{(n)}) = n\mathrm{Tr}(\mathbf{O}\rho),$$

where $\rho=n^{-1}\Sigma_i \mathrm{Tr}_{\mathrm{All}\setminus\{i\}}(\rho^{(n)})$ is the density matrix of the average state measured. So we can estimate the number of phase errors using the average state, even if the eavesdropper interacts jointly with all the states $(\rho^{\otimes n}\neq\rho^{(n)})$, in which case we say that the eavesdropping is joint.

If the measurement of $\mathbf{O}=\mathbf{X}_\mathsf{s}\mathbf{I}_{\mathsf{a}_2}\mathbf{X}_\mathsf{e}$ cannot be made directly, one instead looks for a quorum of operators $\mathbf{Q}_\lambda$ such that $\mathbf{O}=\int d\lambda o(\lambda)\mathbf{Q}_\lambda$; estimating $\langle\mathbf{O}\rangle$ comes down to measuring several times $\mathbf{Q}_\lambda$ for values of λ chosen randomly and independently of each other, and averaging the results weighted by $o(\lambda)$: $\mathbf{O}\approx\Sigma_i o(\lambda_i)\mathbf{Q}_{\lambda_i}$ [26]. If the values of λ are chosen independently of the sample index on which $\mathbf{Q}_\lambda$ is applied, we get unbiased results, as $\mathrm{Tr}(\mathbf{O}\rho)=E_\lambda[\mathrm{Tr}(\mathbf{Q}_\lambda\rho)]$, with E the expectation. Of course, the estimation of $\mathrm{Tr}(\mathbf{O}\rho)$ with a quorum cannot be perfect and results in an estimation variance σ_2^2. The variance of the estimated $\langle\mathbf{O}\rangle$ must increase by this amount, and the resulting total variance is $\sigma^2=\sigma_1^2+\sigma_2^2$.

B. Estimating phase errors using coherent states and homodyne detection

We now explain how the phase error rate can be estimated, in principle, using coherent states modulated in both quadratures and homodyne detection in all quadratures.

It is clear that the knowledge of matrix elements of the average state ρ gives the knowledge of $\langle\mathbf{O}\rangle$. Let $\rho_0=|\Psi\rangle\langle\Psi|$ be the state that Alice and Bob would share if the transmission was perfect. Since the a part of the system stays at Alice's station, we only need to learn about how the b part

of the system is affected. In the prepare-and-measure picture, let T be the completely positive (CP) map that maps the states sent by Alice onto the states received by Bob, $(\mathrm{Id}\otimes T)(\rho_0)=\rho$. In particular, let the coherent state $|x+ip\rangle\langle x+ip|$ be mapped onto $\rho_T(x+ip)$ and the (pseudo)position state $|x\rangle\langle x'|$ be mapped onto $\rho_T(x,x')$. The functions $\rho_T(x+ip)$ and $\rho_T(x,x')$ are related by the following identity:

$$\rho_T(x+ip) \propto \int \mathrm{d}x'\mathrm{d}x'' e^{-(x'-x)^2/4N_0-(x''-x)^2/4N_0} \times e^{i(x'-x'')p/2N_0}\rho_T(x',x''),$$

with N_0 the variance of the vacuum fluctuations. By setting $D=x'-x''$ and $S=x'+x''-2x$, we get

$$\rho_T(x+ip) \propto \int \mathrm{d}D\mathrm{d}S e^{-S^2/8N_0-D^2/8N_0+iDp/2N_0} \times \rho_T(x+S+D,x+S-D), \quad (2)$$

which shows that $\rho_T(x,x')$ is integrated with an invertible kernel (Gaussian convolution in S, multiplication by $e^{-D^2/8N_0}$ and Fourier transform in D). So in principle, any different CP map $T'\neq T$ implies a different effect on coherent states, $\rho_T(x+ip)\neq\rho_{T'}(x+ip)$. The modulation of coherent states in both quadratures is thus crucial for this implication being possible.

By inspecting Eq. (2), it seems that due to the factors $e^{-S^2/8N_0}$ and $e^{-D^2/8N_0}$, two different CP maps T and T' may make $\rho_T(x+ip)$ and $\rho_{T'}(x+ip)$ only vanishingly different. It thus seems unlikely that Eq. (2) should allow us to extract the coefficients $\rho_T(x+S+D,x+S-D)$. However, assuming that T depends only on a finite number of parameters, a variation of these parameters will induce a measurable variation of $\rho_T(x+ip)$. We will now discuss why it is reasonable to make such an assumption.

Due to the finite variance of the modulation of coherent states, the probability of emission of a large number of photons vanishes—this intuitively indicates that we only need to consider the description of T for a bounded number of emitted photons. More precisely, one can consider the emission of w joint copies of the state $\rho_{0\mathrm{b}}=\mathrm{Tr}_{\mathrm{a}}(\rho_0)$. For w sufficiently large $\rho_{0\mathrm{b}}^{\otimes w}$ can be represented in the typical subspace $\Gamma_\delta(\rho_{0\mathrm{b}})$ of dimension not greater than $2^{w(H(\rho_{0\mathrm{b}})+\delta)}$, for any $\delta>0$ [27], where $H(\rho)$ is the von Neumann entropy of a state ρ. The probability mass of $\rho_{0\mathrm{b}}^{\otimes w}$ outside the typical subspace can be made arbitrarily small and does not depend on the eavesdropping strategy. This means that the support for the input of T has finite dimension, up to an arbitrarily small deviation.

The number of photons received by Bob can also be upper bounded. Alice and Bob can first assume that no more than $n_{\max}$ photons are received. This fact may depend on a malicious eavesdropper, so Bob has to do hypothesis testing. The test comes down to estimating $\langle\Pi\rangle$ with $\Pi=\Sigma_{n>n_{\max}}|n\rangle\langle n|$. If the threshold is well chosen so that $n>n_{\max}$ never occurs, we can apply the central limit theorem and upper bound the probability that $\langle\Pi\rangle>\epsilon$ for any chosen $\epsilon>0$. The positivity of the density matrices implies that the off-diagonal coefficients are also bounded. We can thus now express $\rho_T(x+ip)$ as $\rho_T(x+ip)=\Sigma_{n,n'\leq n_{\max}}\rho_T(x+ip,n,n')|n\rangle\langle n'|$. Note that the test can be implemented either by explicitly measuring the intensity of the beam (therefore requiring an additional photodetector) or by exploiting the correlation between the high intensity of the beam and the high absolute values obtained when doing homodyne measurements in all directions.

Finally, the estimation of the coefficient of $|n\rangle\langle n'|$ can be done with arbitrarily small statistical error using homodyne detection in all directions [26,28]. This is achieved by considering the quorum of operators $(\mathbf{x}_\theta)_{0\leq\theta<2\pi}$, where $\mathbf{x}_\theta=\cos\theta\mathbf{x}+\sin\theta\mathbf{p}$ denotes the amplitude of the quadrature in direction θ. Considering a finite combination of arbitrarily small statistical errors on parameters also gives arbitrarily small overall statistical error on the phase error rate.

IV. ENCODING OF MULTIPLE QUBITS IN AN OSCILLATOR

Reconciliation and privacy amplification are integral parts of the prepare-and-measure protocols derived from entanglement purification protocols. In our case, we wish to derive a prepare-and-measure protocol with sliced error correction (SEC) [24] as reconciliation, which allows us to obtain a higher secret key rate and a better resistance to losses than in [21]. We therefore need to describe an entanglement purification procedure that reduces to the SEC when the corresponding prepare-and-measure protocol is derived. An overview of the SEC is proposed next.

A. Sliced error correction with invertible mappings

We here recall the main principles of the SEC in a form that is slightly different from the presentation in [24]. To suit our needs, we here describe the SEC in terms of invertible functions giving the slices and the estimators—the invertibility property will be required when we generalize the SEC to entanglement purification. Also, from the generality of [24], two parameters are fixed here: The binary error correction is operated by sending syndromes of classical linear error-correcting codes (ECC's), and we momentarily restrict ourselves to the case of one-dimensional real values X and X'.

Suppose Alice and Bob have l pairs of correlated random variables $(X_1,X_1'),\ldots,(X_l,X_l')$, with $X_i,X_i'\in\mathbf{R}$, $i=1\ldots l$, from which they intend to extract common bits.

First, Alice wishes to convert each of her variables X into m bits and thereby defines m binary functions: $S_1(X),\ldots,S_m(X)$. To make the mapping invertible, she also defines a function $\overline{S}(X)$ such that mapping from X to the vector $[\overline{S}(X),S_{1,\ldots,m}(X)]$ is bijective. As a convention, the range of $\overline{S}(X)$ is $[0;1]$. The mapping from $\mathbf{R}$ to $[0;1]\times\{0,1\}^m$,

$$x\rightarrow[\overline{S}(x),S_{1,\ldots,m}(x)],$$

is collectively denoted as $\mathcal{S}$.

Concretely, the functions $S_i(X)$ implicitly cut the real line into intervals (see [24] for more details), whereas $\overline{S}(X)$ indicates where to find X within a given interval.

Then, we can assemble the bits produced by the l random variables $X_1,\ldots,X_l$ into m l-bit vectors. To each bit vector ("slice") $S_i(X_{1,\ldots,l})=(S_i(X_1),\ldots,S_i(X_l))$ is associated an ECC that Alice and Bob agreed upon. To proceed with the correction, Alice sends the syndrome $\xi_i^b=H_i^bS_i(X_{1,\ldots,l})$ to Bob over the public authenticated channel, where H_i^b is the $l_i^b\times l$ parity check matrix of the ECC associated with slice i. Alice also sends $\overline{S}(X_{1,\ldots,l})$.

Bob would like to recover $S_{1,\ldots,m}(X_{1,\ldots,l})$ from his knowledge of $X'_{1,\ldots,l}$, $\xi^b_{1,\ldots,m}$, and $\overline{S}(X_{1,\ldots,l})$. To do so, he also converts each of his variables $X'_{1,\ldots,l}$ into m bits, but he does so in a consecutive manner. He tries to produce bits that are best correlated to Alice's and takes advantage of the corrected bits of slices $j<i$ before trying to estimate the bits of slice i. In particular, to produce bits that are best correlated to Alice's first slice $S_1(X_{1,\ldots,l})$, he uses a function $E_1(X',\overline{S}(X))$, which gives his best estimate on Alice's corresponding bit $S_1(X)$ given the known correlations between X and X'. By applying the function E_1 on all the variables $X'_{1,\ldots,l}$ and $\overline{S}(X_{1,\ldots,l})$, Bob is able to construct a string of l bits that is equal to Alice's up to some error rate e_1^b. Given the knowledge of ξ_1^b and assuming the adequacy of the ECC, Bob has enough information to determine $S_1(X_{1,\ldots,l})$ with high probability. Then, for slice $i>1$, he estimates $S_i(X_{1,\ldots,l})$ using the estimator function $E_i(X',\overline{S}(X),\beta_1,\ldots,\beta_{i-1})$, where β_j is the random variable indicating Bob's knowledge of $S_j(X)$, so that $\beta_j=S_j(X)$ with arbitrarily high probability. [Note that the estimators can also be written as jointly working on l samples at once: $E_i(X'_{1,\ldots,l},\overline{S}(X_{1,\ldots,l}),\xi_1^b,\ldots,\xi_{i-1}^b)$, but we will preferably use the previous notation for its simplicity since, besides the ECC decoding, all the operations are done on each variable X or X' independently.]

We also need a supplementary function to ensure that the process on Bob's side is described using bijective functions: $\overline{E}(X',\overline{S}(X),\beta_1,\ldots,\beta_m)$ (or jointly $\overline{E}(X'_{1,\ldots,l},\overline{S}(X_{1,\ldots,l}),\xi_1^b,\ldots,\xi_m^b)$). As a convention, the range of $\overline{E}$ is $[0;1]$. $\overline{E}$ is chosen so that the mapping $\mathcal{E}$ defined below is invertible,

$$\mathcal{E}:(\overline{s},s'_{1,\ldots,m},x')\rightarrow(\overline{s},s'_{1,\ldots,m},E_1(x',\overline{s}),\ldots,E_m(x',\overline{s},s'_{1,\ldots,m-1}),\overline{E}(x',\overline{s},s'_{1,\ldots,m})).$$

Similarly to $\mathcal{S}$, the functions $E_{1,\ldots,m}$ of $\mathcal{E}$ cut the real line into intervals. However, these intervals are adapted as a function of the information sent by Alice, so as to estimate Alice's bits more reliably. Like for $\overline{S}$, the function $\overline{E}$ indicates where to find X' within an interval.

The mapping $\mathcal{S}$ summarizes Alice's process of conversion of her real values X into m bits (plus a continuous component). The mapping $\mathcal{E}$ represents the bits (and a continuous component) produced by Bob from his real values X' and his knowledge of $\overline{S}(X)$ and of the syndromes $\xi^b_{1,\ldots,m}$. The bits produced by the functions E_i are not yet corrected by the ECC, even though they take as input the corrected values of the previous slices $S_j(X)$, $j<i$. The description of the mapping $\mathcal{E}$ with the bits prior to ECC correction allows us to easily express the bit error rate between Alice's slices and Bob's estimators and thereby to deduce the size of the parity matrices of the ECC's needed for the binary correction. Simply, we define $e_i^b=\Pr[S_i(X)\neq E_i(X',\overline{S}(X),S_{1\ldots i-1}(X))]$. As the block size $l\rightarrow\infty$, there exist ECC's with size $l_i^b\rightarrow lh(e_i^b)$ and arbitrarily low probability of decoding error. The number of common (but not necessarily secret) bits produced by SEC is therefore asymptotically equal to $H(S_{1,\ldots,m}(X))-\Sigma_{i=1}^m h(e_i^b)$ per sample [24].

The generalization of the SEC to a quantum entanglement purification protocol is examined next.

B. Quantum sliced error correction

From classical binary error correcting codes, one can construct CSS quantum codes and use them to extract EPR pairs from noisy qubit pairs. We will now show that, similarly, from SEC, it is possible to construct an encoding and decoding procedure, which, when applied to entangled quantum oscillator systems, also allows one to extract pure EPR pairs. Such a purification protocol is formal, as it would of course be very difficult to implement in practice.

The purification uses a few quantum registers, which we now list. Alice's system a_1 is split into m qubit systems $\mathsf{s}_{1,\ldots,m}$ and a continuous register $\overline{\mathsf{s}}$. On Bob's side, the system b is split into m qubit systems $\mathsf{e}_{1,\ldots,m}$ and a continuous register $\overline{\mathsf{e}}$. He also needs m qubit registers $\mathsf{s}'_{1,\ldots,m}$ for temporary storage. All these registers must of course be understood per exchanged sample: As Alice generates l copies of the state $|\Psi\rangle$, the legitimate parties use l instances of the registers listed above.

The usual bit-flip and phase-flip operators $\mathbf{X}$ and $\mathbf{Z}$, respectively, can be defined as acting on a specific qubit register among the systems s_i and e_i. E.g., $\mathbf{Z}_{\mathsf{s}_i}$ is defined as acting on s_i only. These operators are used by Alice and Bob to construct the CSS codes that produce entangled qubits, which are in turn used to produce EPR pairs in the registers $\mathsf{s}_i\mathsf{e}_i$ for $i=1,\ldots,m$. Since each CSS code operates in its own register pair, the action of one does not interfere with the action of the other. It is thus possible to extract more than one EPR pair $|\phi^+\rangle$ per state $|\Psi\rangle$. If asymptotically efficient binary codes are used, the rate or EPR pairs produced is $R=\Sigma_i[1-h(e_i^b)-h(e_i^p)]$, where e_i^b (e_i^p) indicates the bit error rate (the phase error rate) [20].

The process that defines the content of the registers is described next.

1. Mappings $\mathcal{QS}$ and $\mathcal{QE}$

First, we define the unitary transformation $\mathcal{QS}$: $L^2(\mathbf{R}) \rightarrow L^2([0;1]) \otimes \mathcal{H}^{\otimes m}$ by its application to the basis of quadrature eigenstates:

$$|x\rangle_{\mathsf{a}_1} \rightarrow \sigma(x)|\overline{S}(x)\rangle_{\overline{\mathsf{s}}} \otimes |S_1(x)\rangle_{\mathsf{s}_1} \otimes \cdots \otimes |S_m(x)\rangle_{\mathsf{s}_m}. \quad (3)$$

The states $|\overline{s}\rangle_{\overline{\mathsf{s}}}$, $0 \leqslant \overline{s} \leqslant 1$, form an orthogonal basis of $L^2([0;1])$, $\sigma(x) = (\mathrm{d}_x \overline{S})^{-1/2}(x)$ is a normalization function, and $|s_i\rangle_{\mathsf{s}_i}$, $s_i \in \{0,1\}$, denotes the canonical basis of $\mathcal{H}$, the Hilbert space of a qubit. As a convention, the system s_i is called slice i. The transformation $\mathcal{QS}$ is depicted in Fig. 1.

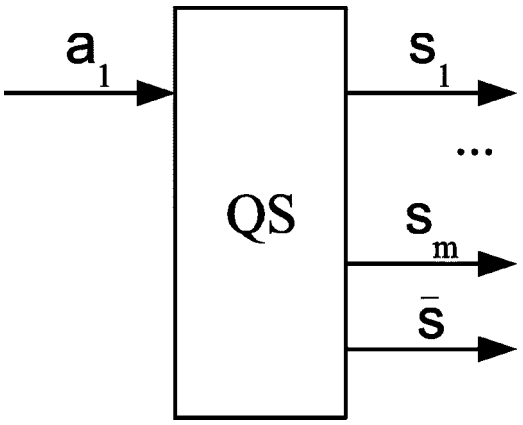

FIG. 1. Schematic description of $\mathcal{QS}$.

For each slice i, Alice and Bob agree on a CSS code, defined by its parity matrices H_i^b for bit error correction and H_i^p for phase error correction. For the entanglement purification, let us assume that Alice computes the syndromes of the CSS code with a quantum circuit. For each slice, she produces l_i^b qubits in the state $|\xi_i^b\rangle$ and l_i^p qubits in the state $|\xi_i^p\rangle$ that she sends to Bob over a perfect quantum channel, so that the syndromes are received without any distortion. In the entanglement purification picture, the syndromes can be transmitted over a nonperfect channel if they are encoded using appropriate error correcting codes. Also, after reduction to a prepare-and-measure protocol, this perfect transmission is actually done over the public authenticated channel. Alice also sends the $\overline{s}$ system to Bob.

Then, the slice estimators are defined as the unitary transformation $\mathcal{QE}$ from $L^2([0;1]) \otimes \mathcal{H}^{\otimes m} \otimes L^2(\mathbf{R})$ to $L^2([0;1]) \otimes \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes m} \otimes L^2([0;1])$:

$$|\overline{s}\rangle_{\overline{\mathsf{s}}}|s'_{1,\ldots,m}\rangle_{\mathsf{s}'_{1,\ldots,m}}|x'\rangle_{\mathsf{b}} \rightarrow \epsilon(x',\overline{s},s'_{1,\ldots,m})|\overline{s}\rangle_{\overline{\mathsf{s}}}|s'_{1,\ldots,m}\rangle_{\mathsf{s}'_{1,\ldots,m}} \otimes_{i=1}^{m} |E_i(x',\overline{s},s'_{1,\ldots,i-1})\rangle_{\mathsf{e}_i}|\overline{E}(x',\overline{s},s'_{1,\ldots,m})\rangle_{\overline{\mathsf{e}}}, \quad (4)$$

where $\epsilon(x',\overline{s},s'_{1,\ldots,m}) = (\partial_{x'}\overline{E})^{-1/2}(x',\overline{s},s'_{1,\ldots,m})$ is a normalization function; $|x'\rangle_{\mathsf{b}}$ is a quadrature eigenstate with $\mathbf{x}$ eigenvalue x'; $|e_i\rangle_{e_i}$, $e_i \in \{0,1\}$, denotes the canonical basis of $\mathcal{H}$; $|\overline{e}\rangle_{\overline{\mathsf{e}}}$, $0 \leqslant \overline{e} \leqslant 1$, form an orthogonal basis of $L^2([0;1])$. As the classical mapping $\mathcal{E}$ is invertible, $\mathcal{QE}$ is unitary with the appropriate normalization function ϵ. This mapping is defined to act on individual states, with the slice values $s'_{1,\ldots,m}$ as input in the system $\mathsf{s}'_{1,\ldots,m}$, whose purpose is actually to hold Bob's sequentially corrected bit values $\beta_{1,\ldots,m}$. The complete transformation jointly involving l systems would be fairly heavy to describe. Only the ECC correction needs to be described jointly, and assuming it is correctly sized (i.e., l_i^b are large enough), Bob has enough information to reconstruct Alice's bit values. Let us now sketch how the system $s'_{1,\ldots,m}$ is constructed.

Assume that Bob first calculates, using a quantum circuit, the first slice estimator [classically: $E_1(X', \overline{S}(X))$], which does not depend on any syndrome. That is, he applies the following mapping, defined on the bases of $\overline{\mathsf{s}}$ and b: $|\overline{s}\rangle_{\overline{\mathsf{s}}}|x'\rangle_{\mathsf{b}} \rightarrow |\overline{s}\rangle_{\overline{\mathsf{s}}}|E_1(x',\overline{s})\rangle_{\mathsf{e}_1}|\overline{E_1}(x',\overline{s})\rangle_{\overline{\mathsf{e}}_1}$ (up to normalization), where the function $\overline{E_1}$ is needed only to make the mapping unitary. From the l qubits in the l systems e_1 and the syndrome sent by Alice $|\xi_1^b\rangle$, there exists a quantum circuit that calculates the relative syndrome of Alice's and Bob's bits—that is, a superposition of the classical quantities $\xi_1^b \oplus H_1^b E_1(X_{1,\ldots,l})$. From this, a quantum circuit calculates the coset leader of the syndrome—that is, (a superposition of) the most probable difference vector between Alice's and Bob's qubits. An extra $l - l_1^b$ blank qubits are needed for this operations; we assume they are all initialized to $|0\rangle$:

$$|H_1^b(s_1^{(l)} \oplus e_1^{(l)})\rangle_{s_1'^{(l_1^b)}}|0\rangle_{s_1'^{(l-l_1^b)}} \rightarrow |s_1^{(l)} \oplus e_1^{(l)}\rangle_{s_1'^{(l)}}.$$

Then, using a controlled-NOT operation between Bob's bits (control) and the difference vector (target), we produce l qubits containing the same bit values as Alice's, with an arbitrarily large probability:

$$|e_1^{(l)}\rangle_{e_1^{(l)}}|s_1^{(l)} \oplus e_1^{(l)}\rangle_{s_1'^{(l)}} \rightarrow |e_1^{(l)}\rangle_{e_1^{(l)}}|s_1^{(l)}\rangle_{s_1'^{(l)}}.$$

This is how the l systems s'_1 are created.

Following this approach for the next slices, we can define $|\overline{s}\rangle_{\overline{s}}|s_1\rangle_{s_1'}|E_1(x',\overline{s})\rangle_{e_1}|\overline{E_1}(x',\overline{s})\rangle_{\overline{e_1}}$ $\rightarrow |\overline{s}\rangle_{\overline{s}}|s_1\rangle_{s_1'}|E_1(x',\overline{s})\rangle_{e_1}|E_2(x',\overline{s},s_1)\rangle_{e_2}|\overline{E_2}(x',\overline{s},s_1)\rangle_{\overline{e_2}}$ and reasonably assume that the bit value given in s'_1 is equal to Alice's $S_1(X)$. This reasoning can be applied iteratively, so as to fill the system $s'_{1,\ldots,m}$ with all the corrected bit values and with an extra step to set $\overline{E}(x',\overline{s},s_{1,\ldots,m})$ in $\overline{e}$.

As a last step, Bob can revert the ECC decoding operations and come back to the situation where he has blank qubits in $s'_{1,\ldots,m}$ as depicted in Fig. 2.

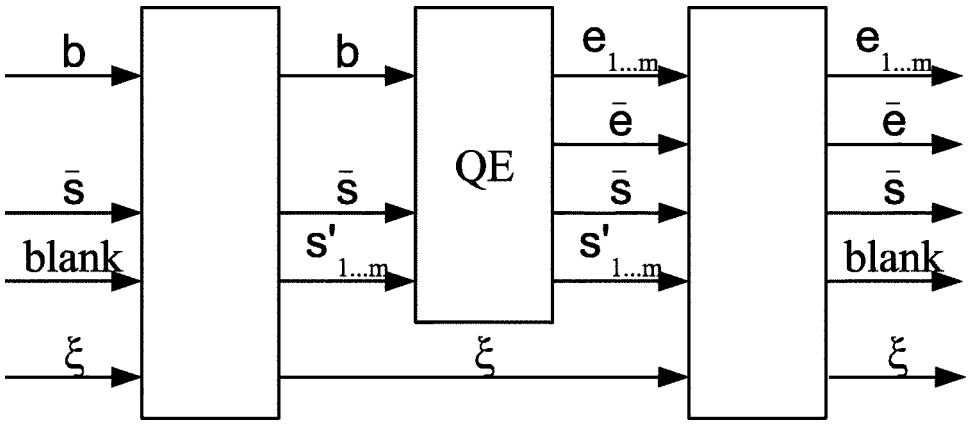

FIG. 2. Schematic description of $\mathcal{QE}$ and the use of the systems $\mathsf{s}'_{1,\ldots,m}$.

Finally, the qubits produced by $\mathcal{QE}$ can be transformed into EPR pairs using the CSS codes and the syndromes Alice sent to Bob.

2. Phase coherence

Neither the unitary transformation $\mathcal{QS}$ nor $\mathcal{QE}$ take into account the modulation of the coherent state in the **p** quadrature. By ignoring what happens in the a_2 system of Eq. (1), the reduced system $\rho_{\mathsf{a}_1\mathsf{b}}$ lacks phase coherence:

$$\rho_{\mathsf{a}_1\mathsf{b}} = \int \mathrm{d}x\mathrm{d}x'\mathrm{d}p\sqrt{G_1(x)G_1(x')}G_2(p)|x\rangle_{\mathsf{a}_1}\langle x'| \otimes D(ip)|x+i0\rangle_{\mathsf{b}}\langle x'+i0|D^{\dagger}(ip).$$

To remedy this, we assume that Alice also sends the a_2 system to Bob, just like she does for the $\bar{\mathsf{s}}$ system and the syndromes, since the modulation in the **p** quadrature is independent of the key. Bob can take it into account before applying $\mathcal{QE}$, by displacing his state along the **p** quadrature in order to bring it on the **x** axis.

Actually, we could formally include this a_2-dependent operation in the $\mathcal{QE}$ mapping by adding $|p\rangle_{\mathsf{a}_2}$ to its input and output (unmodified) and by multiplying by a factor of the form $e^{ix'p/4N_0}$ in Eq. (4) with N_0 the vacuum fluctuations. For notation simplicity, however, we mention it here without explicitly writing it.

Also, for the simplicity of the notation in the next section, we can assume without loss of generality that the coefficients of $|\Psi\rangle$ in the **x** basis of b are real, after adjustment by Bob as a function of p.

3. Construction of $\bar{S}$ and $\bar{E}$

Let us now make explicit the construction of the functions $\bar{S}$ and $\bar{E}$. First assume, for simplicity, that we have only one slice ($m=1$)—for this we do not write the slice index as a subscript. The mapping has thus the following form:

$$|x\rangle_{\mathsf{a}_1}|x'\rangle_{\mathsf{b}} \to \sigma(x)|S(x)\rangle_{\mathsf{s}}|\bar{S}(x)\rangle_{\bar{\mathsf{s}}}\epsilon(x',\bar{S}(x),S(x)) \otimes |E(x',\bar{S}(x))\rangle_{\mathsf{e}}|\bar{E}(x',\bar{S}(x),S(x))\rangle_{\bar{\mathsf{e}}},$$

where $\sigma(x)=(\mathrm{d}_x\bar{S})^{-1/2}(x)$, $\epsilon(x',\bar{s},s)=(\partial_{x'}\bar{E})^{-1/2}(x',\bar{s},s)$, and $\bar{S}$ and $\bar{E}$ range between 0 and 1.

Let us take some state ρ of the systems $\mathsf{s}\bar{\mathsf{s}}\mathsf{e}\bar{\mathsf{e}}$. In the entanglement purification picture, our goal is to be able to extract entangled pairs in the subsystem $\rho_{\mathsf{se}}=\mathrm{Tr}_{\mathrm{All}\setminus\{\mathsf{s},\mathsf{e}\}}(\rho)$. We thus want ρ to be a product state of the form $\rho_{\mathsf{s}\bar{\mathsf{s}}}\otimes\rho_{\mathsf{e}\bar{\mathsf{e}}}$. If $\bar{S}(X)$ contains information about $S(X)$ or if $\bar{E}(X',S(X),S(X))$ contains information about $E(X',\bar{S}(X))$, the subsystem ρ_{se} will not be pure. In the prepare-and-measure picture, information on $S(X)$ in $\bar{S}(X)$ will be known to Eve and therefore may not be considered as secure. Note that information in $\bar{E}(\cdots)$ is not disclosed, but since it is excluded from the subsystems from which we wish to extract entanglement (or secrecy), any correlation with $\bar{\mathsf{e}}$ will reduce the number of entangled qubits (or secret bits); or stated otherwise, the calculated number of secret bits will be done as if $\bar{E}(\cdots)$ was public. As an extreme example, if $S(X)$ and $E(X',\bar{S}(X))$ are perfectly correlated and if $S(X)$ can be found directly as a function of $\bar{S}(X)$, then ρ_{se} will be of the form $\rho_{\mathsf{se}}=p_0|00\rangle\langle 00|+p_1|11\rangle\langle 11|$, which does not allow us to extract any EPR pairs or, equivalently, does not contain any secret information. Consequently, $\bar{S}$ and $\bar{E}$ should be as statistically independent as possible of S and E.

We define $\bar{S}$ and $\bar{E}$ as the following cumulative probability functions: $\bar{S}(x)=\Pr[X\leqslant x|S(X)=S(x)]$ and $\bar{E}(x',\bar{s},s)=\Pr[X'\leqslant x'|\bar{S}(X)=\bar{s},S(X)=s,E(X',\bar{s})=E(x',\bar{s})]$. By definition, these functions are uniformly distributed between 0 and 1, independently of the other variables available to the party calculating it (Alice for $\bar{S}$ and Bob for $\bar{E}$). These functions also enjoy the property of making the subsystem ρ_{se} pure in absence of eavesdropping (i.e., when ρ is pure), indicating that this choice of $\bar{S}$ and $\bar{E}$ does not introduce more impurity in ρ_{se} than ρ already has.

For a pure state $|\psi\rangle = \int dx dx' f(x,x') |x\rangle_{a_1} |x'\rangle_b$, with $|x\rangle_{a_1}$ ($|x'\rangle_b$) an **x** eigenstate in a_1 (in b), the application of $\mathcal{QS}$ and $\mathcal{QE}$ gives

$$\sum_{s,e\in\{0,1\}} \int d\bar{s} d\bar{e} \sigma(x) \epsilon(x',\bar{s},s) f(x,x') |s\rangle_s |\bar{s}\rangle_{\bar{s}} |e\rangle_e |\bar{e}\rangle_{\bar{e}},$$

where x and x' are shorthand notation for $x(s,\bar{s})$ and $x'(e,\bar{e},\bar{s})$, respectively. Let f_1 and f_2 be real and nonnegative functions verifying $f(x,x') = f_1(x) f_2(x,x')$. $f_1(x)$ is chosen such that $|f_1(x)|^2$ is the probability density function of Alice's modulation and $f_2(x,x')$ such that $|f_2(x,x')|^2$ is the probability density function of Bob's measured value x' conditionally to Alice sending x. Then, it is easy to check that we can factor $\Sigma_{a,b\in\{0,1\}} \alpha_{ab} |ab\rangle_{se}$ out of $|\psi\rangle$ by setting

$$\sigma(x(s,\bar{s})) = \sigma_0(s)[f_1(x(s,\bar{s}))]^{-1}, \tag{5}$$

$$\epsilon(\bar{s},x'(e,\bar{e},\bar{s}),s) = \epsilon_0(e,s)[f_2(x(s,\bar{s}),x'(e,\bar{e},\bar{s}))]^{-1}, \tag{6}$$

where

$$\sigma_0^2(s) = \int_{x:S(x)=s} |f_1(x)|^2 dx, \tag{7}$$

$$\epsilon_0^2(e,s) = \int_{x,x':S(x)=s,E(x',\bar{S}(x))=e} |f_2(x,x')|_2 dx dx'. \tag{8}$$

The conclusion follows from the definition of σ and ϵ.

When more than one slice is involved, the functions $\bar{S}$ and $\bar{E}$ are defined similarly:

$$\bar{S}(x) = \Pr[X \leq x | S_{1,\ldots,m}(X) = S_{1,\ldots,m}(x)], \tag{9}$$

$$\begin{aligned}\bar{E}(x',\bar{s},s_{1,\ldots,m}) = \Pr[X' \leq x' | \bar{S}(X) = \bar{s} \\ \wedge S_{1,\ldots,m}(X) = s_{1,\ldots,m} \\ \wedge E_1(X',\bar{s}) = E_1(x',\bar{s}) \wedge \\ \cdots \wedge E_m(X',\bar{s},s_{1,\ldots,m-1}) \\ = E_m(x',\bar{s},s_{1,\ldots,m-1})].\end{aligned} \tag{10}$$

V. ATTENUATION CHANNEL

We now apply the slicing construction and display some results on the rates one can achieve in an important practical case. These results serve as an example and do not imply an upper bound on the achievable rates or distances. Instead, they can be viewed as lower bounds on an achievable secure rate in the particular case of an attenuation channel with given losses. Stated otherwise, this section simulates the rates we would obtain in a real experiment where Alice and Bob would be connected by an attenuation channel. For more general properties of the construction, refer to Sec. VI.

The purpose of this section is twofold. First, we wish to illustrate the idea of the previous section and show that it serves realistic practical purposes. Beyond the generality of the sliced error correction, its implementation may be easier than it first appears. Furthermore, the purification (distillation) of more than one qubit (bit) per sample is useful, as illustrated below.

Second, it is important to show that the construction works in a case as important as the attenuation channel. Clearly, requesting that a QKD protocol yields a nonzero secret key rate under all circumstances is unrealisitic—an eavesdropper can always block the entire communication. On the other hand, a QKD protocol that would always tell Alice and Bob that zero secure bits are available would be perfectly secure but obviously also completely useless. Of course, between these two extreme situations, the practical efficiency of a QKD protocol is thus important to consider.

The attenuation channel can be modeled as if Eve installed a beam splitter in between two sections of a lossless line, sending vacuum at the second input. We here assume that Alice sends coherent states with a modulation variance of $31N_0$, with N_0 the vacuum fluctuations, which gives Alice and Bob up to $I(A;B) = 2.5$ common bits in absence of losses or noise. This matches the order of magnitude implemented in [14]. We define the slices S_1 and S_2 by dividing the real axis into four equiprobable intervals labeled by two bits, with S_1 representing the least significant bit and S_2 the most significant one. More precisely, $S_1(x) = 0$ when $x \leq -\tau$ or $0 < x \leq \tau$ and $S_1(x) = 1$ otherwise, with $\tau = \sqrt{2 \times 31N_0}\, \mathrm{erf}^{-1}(1/2)$, and $S_2(x) = 0$ when $x \leq 0$ and $S_2(x) = 1$ otherwise.

In this constructed example, we wish to calculate the theoretical secret key rate we would obtain in an identical setting. For various loss values, the secret key rates are evaluated by numerically calculating $\mathrm{Tr}[(\mathbf{Z}_{s_i} \otimes \mathbf{Z}_{e_i})\rho]$, to obtain the bit error rates of slices $i = 1,2$ and $\mathrm{Tr}[(\mathbf{X}_{s_i} \otimes \mathbf{X}_{e_i})\rho]$ to obtain the phase error rates. Then, assuming asymptotically efficient binary codes, the rate is $R = R_1 + R_2 = \Sigma_{i=1,2}[1 - h(e_i^b) - h(e_i^p)]$.

Using this two-slice construction, we were able to get the EPR rates described in Table I. For the case with no losses, it is thus possible to distill $R = 0.752 + 0.938 = 1.69$ EPR pairs per sample. Also, note that the phase error rate increases faster with the attenuation for ρ_2 than for ρ_1, with $\rho_i = \rho_{s_i e_i} = \mathrm{Tr}_{\mathrm{All}\setminus\{s_i,e_i\}}(\rho)$. This intuitively follows from the fact that the information Eve can gain from her output of the beam splitter affects first the most significant bit contained in $S_2(X)$.

Due to the higher bit error rate in ρ_1, it was not possible to distill EPR pairs in slice 1 with losses beyond 0.7 dB. It was, however, still possible to distill EPR pairs in slice 2, up to 1.4 dB losses (about 10 km with fiber optics with losses of 0.15 dB/km). This result does not pose any fundamental limit, as it can vary with the modulation variance and with the choice of the functions S_1 and S_2. Note that the slice functions could be optimized in various ways, one of which being to use other intervals (as done in [24], not necessary equiprobable and possibly chosen as a function of the losses) and another being to consider multidimensional slices as explained in the next section.

Finally, note that although this example involves a Gaussian channel, this particularity is not exploited here and such a calculation can be as easily done for a non-Gaussian attack.

TABLE I. Error and EPR rates with two slices in an attenuation channel.

Losses (dB)	ρ_1			ρ_2		
	e_1^b	e_1^p	R_1	e_2^b	e_2^p	R_2
0.0	3.11%	0.53%	0.752	0.0000401	0.710%	0.938
0.4	3.77%	13.7%	0.193	0.0000782	28.6%	0.135
0.7	4.32%	20.0%	0.0204	0.000125	37.5%	0.0434
1.0		—		0.000194	42.3%	0.0147
1.4		—		0.000335	45.6%	0.00114

VI. ASYMPTOTIC BEHAVIOR

In this section, we study the behavior of the slice construction when the slice and slice estimator mappings take as input a block of w states, with w arbitrarily large. In [24], the classical sliced error correction is shown to reduce to Slepian-Wolf coding [29] (asymmetric case with side information) when using asymptotically large block sizes. We here study the quantum case, which is different at least by the fact that privacy amplification is explicitly taken into account.

For simplicity of the notation, we will study the asymptotic behavior in the case of an individually probed channel only (although Eve's measurement can be collective). A study of finite–width probing with a width much smaller than the key size would give the same results, since in both cases it allows us to consider a sequence of identical random experiments and to study the typical case. However, joint attacks, with the width as large as the key size, are outside the scope of this section, as the statistical tools presented here would not be suitable.

It is important to stress that we here investigate what the secret key rates would be if the actual channel is an individually probed one. The use of the protocol of this paper still requires us to evaluate the phase error rate in all cases and this quantity is sufficient to determine the number of secret key bits. In the case of joint attacks, the secret key rates stated in the special cases below would then differ from the one obtained using the phase error rate.

A. Direct reconciliation

We thus here consider a block of w states and the functions S, $\overline{S}$, E, and $\overline{E}$ on blocks of w variables as well. Among the qubits produced by $\mathcal{QS}$, there is a certain number of them whose disclosed value allows Alice and Bob to correct (almost) all bit errors for the remaining slices. Then, among the remaining slices, a certain number of qubits allows Alice and Bob to correct (almost) all phase errors for the rest of the qubits. These last qubits are thus equivalent to secret key bits in the prepare-and-measure protocol.

We consider the following state, with the action of the channel modeled as joining system b with that of an eavesdropper Eve and with p left out as a public classical parameter:

$$|\Psi(p)\rangle = \int \mathrm{d}x g(x)|x\rangle_{\mathsf{a}_1}|\phi(x,p)\rangle_{\mathsf{b,eve}}. \tag{11}$$

We consider w such states coherently, and the mappings $\mathcal{QS}$ and $\mathcal{QE}$ take all w states as input. We will follow the lines of the reasoning in [27,30,31] to show that the secret key rate tends to $I(X;X')-I(X;E)$ for $w\to\infty$, with X the random variable representing Alice's measure of a_1 with $\mathbf{x}$, X' the measure of b with $\mathbf{x}$, and $I(X;E)=H(X)+H(\rho_{\mathsf{eve}})-H(\rho_{\mathsf{a}_1,\mathsf{eve}})$, where $H(\rho)$ is the von Neumann entropy of a state ρ. The remainder of the discussion must be understood for any $\epsilon,\epsilon_U>0$, with w sufficiently large.

Consider a mapping U from $\mathbf{R}$ to a finite set $\mathcal{U}$ of size 2^m, for some sufficiently large m, such that $I(U(X);X') \geqslant I(X;X')-\epsilon_U$. Let $\overline{S}(X)$ be the remaining continuous information not contained in $U(X)$, defined as in Sec. IV B 3. Let $x(\overline{s},u)$ be the mapping that recovers x from $\overline{S}(x)$ and $U(x)$.

We here recall some definitions from [30]. For a given value of $\overline{s}^{(w)}$ and $p^{(w)}$ ($\overline{s}^{(w)},p^{(w)}\in\mathbf{R}^w$), a Holevo-Schumacher-Westmoreland (HSW) code [27,31] $\mathcal{B}$ is a subset of $\mathcal{U}^w$ such that the corresponding w-wide states $|\phi^{(w)}(x^{(w)}(\overline{s}^{(w)},u^{(w)}),p^{(w)})\rangle_{\mathsf{b}^{(w)},\mathsf{eve}}$, $u^{(w)}\in\mathcal{B}$, can be distinguished by Bob with probability at least $1-\epsilon$. A privacy amplification (PA) set $\mathcal{E}$ is a subset of $\mathcal{U}^w$ such that the sum of the corresponding states

$$\sum_{u^{(w)}\in\mathcal{E}}|\phi^{(w)}(x^{(w)}(\overline{s}^{(w)},u^{(w)}),p^{(w)})\rangle_{\mathsf{b}^{(w)},\mathsf{eve}}$$

factors Eve. Finally, a key generation code $\mathcal{B}$ is a HSW code that can be divided into a collection of nonoverlapping PA sets $\mathcal{B}=\cup_k\mathcal{E}_k$. In the sequel, we drop the w superscript for simplicity.

Consider three consecutive ranges $I=1,\ldots,|I|$, $J=|I|+1,\ldots,|I|+|J|$, and $K=|I|+|J|+1,\ldots,|I|+|J|+|K|$ with sizes $|I|=\lceil wH(U(X)|X')+\epsilon\rceil$, $|J|=\lceil wI(U(X);E)\rceil$, and $|K|=\lfloor wI(U(X);X')-wI(U(X);E)-\epsilon\rfloor$. Note that $|I|+|J|+|K|\leqslant wH(U(X))+2\leqslant wm+2$. These three ranges will correspond to three kinds of slices in the derived prepare-and-measure protocol: S_I, S_J, and S_K. S_I will give Bob enough information to perform error correction, S_J will contain bits, equal between Alice and Bob, which will be sacrificed with PA since they are not necessarily secret, and S_K will contain equal and secret bits (i.e., key bits).

From [30], it is possible to cover the space of $(wm+2)$-bit vectors with $2^{|I|}$ key generation codes $\mathcal{C}_{s_I}$ of size $2^{|J|+|K|}$. To

each element of $\mathcal{U}^w$, we assign a $|I|$-bit vector that identifies the key generation code it belongs to; this defines the first $|I|$ slices $S_I(X)$.

By providing the bit syndromes ξ_I^b to Bob, he can identify $S_I(X)=s_I$ and the associated key generation code C_{s_I}. By definition, he has enough information to identify an element within it. Such an element can be uniquely labeled by a $(|J|+|K|)$-bit vector, thereby defining S_J and S_K. So there exists a mapping that maps $|s_I\rangle_{\mathsf{s}_I'}|\phi(x(\overline{s,u}),p)\rangle_{\mathsf{b,eve}}$ onto $|s_I\rangle_{\mathsf{s}_I'}|s_{JK}\rangle_{\mathsf{e}_{JK}}|\phi'(x(\overline{s,u}),p)\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}}$ with probability at least $1-\epsilon$ and, thus, $e_i^b \leqslant \epsilon$, $\forall i \in J\cup K$.

Each key generation code contains $2^{|K|}$ PA sets of size $2^{|J|}$ each [30]. The labeling can be such that S_K corresponds to the identification of the PA set and S_J the element inside the PA set.

Providing the phase syndromes ξ_J^p to Bob gives him enough information to determine the phase of Alice's qubits in s_J. If the phase errors are corrected by Bob, measuring or tracing out subsystems $\mathsf{s}_J\mathsf{e}_J$ is equivalent to summing the slices in J over all possible bit values and thus factoring out Eve. More precisely, with $\overline{s}$, s_I, and p fixed (and the corresponding subsystems not shown) and with $|s_j^*\rangle_{\mathsf{s}_j^*}=2^{-1/2}[|0\rangle_{\mathsf{s}_j}+(-1)^{s_j^*}|1\rangle_{\mathsf{s}_j}]$ (and similarly for e_j and s_j'), the system after correction of s_I is of the form

$$
\begin{aligned}
|\Psi\rangle &= \sum_{s_K s_J} |s_{JK}\rangle_{s_{JK}}|0\rangle_{\mathsf{s}_J'}|s_{JK}\rangle_{\mathsf{e}_{JK}}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}} \\
&= \sum_{s_K s_J s_J^* e_J^*} (-1)^{s_J(s_J^*+e_J^*)}|s_J^*\rangle_{\mathsf{s}_J^*}|s_K\rangle_{\mathsf{s}_K} \\
&\quad \otimes |0\rangle_{\mathsf{s}_J'}|e_J^*\rangle_{\mathsf{e}_J^*}|s_K\rangle_{\mathsf{e}_K}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}}.
\end{aligned}
$$

Then Alice sends to Bob information about her phase (s_J^*), which he stores in his auxiliary register s_J'. The state becomes

$$
\begin{aligned}
&\sum_{s_K s_J s_J^* e_J^*} (-1)^{s_J(s_J^*+e_J^*)}|s_J^*\rangle_{\mathsf{s}_J^*}|s_K\rangle_{\mathsf{s}_K} \\
&\quad \otimes |s_J^*\rangle_{\mathsf{s}_J'}|e_J^*\rangle_{\mathsf{e}_J^*}|s_K\rangle_{\mathsf{e}_K}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}}.
\end{aligned}
$$

The difference between Alice's and Bob's phases is calculated in s_J' and the correction is applied to e_J^*. Overall, this transformation can be summarized as $|s_J^*\rangle_{\mathsf{s}_J'}|e_J^*\rangle_{\mathsf{e}_J^*}\rightarrow|s_J^*+e_J^*\rangle_{\mathsf{s}_J'}|s_J^*\rangle_{\mathsf{e}_J^*}$. This gives the following state:

$$
\begin{aligned}
&\sum_{s_K s_J^*} |s_J^*\rangle_{\mathsf{s}_J^*}|s_K\rangle_{\mathsf{s}_K}|s_J^*\rangle_{\mathsf{e}_J^*}|s_K\rangle_{\mathsf{e}_K} \otimes \sum_{s_J,(s_J^*+e_J^*)} (-1)^{s_J(s_J^*+e_J^*)} \\
&\quad \times|s_J^*+e_J^*\rangle_{\mathsf{s}_J'}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}} = \sum_{s_K s_J^*} |s_J^*\rangle_{\mathsf{s}_J^*}|s_K\rangle_{\mathsf{s}_K}|s_J^*\rangle_{\mathsf{e}_J^*}|s_K\rangle_{\mathsf{e}_K} \\
&\quad \otimes \sum_{s_J} |s_J\rangle_{\mathsf{s}_J'^*}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}}.
\end{aligned}
$$

Finally, the sum $\Sigma_{s_J}|s_J\rangle_{\mathsf{s}_J'^*}|\phi'(s_{JK})\rangle_{\overline{\mathsf{e}},\mathsf{e}_I,\mathsf{eve}}$ factors out Eve, by definition of a PA set.

Given the size of K, we conclude that the secret bit rate can asymptotically come as close as desired to $I(X;X')-I(X;E)$. Note that in the particular case of the attenuation channel, an evaluation of the secret key rate can be found in [16,17].

B. Reverse reconciliation

So far, we have always assumed that the slices apply to Alice and the slice estimators to Bob. However, there are some cases for which the opposite case increases the secret bit rate [14].

Let us start again from the state $|\Psi(p)\rangle$ as in Eq. (11) and rewrite $|\phi(x,p)\rangle_{\mathsf{b,eve}}$ as $|\phi(x,p)\rangle_{\mathsf{b,eve}}=\int dx' f(x,p,x')|x'\rangle_{\mathsf{b}}|\phi(x,p,x')\rangle_{\mathsf{eve}}$. Let $h(x',p)$ be a nonnegative real function such that $h^2(x',p)=\int dx|g(x,p)f(x,p,x')|^2$. Then,

$$
|\Psi(p)\rangle = \int dx' h(x',p)|x'\rangle_{\mathsf{b}}|\phi'(x',p)\rangle_{\mathsf{a}_1,\mathsf{eve}},
$$

with

$$
\begin{aligned}
|\phi'(x',p)\rangle_{\mathsf{a}_1,\mathsf{eve}} = \int dx g(x,p) f(x,p,x')/h(x',p) \\
\times|x\rangle_{\mathsf{a}_1}|\phi(x,p,x')\rangle_{\mathsf{eve}}.
\end{aligned}
$$

Thus, by applying the same argument as for direct reconciliation, we can asymptotically reach $I(X;X')-I(X';E)$ secret bits when $\mathcal{QS}$ is applied on system b and $\mathcal{QE}$ on system a_1. The evaluation of the secret key rate for reverse reconciliation can also be found in [16,17], which indicates that such a quantity is always strictly positive in the case of an attenuation channel, regardless of the losses, for a sufficiently large modulation variance.

VII. CONCLUSION

In this paper, we studied the equivalence between an EP protocol and a QKD protocol with sliced error correction for reconciliation. In the QKD protocol, Alice sends Gaussian-modulated coherent states to Bob, who measures the result using homodyne detection. To probe the channel and determine the amount of entanglement that can be transmitted through it, Bob has to make homodyne measurements in all quadratures.

We found that the EP protocol based on sliced error correction is indeed efficient and allows its equivalent prepare-and-measure QKD protocol to produce a secret key which is secure against any eavesdropping strategy. Although the qubit encoding scheme is derived from a reconciliation protocol easily implementable in practice [14], the main drawback of the method is the possibly huge number of measurements to get a statistically relevant estimation of the phase error rate and thus the number of secret key bits. Yet in theory, the sample set can be reduced to an arbitrarily small fraction of the produced key, when an arbitrarily large number of quantum states are processed through secret key distillation.

An advantage of this method is that it can in principle be adapted to other modulation distributions—the fact that the modulation is Gaussian is not crucial. In practice, the finite range of the amplitude modulator does not allow one to pro-

duce a real Gaussian distribution for the prepare-and-measure protocol, and one can take this effect explicitly into account. Also, it may be more efficient to consider a modulation of coherent states along a uniform distribution over a finite domain of (x,p) [e.g., a square or a circle centered on (0,0)] so as to increase the correlations between Alice and Bob.

Open problems for further research include the improvement of the statistical estimation of the EP parameters, the investigation of other modulation distributions, and the optimization of the encoding scheme for practical implementations.

ACKNOWLEDGMENTS

We acknowledge discussions with Frédéric Bourgeois, Jaromír Fiurášek, Philippe Grangier, Frédéric Grosshans, Patrick Navez, John Preskill, and Serge Van Criekingen. We acknowledge financial support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, from the IUAP programme of the Belgian government under Grant No. V-18, and from the EU under Project SECOQC (Grant No. IST-2002-506813), COVAQIAL (Grant No. FP6-511004), and RESQ (Grant No. IST-2001-35759). S.I. acknowledges support from the Belgian FRIA Foundation, as well as the Swiss NCCR.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] T. C. Ralph, Phys. Rev. A **61**, 010303 (2000).
[3] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[4] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[5] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[6] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[7] K. Bencheikh, T. Symul, A. Jankovic, and J.-A. Levenson, J. Mod. Opt. **48**, 1903 (2001).
[8] P. Navez, Eur. Phys. J. D **18**, 219 (2002).
[9] C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[10] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[11] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003).
[12] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B: Lasers Opt. **79**, 273 (2004).
[13] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[14] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[15] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[16] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[17] M. Navascués and A. Acín, Phys. Rev. Lett. **94**, 020505 (2005).
[18] M. Christandl, R. Renner, and A. Ekert, e-print quant-ph/0402131.
[19] R. Renner and R. König, *Second Theory of Cryptography Conference, TCC 2005* (Springer, New York, 2005), Vol. 3378, p. 407.
[20] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[21] S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
[22] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[23] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[24] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
[25] F. Grosshans, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[26] G. D'Ariano, M. G. Paris, and M. F. Sacchi, Adv. Imaging Electron Phys. **128**, 205 (2003).
[27] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[28] G. D'Ariano, C. Macchiavello, and N. Sterpi, Quantum Semiclassic. Opt. **9**, 929 (1997).
[29] D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **19**, 471 (1973).
[30] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[31] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).