Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution

Frédéric Grosshans*
Max-Planck-Institut für Quantumoptik, Hans-Kopfermann-Strasse 1, D-85746 Garching, Germany
(Received 27 July 2004; published 21 January 2005)

We present here an information theoretic study of Gaussian collective attacks on the continuous variable key distribution protocols based on Gaussian modulation of coherent states. These attacks, overlooked in previous security studies, give a finite advantage to the eavesdropper in the experimentally relevant lossy channel, but are not powerful enough to reduce the range of the reverse reconciliation protocols. Secret key rates are given for the ideal case where Bob performs optimal collective measurements, as well as for the realistic cases where he performs homodyne or heterodyne measurements. We also apply the generic security proof of Christiandl *et al.* to obtain unconditionally secure rates for these protocols.

DOI: 10.1103/PhysRevLett.94.020504 PACS numbers: 03.67.Dd, 42.50.–p, 89.70.+c

Over the past few years, quantum continuous variables (CV) have been explored as an alternative to qubits for quantum key distribution (QKD) [1–7]. More specifically, protocols using coherent states and homodyne [1,2,8] or heterodyne [3] measurements have been proposed and experimentally demonstrated [9,10]. Relying on technologies allowing much higher rates than allowed by the single photon detectors used in qubit based QKD, those protocols are the only ones which could allow key rates in the GHz range in the foreseeable future.

However, the security proofs of these new protocols are not yet as strong as the ones of the qubits-based protocols: they are almost all limited to individual or finite-size [11] attacks. To our knowledge, the only unconditional security proofs of CV QKD protocols are [6,12,13], only the latter studying coherent-states based protocols. These proofs all rely on specific suboptimal key extraction procedures, and, for each case, it is difficult to separate the effects of the technical inefficiencies of the encoding scheme from the more fundamental effect of the possibility of real attacks of Eve—the eavesdropper.

In this Letter, we study the effects of a Gaussian collective attack on the key rate of CV QKD protocols based on the Gaussian modulation of coherent states [1–3] sent through a lossy channel. In these attacks, Eve uses a Gaussian unitary to interact with each of the transmitted pulse and stores her ancillas in a quantum memory. She performs then a collective measurement on her ancillas after Alice and Bob—the partners performing QKD—have used the public classical channel to fulfill the protocol.

After introducing the notation used in this Letter, we recall the values of various information theoretic quantities for Gaussian states. Then, we compute the secret key rate which can be achieved using direct reconciliation when Bob is allowed to do collective, heterodyne, or homodyne measurements. Those results are then extended to reverse reconciliation protocols and compared with the unconditionally secure rates obtained from the generic security proof of Christiandl *et al.* [4].

While completing this work, we learned Navascués and Acín used very similar techniques to study the security bounds of these protocols [14].

Notations.—In all the QKD protocols discussed in this Letter, Alice sends n Gaussian modulated coherent states through a lossy channel of transmission T.

Bob then makes measurements on the pulses he receives. It can be an optimal collective measurement or, more realistically, a series of heterodyne [3] or homodyne [1,2,9] measurements. Alice and Bob then agree on a secret key through a (direct or reverse) reconciliation procedure. We are interested in the asymptotic key rates obtained at the limit $n \to \infty$.

In the following, A refers to the quantum state of the light pulse prepared by Alice, B and E to the one received by Bob and Eve. X refers to the (classical) value of Alice's modulation and Y to the one of Bob's measurement. For instance, H_B denotes the Von Neumann entropy of the density matrix ρ_B at Bob's side, while H_Y denotes the Shannon differential entropy of Bob's measurements.

Alice modulates the two quadratures Q_X and P_X of the coherent states she sends with random values following Gaussian distribution. To simplify the analysis, we assume this modulation to be symmetric in Q and P.

If Bob performs a heterodyne measurement, he gets the two noisy measurements $Q_\mathsf{Y}^{\mathrm{het}} = Q_\mathsf{B} + Q_{\mathrm{noise}}$ and $P_\mathsf{Y}^{\mathrm{het}} = P_\mathsf{B} + P_{\mathrm{noise}}$, where Q_{noise} and P_{noise} are two independent Gaussian random variables of variance 1. (The units used in this Letter correspond to a unity variance of the vacuum.) If he performs a homodyne measurement, he perfectly measures one quadrature—say, Q—and obtains no information on the other—P. One has therefore $Q_\mathsf{Y}^{\mathrm{hom}} = Q_\mathsf{B}$ and $P_\mathsf{Y}^{\mathrm{hom}} = P_{\mathrm{noise}}$ (or, of course, the symmetric case, where $P_\mathsf{Y}^{\mathrm{hom}} = P_\mathsf{B}$ and $Q_\mathsf{Y}^{\mathrm{hom}} = Q_{\mathrm{noise}}$).

 © 2005 The American Physical Society

The lossy channel is modeled by a beam splitter of transmittivity T and reflectivity $1 - T$, the reflected beam being given to Eve. In the equivalent entanglement-based scheme [15], this attack gives Eve the purification of the mixed state $\rho_{\mathsf{AB}}^{\otimes n}$ shared by Alice and Bob. Eve then performs a collective measurement on her part of the purification, after Alice and Bob's classical communication has occurred. As shown below, this attack is more powerful than the ones studied in [1–3,9,11]. However, this attack model is not generic in two aspects.

First, the channel model itself is not generic, since we restrict ourselves to the lossy channel and omit considering nonzero added noise and non-Gaussian attacks. This restriction is only due to brevity consideration and will be lifted in a longer article [16], which will also contain a study of squeezed states protocols. Of course, in an experiment, the amount of added noise has to be measured by Alice and Bob through some sampling and is never exactly zero. They would thus have to use the more general results of [16].

A more fundamental restriction comes from the fact that we suppose Alice and Bob share a state of the form $\rho_{\mathsf{AB}}^{\otimes n}$. In other words, we restrict Eve to individual attacks on the channel, even if she is allowed to make collective measurements on the ancillas obtained through these attacks. This restriction is lifted at the end of this Letter, where we apply the generic security proof [4] that does not rely on any assumption about Eve's attack.

Entropies and mutual information.—Let V_{Q_B} (V_{P_B}) be the variance in the Q quadrature (P quadrature) of the Gaussian state ρ_B. Since squeezing is a reversible operation, it does not alter the Von Neumann entropy of ρ_B, which is an increasing function of $V_\mathsf{B} := \sqrt{V_{Q_\mathsf{B}} V_{P_\mathsf{B}}}$ [17]:

$$\begin{aligned} H_\mathsf{B} &= \tfrac{V_\mathsf{B}+1}{2}\log\tfrac{V_\mathsf{B}+1}{2} - \tfrac{V_\mathsf{B}-1}{2}\log\tfrac{V_\mathsf{B}-1}{2} \\ &= \log\tfrac{V_\mathsf{B}+1}{2} + \tfrac{V_\mathsf{B}-1}{2}\log\tfrac{1+1/V_\mathsf{B}}{1-1/V_\mathsf{B}}. \end{aligned} \tag{1}$$

The logarithms in the above expression should be taken in base 2 if one wants the result in bits, or in base e if one wants it in nats. For strong modulation ($V_\mathsf{B} \gg 1$), one uses the Taylor expansion

$$H_\mathsf{B} = \log V_\mathsf{B} + \log\tfrac{e}{2} + \mathcal{O}\Big(\tfrac{1}{V_\mathsf{B}}\Big).$$

Let V_{Q_Y} and V_{Q_Y} be the variances of Bob's two orthogonal quadrature measurements. The Shannon differential entropy H_Y is simply the logarithm of $V_\mathsf{Y} := \sqrt{V_{Q_\mathsf{Y}} V_{P_\mathsf{Y}}}$, up to an arbitrary additive constant [18], which can be set to 0:

$$H_\mathsf{Y} = \log V_\mathsf{Y}. \tag{2}$$

The rate of common information Alice and Bob can extract from their classical values is given by the mutual information [18]

$$I_{\mathsf{X;Y}} := H_\mathsf{Y} - H_{\mathsf{Y|X}} = H_\mathsf{X} + H_\mathsf{Y} - H_{\mathsf{XY}}.$$

If Bob uses a heterodyne detection, which adds a unit of noise, $V_\mathsf{Y}^{\mathrm{het}} = V_\mathsf{B} + 1$. Since a coherent state sent through a lossy channel stays a coherent state, the conditional variance are $V_{\mathsf{B|X}} = 1$ and $V_{\mathsf{Y|X}}^{\mathrm{het}} = V_{\mathsf{B|X}} + 1 = 2$. One has therefore

$$I_{\mathsf{X;Y}}^{\mathrm{het}} = \log\tfrac{V_\mathsf{B}+1}{2}. \tag{3}$$

If Bob is allowed to make arbitrary measurements on the pulses, the information they share is then given by the Holevo information [19,20]

$$I_{\mathsf{X;B}} := H_\mathsf{B} - H_{\mathsf{B|X}},$$

which is attained by collective measurements. Since Bob receives pure (coherent) states, $H_{\mathsf{B|X}} = 0$ and

$$I_{\mathsf{X;B}} = H_\mathsf{B} = I_{\mathsf{X;Y}}^{\mathrm{het}} + \tfrac{V_\mathsf{B}-1}{2}\log\tfrac{1+1/V_\mathsf{B}}{1-1/V_\mathsf{B}}. \tag{4}$$

If $V_\mathsf{B} \gg 1$, one has

$$I_{\mathsf{X;B}} = I_{\mathsf{X;Y}}^{\mathrm{het}} + \log e + \mathcal{O}\Big(\tfrac{1}{V_\mathsf{B}}\Big). \tag{5}$$

Therefore, by using heterodyne detection instead of the optimal collective measurement, Bob loses an amount of information up to $\log e$ (i.e., 1 nat $\simeq$ 1.44 bits) per pulse.

Direct key distribution.—To attain the rate $I_{\mathsf{X;Y}}$, Alice and Bob can use random codes of size $\exp(nI_{\mathsf{X;Y}})$, where the basis of the logarithms and the exponential are the same. Devetak and Winter have recently shown [21] that Alice can divide this code into privacy amplification subsets of size close to $\exp(nI_{\mathsf{X;E}})$. This allows Alice and Bob to generate a secret key through a direct reconciliation procedure using only forward communication. This key can be generated at a rate asymptotically close to

$$\Delta I_\triangleright := I_{\mathsf{X;Y}} - I_{\mathsf{X;E}}. \tag{6}$$

If Bob makes the optimal collective measurement, substituting $I_{\mathsf{X;Y}}^{\mathrm{coll}} = I_{\mathsf{X;B}}$ in the above expression and using Eq. (4) [with $V_\mathsf{B} = TV_\mathsf{A} + 1 - T$ and $V_\mathsf{E} = (1-T)V_\mathsf{A} + T$] gives us the attainable direct reconciliation key rate. At the high modulation limit, where $V_\mathsf{A} \gg 1/T; 1/(1-T)$, one has [22]

$$\Delta I_\triangleright^{\mathrm{coll}} = \log\tfrac{T}{1-T} + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_\mathsf{A}}\Big).$$

This limit is the same as the one found assuming Bob *and Eve* are restricted to heterodyne measurements [3] (individual attacks).

Direct heterodyne key distribution.—Equation (6) can be applied to the case where Bob uses heterodyne detection [3]. We have then a lossy channel of transmission T between Alice and Bob and another lossy channel of transmission $1 - T$ between Alice and Eve. We can therefore use Eqs. (3) and (4) to expand this expression into

$$\Delta I_\triangleright^{\mathrm{het}} = \log\tfrac{V_\mathsf{B}+1}{V_\mathsf{E}+1} - \tfrac{1}{V_\mathsf{E}-1}2\log\tfrac{1+1/V_\mathsf{E}}{1-1/V_\mathsf{E}}.$$

As shown by Eq. (5), Eve can gain up to 1 nat per pulse by using collective measurement. The best situation for Alice and Bob is the high modulation limit $V_{\mathsf{A}} \gg \frac{1}{1-T}$, where

$$\Delta I_{\triangleright}^{\mathrm{het}} = \log\frac{T}{1-T}\frac{1}{e} + \mathcal{O}\Big(\frac{1}{(1-T)V_{\mathsf{A}}}\Big).$$

It is therefore not possible to perform direct heterodyne QKD if the channel transmission is smaller than $T_{\min}^{\mathrm{het}} = e/(e+1) \simeq 0.73$. These maximal losses of 1.4 dB imply a shorter range for this protocol than the 3 dB deduced if one considers only individual attacks or if Bob uses optimal collective measurements.

Direct homodyne key distribution.—Surprisingly, the original proposal [1] of direct homodyne QKD is more robust. For those protocols, Alice modulates both quadratures Q and P with the same variance V_{A} and Bob chooses randomly one quadrature to measure (say, Q). After the public disclosure of this quadrature choice, the information on P is useless and can be forgotten by Alice. The state she has sent to Bob is therefore a mixture of coherent states with a given value of Q but different values of P. The mixture received by Bob is a Gaussian mixed state with variances $V_{Q_{\mathsf{B}}|\mathsf{X}}^{\mathrm{hom}} = 1$ and $V_{P_{\mathsf{B}}|\mathsf{X}}^{\mathrm{hom}} = V_{\mathsf{B}}$; therefore $V_{\mathsf{B}|\mathsf{X}}^{\mathrm{hom}} = \sqrt{V_{\mathsf{B}}}$. When $\sqrt{V_{\mathsf{B}}} \gg 1$, one has [22]

$$\begin{aligned} H_{\mathsf{B}|\mathsf{X}}^{\mathrm{hom}} &= \log\sqrt{V_{\mathsf{B}}} + \log\tfrac{e}{2} + \mathcal{O}\Big(\tfrac{1}{\sqrt{V_{\mathsf{B}}}}\Big), \\ H_{\mathsf{B}}^{\mathrm{hom}} &= \log V_{\mathsf{B}} + \log\tfrac{e}{2} + \mathcal{O}\Big(\tfrac{1}{V_{\mathsf{B}}}\Big), \\ I_{\mathsf{X};\mathsf{B}}^{\mathrm{hom}} &= \tfrac{1}{2}\log V_{\mathsf{B}} + \mathcal{O}\Big(\tfrac{1}{\sqrt{V_{\mathsf{B}}}}\Big) = I_{\mathsf{X};\mathsf{Y}}^{\mathrm{hom}} + \mathcal{O}\Big(\tfrac{1}{\sqrt{V_{\mathsf{B}}}}\Big). \end{aligned} \tag{7}$$

Thus, collective measurements give only a small amount (of order $1/\sqrt{V_{\mathsf{B}}}$) of supplementary information over homodyne detection; the noise in the useless quadrature (P) plays a crucial role in this.

Eve receives similar mixed states, and, in the strong modulation regime $[V_{\mathsf{A}} \gg 1/T; 1/(1-T)]$, one has

$$\Delta I_{\triangleright}^{\mathrm{hom}} = \tfrac{1}{2}\log\tfrac{T}{1-T} + \mathcal{O}\Big(\Big\{\tfrac{1}{\sqrt{T}} + \tfrac{1}{\sqrt{1-T}}\Big\}\tfrac{1}{\sqrt{V_{\mathsf{A}}}}\Big).$$

The advantage given to Eve by collective measurements is therefore of order $1/\sqrt{V_{\mathsf{A}}}$ and can be arbitrarily reduced by Alice's use of a strong enough modulation. Therefore, unlike the heterodyne protocol, the key rate of the direct homodyne key distribution protocol remains almost unchanged when compared to [1], where Eve was restricted to (postponed) homodyne measurements. More specifically the range limit of this protocol stays at 3 dB (50%) of losses, whether one considers collective measurements or not.

Reverse key generation.—For symmetry reasons, backward communication is needed to distribute a quantum key beyond this 3 dB limit. Either postselection [8,12] or a reverse reconciliation procedure [2,3,9] can be used for this purpose. In the latter case, the attainable rate is given by [21]

$$\Delta I_{\triangleleft} := I_{\mathsf{X};\mathsf{Y}} - I_{\mathsf{Y};\mathsf{E}}.$$

If Bob performs an optimal collective measurement, one has to replace the above expression by $I_{\mathsf{X};\mathsf{B}} - I_{\mathsf{B};\mathsf{E}}$, where $I_{\mathsf{B};\mathsf{E}}$ is the quantum mutual information

$$I_{\mathsf{B};\mathsf{E}} := H_{\mathsf{B}} + H_{\mathsf{E}} - H_{\mathsf{BE}}.$$

Since the joint state ρ_{BE} is obtained by the (reversible) mixture of ρ_{A} and a vacuum state in the mode N, one has $H_{\mathsf{BE}} = H_{\mathsf{A}} + H_{\mathsf{N}} = H_{\mathsf{A}}$. At the high modulation limit $[V_{\mathsf{A}} \gg 1/T; 1/(1-T)]$, one has therefore

$$\begin{aligned} I_{\mathsf{B};\mathsf{E}} &= \log V_{\mathsf{A}} + \log T(1-T)\tfrac{e}{2} + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_{\mathsf{A}}}\Big), \\ \Delta I_{\triangleleft}^{\mathrm{coll}} &= \log\tfrac{1}{1-T} + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_{\mathsf{A}}}\Big), \end{aligned}$$

which is, like in the direct case, very close to the result obtained with heterodyne detection in an individual attacks scenario [3]. For strong losses ($1/V_{\mathsf{A}} \ll T \ll 1$), this expression becomes

$$\Delta I_{\triangleleft}^{\mathrm{coll}} = T\log e + \mathcal{O}\Big(T^2 + \tfrac{1}{TV_{\mathsf{A}}}\Big).$$

Reverse heterodyne key generation.—In the heterodyne case [3], which is symmetric in Q and P, one has

$$\begin{aligned} V_{P_{\mathsf{E}}|\mathsf{Y}}^{\mathrm{het}} &= V_{Q_{\mathsf{E}}|\mathsf{Y}}^{\mathrm{het}} := V_{Q_{\mathsf{E}}} - \frac{\langle Q_{\mathsf{E}} Q_{\mathsf{Y}}^{\mathrm{het}}\rangle^2}{V_{Q_{\mathsf{Y}}}^{\mathrm{het}}} = \frac{2-T+T/V_{\mathsf{A}}}{T+(2-T)/V_{\mathsf{A}}}, \\ H_{\mathsf{E}|\mathsf{Y}}^{\mathrm{het}} &= \log\frac{1+1/V_{\mathsf{A}}}{T+(2-T)/V_{\mathsf{A}}} + \frac{(1-T)(1-1/V_{\mathsf{A}})}{T+(2-T)/V_{\mathsf{A}}}\log\frac{1+1/V_{\mathsf{A}}}{(1-T)(1-1/V_{\mathsf{A}})}. \end{aligned}$$

When $V_{\mathsf{A}} \gg 1/T$, this expression becomes

$$H_{\mathsf{E}|\mathsf{Y}}^{\mathrm{het}} = \log\tfrac{1-T}{T} - \tfrac{1}{T}\log(1-T) + \mathcal{O}\Big(\tfrac{1}{TV_{\mathsf{A}}}\Big).$$

If one also has $V_{\mathsf{A}} \gg 1/(1-T)$ [22],

$$\begin{aligned} H_E &= \log V_{\mathsf{A}} + \log\tfrac{e}{2}(1-T) + \mathcal{O}\Big(\tfrac{1}{(1-T)V_{\mathsf{A}}}\Big), \\ I_{\mathsf{Y};\mathsf{E}}^{\mathrm{het}} &= \log\tfrac{e}{2}TV_{\mathsf{A}} + \tfrac{1}{T}\log(1-T) + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_{\mathsf{A}}}\Big), \\ \Delta I_{\triangleleft}^{\mathrm{het}} &= \tfrac{1}{T}\log\tfrac{1}{1-T} - \log e + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_{\mathsf{A}}}\Big). \end{aligned}$$

As in the direct case, Eve gains a finite amount of information by using collective measurement instead of heterodyne measurements. However, this gain is not sufficient to reduce the range of the protocol, which still works for arbitrary long ranges. For strong losses ($1/V_{\mathsf{A}} \ll T \ll 1$), the rate is twice smaller than the collective measurement rate

$$\Delta I_{\triangleleft}^{\mathrm{het}} = \tfrac{1}{2}T\log e + \mathcal{O}\Big(T^2 + \tfrac{1}{TV_{\mathsf{A}}}\Big) \simeq \tfrac{1}{2}\Delta I_{\triangleleft}^{\mathrm{coll}}.$$

Reverse homodyne key generation.—In the homodyne case [2], similar calculations give us

$$V_{Q_{\mathsf{E}}|\mathsf{Y}}^{\mathrm{hom}} = \frac{1}{T+(1-T)/V_{\mathsf{A}}}, \qquad V_{P_{\mathsf{E}}|\mathsf{Y}}^{\mathrm{hom}} = V_{\mathsf{E}} = (1-T)V_{\mathsf{A}} + T,$$

$$V_{\mathsf{E}|\mathsf{Y}}^{\mathrm{hom}} = \sqrt{V_{\mathsf{A}}\frac{1-T+T/V_{\mathsf{A}}}{T+(1-T)/V_{\mathsf{A}}}}.$$

In the large modulation limit $[V_{\mathsf{A}} \gg 1/T; 1/(1-T)]$ [22],

$$V_{\mathsf{E|Y}}^{\mathrm{hom}} = \sqrt{V_{\mathsf{A}}\tfrac{1-T}{T}}\Big[1 + \mathcal{O}\Big(\Big\{\tfrac{1}{T} + \tfrac{1}{1-T}\Big\}\tfrac{1}{V_{\mathsf{A}}}\Big)\Big],$$

$$H_{\mathsf{E|Y}}^{\mathrm{hom}} = \tfrac{1}{2}\log\tfrac{1-T}{T}V_{\mathsf{A}} + \log\tfrac{e}{2} + \mathcal{O}\bigg(\tfrac{1}{TV_{\mathsf{A}}} + \sqrt{\tfrac{T}{(1-T)V_{\mathsf{A}}}}\bigg),$$

$$I_{\mathsf{Y;E}}^{\mathrm{hom}} = \tfrac{1}{2}\log(1-T)TV_{\mathsf{A}} + \mathcal{O}\bigg(\tfrac{1}{TV_{\mathsf{A}}} + \sqrt{\tfrac{T}{(1-T)V_{\mathsf{A}}}}\bigg),$$

$$\Delta I_{\triangleleft}^{\mathrm{hom}} = \tfrac{1}{2}\log\tfrac{1}{1-T} + \mathcal{O}\bigg(\tfrac{1}{TV_{\mathsf{A}}} + \sqrt{\tfrac{T}{(1-T)V_{\mathsf{A}}}}\bigg).$$

As for the direct case, the use of homodyne detection by Alice and Bob allows them to reduce the advantage given to Eve by coherent measurement to an arbitrarily small amount and to attain a secret key rate arbitrarily close to the one given in [2], where only individual attacks were considered. In the strong losses regime ($1/V_{\mathsf{A}} \ll T \ll 1$), the rate obtained is almost equal to the one obtained in heterodyne measurements:

$$\Delta I_{\triangleleft}^{\mathrm{hom}} = \tfrac{1}{2}T\log e + \mathcal{O}\Big(T^2 + \tfrac{1}{TV_{\mathsf{A}}}\Big) \simeq \Delta I_{\triangleleft}^{\mathrm{het}}.$$

The (almost) factor of two advantage in the rate given by heterodyne measurement at low losses cancels for strong losses. The use of the homodyne setup is also attractive in experimental QKD because of the sensitivity of the current continuous variable reconciliation algorithms [23,24] to the signal-to-noise ratio.

Unconditional security.—One can also compare these rates to the unconditionally secure rates S obtained from the generic security proof of Christiandl *et al.* [4]

$$S = I_{\mathsf{X;Y}} - H_{\mathsf{E}}, \tag{8}$$

which is independent of the reconciliation direction. Since Alice sends coherent states, as shown above $H_{\mathsf{E}} = I_{\mathsf{X;E}}$ and this unconditional secure rate is equal to the direct reconciliation rate $\Delta I_{\triangleright}^{\mathrm{coll}}$ ($\Delta I_{\triangleright}^{\mathrm{het}}$) when Bob makes collective (heterodyne) measurements, regardless of the actual reconciliation direction (direct or reverse).

The role of the unmeasured (P-)quadrature modulation makes the homodyne case different. If it decreased the efficiency of the collective attacks considered above, it increases the entropy H_{E}, decreasing the secure rate S given by Eq. (8). However, giving the information about this modulation to Eve could only decrease the secret rate. H_{E} is then given by (7) and, in the strong modulation regime [$V_{\mathsf{A}} \gg 1/(1-T)$], Eq. (8) becomes [22]

$$S^{\mathrm{hom}} = \tfrac{1}{2}\log\tfrac{T}{1-T}\tfrac{4}{e^2} + \mathcal{O}\bigg(\tfrac{1}{\sqrt{(1-T)V_{\mathsf{A}}}}\bigg).$$

Unconditionally secure homodyne QKD is therefore possible if the channel transmission T is greater than $T_{\min}^{\mathrm{hom}} = e^2/(e^2+4) \simeq 0.65$ (1.9 dB).

Conclusion.—We have quantified the effect of collective attacks on coherent-states based CV QKD protocols through a lossy channel. These attacks are strictly more powerful than the individual attacks studied before. However, if Bob makes homodyne measurements, the advantage given to Eve by these attacks can be made arbitrarily small if Alice uses a strong modulation. On the contrary, if Bob uses heterodyne measurement, these attacks give a finite advantage to Eve. For comparison, we have computed the key rate in the (theoretical) optimal case, where Bob performs a collective measurement.

We also have applied the generic security proof of Christiandl *et al.* [4] to compute an unconditional secure rate for these protocols. This rate is usually lower than the one obtained above, but, this bound being known not to be tight, this does not rule out the possibility for the considered collective attacks to be optimal.

This research was supported by a Marie Curie Intra European Fellowship within the 6th European Community Framework Programme (Contract No. MEIF-CT-2003-502045). I thank J. I. Cirac for enlightening discussions and his hospitality at the MPQ, and N. Lütkenhaus for bringing Ref. [21] to my attention. I acknowledge discussions with Ph. Grangier, M. M. Wolf, A. Acín, M. Navascués, S. Iblisdir, G. Giedke, and B. Kraus.

*Electronic address: frederic.grosshans@m4x.org

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

[2] F. Grosshans and Ph. Grangier, in *Proceedings of the 6th International Conference on Quantum Communications, Measurement, and Computing*, edited by J. H. Shapiro and J. O. Hirota (Rinton Press, Princeton, NJ, 2002), p. 351.

[3] Ch. Weedbrook *et al.*, Phys. Rev. Lett. **93**, 170504 (2004).

[4] M. Christiandl *et al.*, quant-ph/0402131 (2004).

[5] M. Hillery, Phys. Rev. A **61**, 022309 (2000),

[6] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001),

[7] N. J. Cerf *et al.*, Phys. Rev. A **63**, 052311 (2001),

[8] Ch. Silberhorn *et al.*, Phys. Rev. Lett. **89**, 167901 (2002),

[9] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).

[10] S. Lorenz *et al.*, quant-ph/0403064.

[11] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004),

[12] M. Navascués *et al.*, quant-ph/0405047 [Phys. Rev. Lett. (to be published)].

[13] S. Iblisdir *et al.*, Phys. Rev. Lett. **93**, 170502 (2004).

[14] M. Navascués and A. Acín, following Letter, Phys. Rev. Lett. **94**, 020505 (2005).

[15] F. Grosshans *et al.*, Quantum Inf. Comput. **3**, 535 (2003),

[16] M. Navascués, A. Acín, and F. Grosshans (to be published).

[17] G. S. Agarwal, Phys. Rev. A **3**, 828 (1971).

[18] C. E. Shannon, Bell Syst. Tech. J. **27**, 653 (1948).

[19] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).

[20] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

[21] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); quant-ph/0306078.

[22] The exact expressions, straightforward to compute but not very enlightening, have been omitted.

[23] G. Van Assche *et al.*, IEEE Trans. Inf. Theory **50**, 394 (2004).

[24] K.-C. Nguyen *et al.*, cs.IT/0406001 [in Proceedings of the 2004 International Symposium on Information Theory and its Applications (ISITA2004) (to be published)].