Quantum Information and Computation, Vol. 3, No. Special (2003) 535–552

VIRTUAL ENTANGLEMENT AND RECONCILIATION PROTOCOLS FOR QUANTUM CRYPTOGRAPHY WITH CONTINUOUS VARIABLES

FRÉDÉRIC GROSSHANS and NICOLAS J. CERF
École Polytechnique, CP 165, Université Libre de Bruxelles
B-1050 Brussels, Belgium

JÉRÔME WENGER, ROSA TUALLE-BROURI and PHILIPPE GRANGIER
Laboratoire Charles Fabry de l'Institut d'Optique
F-91403 Orsay cedex, France

Received June 20, 2003
Revised August 17, 2003

We discuss quantum key distribution protocols using quantum continuous variables. We show that such protocols can be made secure against individual gaussian attacks regardless the transmission of the optical line between Alice and Bob. This is achieved by reversing the reconciliation procedure subsequent to the quantum transmission, that is, using Bob's instead of Alice's data to build the key. Although squeezing or entanglement may be helpful to improve the resistance to noise, they are not required for the protocols to remain secure with high losses. Therefore, these protocols can be implemented very simply by transmitting coherent states and performing homodyne detection.

Here, we show that entanglement nevertheless plays a crucial role in the security analysis of coherent state protocols. Every cryptographic protocol based on displaced gaussian states turns out to be equivalent to an entanglement-based protocol, even though no entanglement is actually present. This equivalence even holds in the absence of squeezing, for coherent state protocols. This "virtual" entanglement is important to assess the security of these protocols as it provides an upper bound on the mutual information between Alice and Bob if they *had* used entanglement. The resulting security criteria are compared to the separability criterion for bipartite gaussian variables. It appears that the security thresholds are well within the entanglement region. This supports the idea that coherent state quantum cryptography may be unconditionally secure.

Keywords: Quantum key distribution, quantum cryptography, continuous variables, coherent states, quantum entanglement
Communicated by: J Shapiro & H-K Lo

1 Introduction

1.1 Continuous-variable quantum cryptography

In the presently very active field of continuous variable quantum information processing, a stimulating question is whether quantum continuous variables (QCV) [1] may provide a valid alternative to the usual "single photon" quantum key distribution (QKD) schemes [2]. Many recent proposals to use QCV for QKD (for a short review see [3]) have been based upon the use of "non-classical" states, such as squeezed or entangled light beams. We have nevertheless shown [3], and experimentally demonstrated [4], that there is actually no need for squeezed

or entangled light: QKD can be implemented simply by generating and transmitting random distributions of coherent states. More precisely, coherent state protocols are secure against individual gaussian attacks, while their security with respect to the line transmission depends on the *reconciliation protocol* which is used by Alice and Bob to correct the transmission errors. Using the so-called "direct reconciliation" (DR) protocols, a whole family of secure protocols can be obtained by using either coherent states, squeezed states, or Einstein-Podolsky-Rosen [5] (EPR) entangled beams [3, 6, 7], provided that the transmission of the line is larger than 50 percent (*i.e.* the losses are less than 3 dB). The security of these protocols is related to the limit imposed on the cloning of gaussian states [8, 9, 10], so that non-classical features like squeezing or EPR correlations have no influence on the achievable secret key rate. Interestingly, the 3 dB loss limit of these cryptographic protocols may be circumvented by modifying the reconciliation protocol. In ref. [4, 11], we have introduced "reverse reconciliation" (RR) protocols, and demonstrated their security for any value of the line transmission. Note that there exist, in principle, other ways for Alice and Bob to go beyond the 3 dB limit of DR protocols, namely by using entanglement purification [12] or postselection [13].

In the present paper, we will first review some basic properties of the direct and reverse reconciliation protocols. Then, we will show that each prepare-and-measure continuous-variable protocol is equivalent to an entanglement-based QKD protocol. This equivalence reminds us the link between the entanglement-free BB84 protocol [14] and the EPR-based protocol proposed by Ekert [15] that was pointed out in [16]. This equivalence allows us to compute the best estimate Alice may have on Bob's measurement outcome, if she *had* used an entanglement-based protocol. This, in turn, allows us to upper bound the information that an eavesdropper, Eve, can have on Bob's measurement results. In the case of a channel with losses but no added noise, Eve's estimate turns out to be always worse than Alice's estimate, which is the main reason for the increased security achieved by reversing the reconciliation protocol. Finally we will compare the security criteria derived from our approach to the entanglement criterion for bipartite gaussian variables. It appears that the corresponding security thresholds are well within the entanglement region, supporting the idea that coherent states quantum cryptography may be unconditionally secure.

1.2 Direct and reverse reconciliation protocols

In the first step of a generic QKD protocol, Alice prepares a quantum state and sends it to Bob, who makes a measurement on the state. Alternatively, Alice and Bob may share a pair of EPR-correlated systems and both make a measurement on their part. In order to warrant security, Alice and Bob must randomly choose to use different measurement bases, the transmitted data being kept only when the bases are compatible. After the quantum exchange, they thus have to agree on a common measurement basis, and discard the wrong measurements. At the end of this step, Alice, Bob, and the potential eavesdropper Eve, share a set of correlated data, called "key elements".

In a second step, Alice reveals some randomly chosen sample of the data that she sent, and Bob reveals his corresponding measurement outcomes. These samples allow them to measure some relevant parameters of the quantum channel, *e.g.* the error rate and the transmission (called "channel gain" for QCV protocols). Knowing the correlations between their key elements, Alice and Bob can evaluate the amount of information they share (I_{AB}), and the

information the eavesdropper Eve may have at most about their key elements (I_{AE} and I_{BE}). Therefore they can evaluate the size of the secret key they will be able to generate at the end of the protocol. If Eve knows too much, the size of this secret key will be zero, and Alice and Bob abort the protocol at this point.

In a third step, called "reconciliation", Alice and Bob use classical communications to extract a common binary key from their correlated key elements, revealing as little information as possible to a third party ignoring these key elements. This step usually uses parity-based algorithms like Cascade. It was adapted to continuous variables in Refs. [7, 17], where a "sliced" error correction procedure was devised in order to provide reconciled bits from real-valued key elements. There are actually two main options for doing the reconciliation, depending on whether Alice's or Bob's data are used to build the key. We will call these two options "direct reconciliation" (DR) and "reverse reconciliation" (RR), respectively, and will detail these procedures in Sections 1.2.1 and 1.2.2. The starting point will be the Csiszar-Körner theorem [18, 19] stating that a sufficient condition for distilling a secret key is that $\max(I_{AB} - I_{AE}, I_{AB} - I_{BE}) > 0$, the first and second term corresponding to DR and RR, respectively.

Finally, the fourth step of a practical QKD protocol consists in Alice and Bob performing "privacy amplification" in order to filter out Eve's information. Since this step is based on an evaluation of the amount of information collected by Eve on the reconciled key, a crucial requirement is to get a bound on I_{AE} for DR, or on I_{BE} for RR. For a coherent state protocol, the DR bound was given in ref. [3], and leads to a security limit for a line with a transmission of 1/2. In the following, we will establish the RR bound and show that it is not associated with a minimum value of the line transmission. In order to have a general approach, we will start by considering the exchange of entangled beams, and we will show later that for a particular choice of the measurement performed by Alice, this is equivalent to exchanging coherent states.

1.2.1 Direct Reconciliation (DR).

In direct reconciliation, Alice sends correction information to Bob, who accordingly corrects his key elements to have the same values as Alice. Alice infers from her estimate of I_{AB} the minimum amount of information she needs to reveal at this step. If the reconciliation protocol is perfect, it keeps $I_{AB} - I_{AE}$ constant. After reconciliation, Alice and Bob know a common bit string of length I_{AB} (slightly less if the reconciliation protocol is not perfect), and Eve knows I_{AE} bits of this string. It will provide a usable secret key if $I_{AB} - I_{AE} > 0$. We call this "direct reconciliation" (DR) because Bob is reconstructing what was sent by Alice, and the classical information flow in this step has the same direction as the initial quantum information flow.

Direct reconciliation is quite intuitive, and it was used in the coherent state QCV protocol that we proposed in ref. [3]. However, it is not secure as soon as the quantum channel transmission falls below 1/2. Intuitively, Eve could simulate the losses by a beam splitter and look at one output port of this beamsplitter. It seems obvious that, if she keeps the biggest part of the beam sent by Alice (*i.e.* if she simulate losses higher than 3 dB), she can extract more information from her beam than Bob ($I_{AE} > I_{AB}$), thus forbidding any secret key generation.

Note that this limitation is actually not specific to QCV: a "direct" version of BB84 would be a protocol where Bob would try to fill in the "empty slots" where he did not get any photon. Such a protocol actually only works when the losses are smaller than 3 dB. Indeed, suppose Alice has a perfect photon-gun and sends single photons to Bob, who measures their polarization with perfect detectors. If $G < 1$ denotes the transmission of the errorless lossy channel, Bob only receives and measures a fraction G of these photons. Even if we suppose that Bob has a quantum memory, allowing him to always make the right basis choice, we have $I_{AB} = G$. If the losses are due to Eve, which keeps the lost photons, $I_{AE} = 1 - G$. The security condition $I_{AB} - I_{AE} > 0$ for a "direct" version of BB84 is therefore $G > \frac{1}{2}$. The usual BB84 protocol works for higher losses because only the photons received by Bob (and therefore not intercepted by Eve) are considered for the key. As we will show in Sect. 1.2.2, this may be viewed as a reverse reconciliation where Alice corrects her value to match the ternary digit (0,1,no photon) held by Bob.

1.2.2 Reverse Reconciliation (RR).

We may instead reverse the reconciliation in the sense that Bob sends the correction information while Alice corrects her key elements to have the same values as Bob. Since Bob gives the correction information (also to Eve), this type of reconciliation keeps $I_{AB} - I_{BE}$ constant, and provides a usable key if $I_{AB} - I_{BE} > 0$. We call it "reverse reconciliation" (RR) because Alice adapts herself to what was received by Bob.

In a noiseless BB84 with finite line transmission, this step corresponds to Bob informing Alice of his "empty slots" where he did not get any photon, and Alice discarding the corresponding bits in order to have the same key. In our QCV protocol, there is no "empty slot" since homodyning the vacuum gives a gaussian distribution, and the RR procedure is intertwined with error correction. Then, alike BB84, it allows Alice and Bob to cross the 3-dB loss limit and extract a secret key for an arbitrarily low value of the line transmission.

However, in a practical realization, one cannot attain very high losses for several reasons. First, a realistic reconciliation protocol cannot reach the Shannon limit, so Alice and Bob actually obtain only a fraction of the information I_{AB} while one has to assume that Eve gets the full information I_{BE}. Said otherwise, the correction information that must be sent by Bob to Alice (but which is also monitored by Eve) is slightly larger than its ideal value predicted by Shannon theory. This makes the information difference vanish at some finite value of the line transmission. Another problem which must be taken into account is the following: while the RR procedure should be unidirectional (from Bob to Alice), the error correction using Cascade is a bidirectional process, so that some information also "leaks" from Alice to Eve. We have numerically evaluated this information leakage in practical cases [4] and it appears to be small, so we will not consider it further in the present paper. However, it must be kept in mind that the one-way or two-way character of the used error correction procedure plays a role, which should not be underestimated.

2 Preparation of a modulated gaussian beam through entanglement

The QKD protocols of the references [3, 4, 6, 7, 11] are based on randomly displaced squeezed or coherent states prepared by Alice. We will show in this section that Alice could equivalently prepare a pair of quantum entangled beams, measure one (or both) quadratures on one beam,

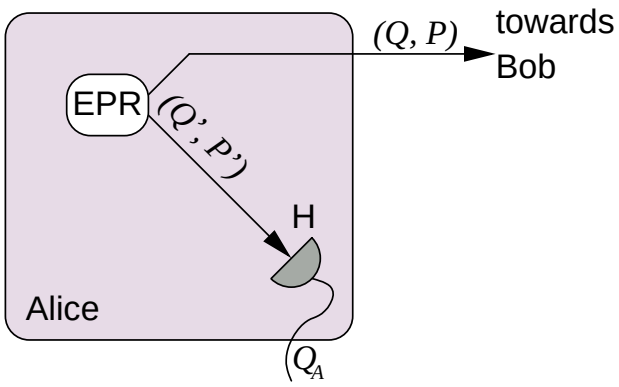

Fig. 1. **Measurement of a single quadrature.** Alice prepares two entangled beams (Q, P) and (Q', P') using an EPR source (EPR). She measures one quadrature on one beam with an homodyne detector (H) and deduces from it Q_A (or P_A), which is an estimate of Q (or P). She sends the other beam to Bob.

and send the other beam to Bob. This will be used in Sections 3 and 4 to find the maximum information Alice may have on Bob's data if she was using quantum entangled beams, and in Sect. 5 to compare the security conditions with the entanglement criterion for bipartite gaussian states.

2.1 Measurement of a single quadrature

Let us assume Alice prepares a pair of EPR beams, and denote by (Q, P) the quadratures of the beam sent to Bob and by (Q', P') the quadratures of the beam kept by Alice (see Fig. 1). To simplify the notations, we will suppose those beams to be initially symmetric in the two quadratures, *i.e.*

$$\langle Q^2 \rangle = \langle {Q'}^2 \rangle = V\, N_0 \qquad\qquad \langle P^2 \rangle = \langle {P'}^2 \rangle = V\, N_0, \tag{1}$$

where N_0 is the shot-noise variance.

These beams are entangled, and the measurement of a quadrature of one beam (*e.g.* Q') gives Alice information on the same quadrature of the other beam (Q). One can show [20, 21] that the best estimate Alice can have on Q knowing Q' is of the form $Q_A = \alpha Q'$ with $\alpha = \frac{\langle Q\, Q' \rangle}{\langle {Q'}^2 \rangle}$, the value of α being found by minimizing the variance of the error operator $\delta Q_A = Q - Q_A$. The *conditional variance* $V_{Q|Q_A}$ of Q knowing Q_A quantifies the remaining uncertainty on Q after the measurement of Q' giving the estimate Q_A of Q, and we have

$$V_{Q|Q_A} = \langle {\delta Q_A}^2 \rangle = \langle Q^2 \rangle - \frac{|\langle Q'\, Q \rangle|^2}{\langle {Q'}^2 \rangle}. \tag{2}$$

By using the commutation relation

$$[\delta Q_A, P] = \underbrace{[Q, P]}_{2i\,N_0} - \alpha\, \underbrace{[Q', P]}_{0}, \tag{3}$$

which directly follows from the definition of δQ_A, we find that the following uncertainty relation on the beam (Q,P) after the measurement of Q' holds :

$$V_{Q|Q_A} \times \langle P^2 \rangle \geq N_0^2. \tag{4}$$

Using the expression (2), we obtain

$$|\langle Q'\, Q \rangle|^2 \leq \langle Q'^2 \rangle \langle Q^2 \rangle - N_0^2 \frac{\langle Q'^2 \rangle}{\langle P^2 \rangle}. \tag{5}$$

By definition, the EPR beams are maximally correlated and saturate this limit, which gives

$$\langle Q'\, Q \rangle = \sqrt{V^2 - 1}\, N_0 \qquad\qquad V_{Q|Q_A} = \frac{N_0}{V} \tag{6}$$

Since by measuring Q' Alice deduces Q_A, and since $Q = Q_A + \delta Q_A$, the beam (Q,P) is projected onto a Q-squeezed state of squeezing parameter $s = V_{Q|Q_A}/N_0 = 1/V$ centered on $(Q_A, 0)$.

Alternatively, Alice could measure the quadrature P', yielding the estimator $P_A = -\alpha P'$, which gives

$$\langle P'\, P \rangle = -\sqrt{V^2 - 1}\, N_0 \qquad\qquad V_{P|P_A} = \frac{N_0}{V} \tag{7}$$

Of course, by measuring P', Alice learns P_A and projects the other beam onto a P-squeezed state centered on $(0, P_A)$ with the same squeezing parameter $s = 1/V$.

2.2 Simultaneous measurement of Q' and P'

Another possibility for Alice is to measure simultaneously Q' and P'. In this case, her measurement outcomes are more noisy, so she projects the beam (Q,P) onto a lesser squeezed state. A crucial point for our protocol is that she prepares a coherent state if her measurement is balanced in Q and P, as we will show below.

Denoting as Q'_A and P'_A the values of Q' and P' measurements, the associated added noises $\delta Q'_A$ and $\delta P'_A$ are defined as

$$\delta Q'_A = Q' - Q'_A \qquad\qquad \delta P'_A = P' - P'_A, \tag{8}$$

A possible way to perform such a joint measurement is to split Alice's beam with a beamsplitter of transmission T (in intensity), measuring separately each quadrature at each output port of the beamsplitter (see Fig. 2). Then, Q'_A and P'_A are the best estimators of Q' and P', proportional to the outputs of homodyne detectors placed on each of the output port.

Since Q'_A and P'_A are known simultaneously, they commute, $[Q'_A, P'_A] = 0$. Therefore, $[\delta Q'_A, \delta P'_A] = -[Q', P']$ and the noise variances obey the following inequality:

$$\langle \delta {Q'_A}^2 \rangle \langle \delta {P'_A}^2 \rangle \geq {N_0}^2. \tag{9}$$

If this inequality is saturated, that is if Alice makes an optimal joint measurement, this measure is characterized by the positive number μ, defined by

$$\langle \delta {Q'_A}^2 \rangle = \mu\, N_0 \qquad \text{and} \qquad \langle \delta {P'_A}^2 \rangle = \frac{1}{\mu}\, N_0. \tag{10}$$

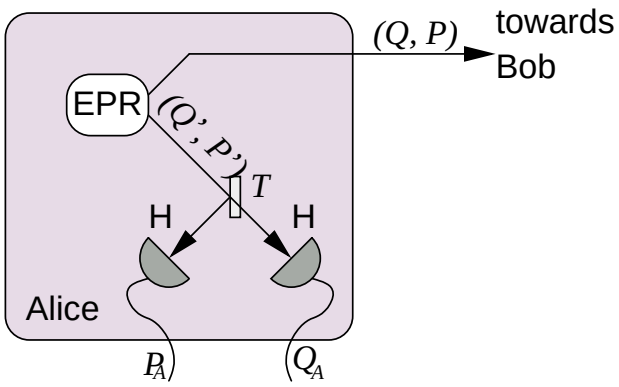

Fig. 2. **Measurement of both quadratures.** Alice can measure both quadratures of her beam, as explained in the text, using a beamsplitter of transmission T and two homodyne detectors H. She then simultaneously obtains Q_A and P_A, which are estimates of Q and P.

If the measurement is made with the beamsplitter setup described above, we have

$$\mu = \frac{1-T}{T} \qquad \text{or} \qquad T = \frac{1}{1+\mu} \tag{11}$$

If $\mu = 1$, Alice measures Q' and P' with the same (shot-noise limited) precision. This case corresponds to a 50:50 beamsplitter ($T = \frac{1}{2}$). If $\mu < 1$, Alice measures Q' with a sub-shotnoise accuracy. At the limit $\mu \to 0$, Alice measures perfectly Q' but not at all P', since the noise $\delta P'_A$ needs to be infinite in order to fulfill the Heisenberg inequality (9). This limit corresponds to the perfectly transmitting beamsplitter ($T = 1$), where nothing is reflected to the "P-measuring port". If $\mu > 1$, the situation is reversed, and Alice measures P' more accurately than Q'. At the limit $\mu \to \infty$, she only measures P', gaining no information on Q'.

Now, from the measured quadratures Q' and P', Alice can again estimate the correlated quadratures Q and P. Her best estimate of the state of the beam (Q, P) is given by (Q_A, P_A), which are now defined simultaneously:

$$Q_A = \frac{\langle Q\, Q'_A \rangle}{\langle {Q'_A}^2 \rangle} Q'_A = \frac{\sqrt{V^2-1}}{V+\mu}(Q' - \delta Q'_A) \qquad \text{and} \qquad P_A = -\frac{\sqrt{V^2-1}}{V+\frac{1}{\mu}}(P' - \delta P'_A). \tag{12}$$

Using

$$Q = Q_A + \delta Q_A \qquad \text{and} \qquad P = P_A + \delta P_A, \tag{13}$$

with δQ_A and δP_A defining the noise of the estimators, the conditional variances can be expressed as

$$\begin{aligned} V_{Q|Q_A} = \langle {\delta Q_A}^2 \rangle &= \langle Q^2 \rangle - \frac{\langle Q\, Q_A \rangle^2}{\langle {Q_A}^2 \rangle} = \left(V - \frac{(V^2-1)}{(V+\mu)} \right) N_0 \\ &= \frac{\mu V + 1}{V+\mu} N_0 \end{aligned} \tag{14a}$$

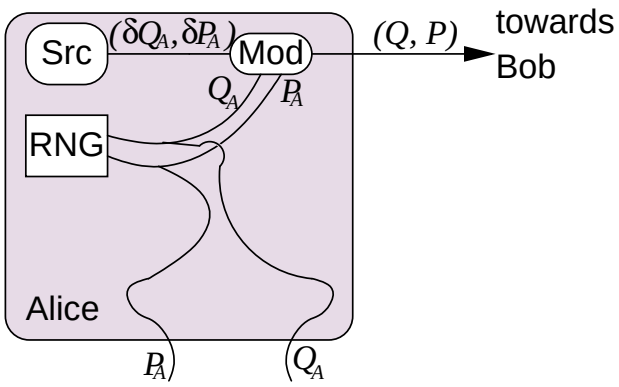

Fig. 3. **Equivalent black box.** The system sketched in Fig. 2 is equivalent to this black box. A random number generator (RNG) gives two values Q_A and P_A. A squeezed (or coherent if $s = 1$) state source (Src) generates the beam $(\delta Q_A, \delta P_A)$, wich is then displaced in phase space by (Q_A, P_A) using a modulator (Mod).

and

$$V_{P|P_A} = \langle \delta {P_A}^2 \rangle = \langle P^2 \rangle - \frac{\langle P\, P_A \rangle^2}{\langle {P_A}^2 \rangle} = \left(V - \frac{(V^2-1)}{(V + \frac{1}{\mu})} \right) N_0$$
$$= \frac{V + \mu}{\mu V + 1} N_0 = \frac{{N_0}^2}{V_{Q|Q_A}} \tag{14b}$$

Said otherwise, the measurement of Q' and P' projects the beam (Q, P) onto a squeezed state of variances $V_{Q|Q_A}$ and $V_{P|P_A}$. Then, it is clear that if the measurement is symmetric in Q' an P' (*i.e.* if $\mu = 1$), one has $V_{Q|Q_A} = V_{P|P_A} = N_0$ and the beam (Q, P) is projected onto a coherent state. The mean values of the quadratures of the beam (Q, P) are given by Q_A and P_A, so things happen as if Alice had prepared a randomly displaced squeezed (or coherent) state.

2.3 Virtual entanglement

Let us suppose the EPR source and the measuring apparatus of Alice are hidden in a black box. The only things coming out of this black box are the values of Q_A and P_A, and the beam (Q, P). This black box is indistinguishable from an equivalent black box, sketched in Fig. 3, where Q_A and P_A are chosen by the adequate random generator and the beam (Q, P) is in the displaced squeezed state centered around (Q_A, P_A). Its squeezing factor is

$$s = \frac{V_{Q|Q_A}}{N_0} = \frac{\mu V + 1}{V + \mu}, \tag{15}$$

and the equations (14) can be rewritten

$$V_{Q|Q_A} = \langle \delta {Q_A}^2 \rangle = s\, N_0 \qquad \text{and} \qquad V_{P|P_A} = \langle \delta {P_A}^2 \rangle = \frac{N_0}{s} \tag{16}$$

The black box with $\mu = 0$ and in the case Q and P are randomly interchanged allows therefore to prepare the randomly displaced squeezed states that are used in the QKD protocol

described in [6, 7]. If we fix μ to any given value, we realize all of the protocols presented in [3]. In particular, since $\mu = 1$ corresponds to the preparation of a coherent state ($s = 1$), the modulated coherent states QKD protocols used in [3, 4, 11] are equivalent to entanglement-based protocols even if they neither use squeezing nor entanglement. This possibility to prepare randomly displaced coherent states with an entanglement-based setup was implicitly present in our previous security studies of individual gaussian attacks on reverse reconciliation protocols [4, 11]. It is also useful to extend the Gottesman-Preskill proof of unconditional security of squeezed-state protocols [22] in an attempt to demonstrate the security of coherent-state protocols with respect to general attacks [23].

We call this possibility *virtual entanglement*: even if Alice does not actually use entanglement to create her coherent (or squeezed) states, there exists an equivalent setup (the black box described above) which uses entanglement to create them. This relies on the fact that the outputs of any physical apparatus, including Eve's eavesdropping system, can only depend on the density matrix of its input (in this case, the beam sent by Alice), and not on the way it was prepared. Cryptographic security is then related not to the transmission of "real" entanglement, but rather to the ability of the quantum channel to transmit entanglement, as we will show below.

3 Bounding Eve's attack on reverse reconciliation

3.1 Entangling cloner

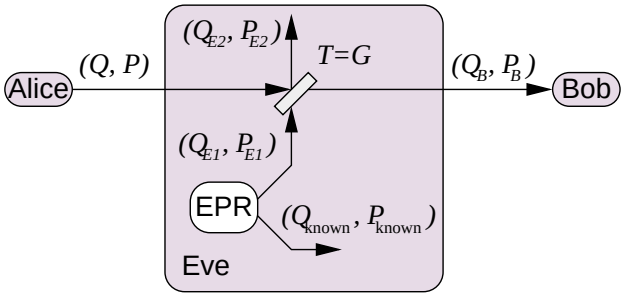

Fig. 4. **Eve's attack on reverse reconciliation.** To attack a reverse reconciliation QKD protocol, Eve uses an entangling cloner (EC). It takes Alice's beam (Q, P) as input and produces two entangled outputs, (Q_E, P_E), which is kept by Eve, and (Q_B, P_B), which is sent to Bob through a perfect line.

To eavesdrop a reverse reconciliation scheme, Eve needs to guess the results of Bob's measurement. We will call *entangling cloner* a system allowing her to do so, because this kind of system can be described as a cloner creating two entangled outputs, Eve keeping one of them and sending the other one to Bob (see Fig. 4). Here (Q, P) are the input quadratures of the entangling cloner and (Q_B, P_B), (Q_E, P_E) the quadratures of its two outputs. A good entangling cloner should minimize the conditional variances [20, 21] $V_{Q_B|Q_E}$ and $V_{P_B|P_E}$.

Alice and Bob should assume Eve uses the best possible entangling cloner, knowing the Alice-Bob channel quality. This channel can be described by

$$Q_B = \sqrt{G_Q}\,(Q + \delta Q_B) \qquad \text{and} \qquad P_B = \sqrt{G_P}\,(P + \delta P_B), \tag{17}$$

with

$$\left\langle \delta Q_B^2 \right\rangle = \chi_Q \, N_0, \qquad \left\langle \delta P_B^2 \right\rangle = \chi_P \, N_0 \qquad \text{and} \qquad \left\langle Q \, \delta Q_B \right\rangle = \left\langle P \, \delta P_B \right\rangle = 0 \tag{18}$$

3.2 Heisenberg inequalities on Alice's and Eve's conditional variances

For reverse reconciliation protocols, Alice needs to evaluate Q_B. Her estimator can be noted βQ_A, with $\beta = \frac{\langle Q_A \, Q_B \rangle}{\langle {Q_B}^2 \rangle} = \frac{V-s}{\sqrt{G_Q (V+\chi_Q)}}$. Eve's estimator for P_B will be P_E. The error of these estimators are

$$Q_{B|A} = Q_B - \beta Q_A \qquad \text{and} \qquad P_{B|E} = P_B - P_E. \tag{19}$$

The commutator of these two quantities is then equal to

$$[Q_{B|A}, P_{B|E}] = [Q_B, P_B] - \beta \underbrace{[Q_A, P_B]}_{0} - \underbrace{[Q_B, P_E]}_{0} + \beta \underbrace{[Q_A, P_E]}_{0}. \tag{20}$$

We have therefore $[Q_{B|A}, P_{B|E}] = [Q_B, P_B] = 2iN_0$. This commutation relation leads to the following inequality on conditional variances:

$$V_{Q_B|Q_A} V_{P_B|P_E} \geq N_0^2 \qquad \text{and} \qquad V_{P_B|P_A} V_{Q_B|Q_E} \geq N_0^2, \tag{21}$$

the second inequality being obtained by exchanging the roles of Q and P. These inequalities mean that Alice and Eve cannot jointly know more about Bob's field than allowed by the Heisenberg principle.

3.3 Alice's conditional variance

Alice's conditional variance on Q_B is

$$\begin{aligned} V_{Q_B|Q_A} &= \left\langle Q_B^2 \right\rangle - \frac{\langle Q_A \, Q_B \rangle^2}{\langle Q_A^2 \rangle} = G_Q V N_0 + G_Q \chi_Q N_0 - G_Q V N_0 + G_Q s N_0 \\ &= G_Q (\chi_Q + s) N_0 \end{aligned} \tag{22}$$

A similar calculation leads to the symmetric relation

$$V_{P_B|P_A} = G_P (\chi_P + \tfrac{1}{s}) N_0. \tag{23}$$

These conditional variances depend on the amount of squeezing s Alice generates with her black-box. Therefore, the constraint on squeezing $\frac{1}{V} < s < V$ gives us the minimal values of these conditional variances

$$V_{P_B|P_A} \geq V_{P_B|P_A,\min} = G_P (\chi_P + \tfrac{1}{V}) N_0 \tag{24}$$

$$V_{Q_B|Q_A} \geq V_{Q_B|Q_A,\min} = G_Q (\chi_Q + \tfrac{1}{V}) N_0 \tag{25}$$

3.4 Eve's conditional variance

The output-output correlations of an entangling cloner, described e.g. by $V_{P_B|P_E}$, should only depend on the density matrix of the field (Q, P) at its input, and not on the way this field was built. The inequality (21) has thus to be fulfilled for every physically allowed value of $V_{Q_B|Q_A}$, given the density matrix of the field (Q, P). Since this field is gaussian, its density matrix is

uniquely defined by its covariance matrix, *i.e.* by the parameters $\langle Q^2 \rangle = \langle P^2 \rangle = V N_0$ and $\langle Q\ P \rangle = 0$, and we have to consider all possible black-boxes (those of Fig. 2 as well as those of Fig. 3). In order to bound Eve's knowledge by using Eq.(21), we thus have to use the tightest limit on $V_{Q_B|Q_A}$, which is given by $V_{Q_B|Q_A,\min}$ according to (25). Obviously the same reasoning holds for $V_{P_B|P_A}$, with the corresponding tightest limit $V_{P_B|P_A,\min}$.

We have then

$$V_{Q_B|Q_E} \geq V_{Q_B|Q_E,\min} = \frac{N_0}{G_P(\chi_P + 1/V)} \tag{26}$$

and, similarly

$$V_{P_B|P_E} \geq V_{P_B|P_E,\min} = \frac{N_0}{G_Q(\chi_Q + 1/V)} \tag{27}$$

If one of these inequalities was violated and if Alice had prepared her field with an EPR-beams based black-box, then Eve and Alice would be able to make a joint measurement of Bob's field with a better accuracy than allowed by the Heisenberg uncertainty limit.

3.5 Implementation of the entangling cloner

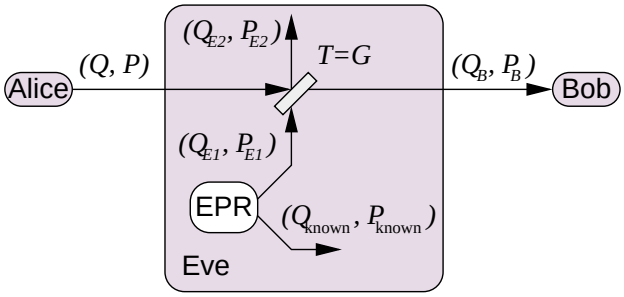

Fig. 5. **Implementation of an entangling cloner** for $G < 1$. Eve uses a beamsplitter of transmission $T = G$ to inject into the line a partially known noise (Q_{E1}, P_{E1}) generated with an EPR source (EPR). She keeps the other output (Q_{E2}, P_{E2}) of the beamsplitter which, combined with her knowledge $(Q_{\text{known}}, P_{\text{known}})$ on the injected noise, gives her an estimate of Bob's beam (Q_B, P_B).

In a practical QKD scheme, Alice and Bob will give the same roles to Q and P. Assuming therefore that $G_Q = G_P = G$ and $\chi_Q = \chi_P = \chi$, the two bounds above reduce to a single one, and it is possible to explicitly describe an entangling cloner achieving this limit. We will consider here only the case where $G < 1$, but the limit is tight for any G. The entangling cloner can then be sketched as shown in Fig 5: Eve uses a beamsplitter with a transmission G to split up part of the Alice-Bob transmitted signal, and she injects into the other input port a field $E1$, with the right variance to induce a noise of variance $G\chi N_0$ at Bob's end. One has therefore:

$$\langle Q_{E1}^2 \rangle = \frac{G\chi N_0}{1-G} \qquad \langle P_{E1}^2 \rangle = \frac{G\chi N_0}{1-G} \tag{28}$$

Eve should know the maximum about this injected field $E1$, and will therefore use an half-pair of EPR-correlated beams, so that she does perform an "entangling" attack. We can then write

$$Q_{E1} = Q_{\text{known}} + Q_{\text{unknown}} \tag{29}$$

where Q_{known} stand for Eve's best estimation of Q_{E1}, given by the measure of its brother-beam, and Q_{unknown} stand for the noise she cannot know. We have

$$\left\langle Q^2_{\text{unknown}} \right\rangle = \frac{N_0^2}{\left\langle Q^2_{E1} \right\rangle} = \frac{(1-G)N_0}{G\chi} \tag{30}$$

$$\left\langle Q^2_{\text{known}} \right\rangle = \left\langle Q^2_{E1} \right\rangle - \left\langle Q^2_{\text{unknown}} \right\rangle \tag{31}$$

Eve also use an output port of the beamsplitter to measure the field $E2$, which gives her information about the input field:

$$Q_{E2} = \sqrt{G}\, Q_{E1} - \sqrt{1-G}\, Q. \tag{32}$$

She can cancel a part of the noise induced by $E1$ by subtracting the part proportional to Q_{known}. Thus she knows

$$Q'_{E2} = \sqrt{G}\, Q_{\text{unknown}} - \sqrt{1-G}\, Q. \tag{33}$$

We also have

$$Q_B = \sqrt{G}\, Q + \sqrt{1-G}\, Q_{E1}. \tag{34}$$

where Eve already knows the part proportional to Q_{known}, injected with Q_{E1} and she only needs to guess

$$Q'_B = \sqrt{G}\, Q + \sqrt{1-G} Q_{\text{unknown}} \tag{35}$$

from Q'_{E2}. We have therefore

$$V_{Q_B|Q_{E1},Q_{E2}} = V_{Q'_B|Q'_{E2}}. \tag{36}$$

The calculation of the quantities $\left\langle Q'^2_B \right\rangle$, $\left\langle Q'^2_{E2} \right\rangle$, $\left\langle Q'_{E2} Q'_B \right\rangle$ leads straightforwardly to the conditional variance

$$V_{Q'_B|Q'_{E2}} = \frac{N_0}{G\chi + G/V} = V_{Q_B|Q_E,\min} \tag{37}$$

showing that the entangling cloner does reach the lower limit of Eqs. (26) and (27).

4 Security of reverse-reconciliation based quantum cryptography

4.1 Tolerable noise

In a reverse reconciliation protocol, Eve's power is limited by the values of $V_{Q_B|Q_E,\min}$ and $V_{P_B|P_E,\min}$ given by Eqs. (26) and (27). In a security analysis, we have to assume that a "perfect" Eve is able to reach this limit, that is,

$$V_{Q_B|Q_E} = V_{Q_B|Q_E,\min} = \frac{N_0}{G_P(\chi_P + 1/V)} \tag{38a}$$

$$V_{P_B|P_E} = V_{P_B|P_E,\min} = \frac{N_0}{G_Q(\chi_Q + 1/V)} \tag{38b}$$

On Alice's side, the relevant conditional variances are given by Eqs. (22) and (23). Alice's and Eve's conditional variances can be converted into mutual informations by using Shannon's formula[24]. For the quadrature Q, we have

$$I_{BA}^{Q} = \frac{1}{2}\log_2 \frac{\langle Q_B^2 \rangle}{V_{Q_B|Q_A}} \qquad I_{BE}^{Q} = \frac{1}{2}\log_2 \frac{\langle Q_B^2 \rangle}{V_{Q_B|Q_E}} \tag{39}$$

while, for the quadrature P, we have

$$I_{BA}^{P} = \frac{1}{2}\log_2 \frac{\langle P_B^2 \rangle}{V_{P_B|P_A}} \qquad I_{BE}^{P} = \frac{1}{2}\log_2 \frac{\langle P_B^2 \rangle}{V_{P_B|P_E}} \tag{40}$$

Following [18, 19], we know that a sufficient condition for reverse reconciliation to give a non-zero secret key rate is $I_{BA}^{Q} > I_{BE}^{Q}$ (for the Q quadrature) or $I_{BA}^{P} > I_{BE}^{P}$ (for the P quadrature). In terms of conditional variances, this translates into

$$V_{Q_B|Q_E} > V_{Q_B|Q_A} \qquad \text{or} \qquad V_{P_B|P_E} > V_{P_B|P_A} \tag{41}$$

Using Eqs. (22), (23) and (38), we obtain (sufficient) conditions for the security of a reverse-reconciliation based protocol

$$(G_Q\chi_Q + G_Q s)(G_P\chi_P + \frac{G_P}{V}) < 1 \qquad \text{or} \qquad (G_P\chi_P + G_P s)(G_Q\chi_Q + \frac{G_Q}{V}) < 1. \tag{42}$$

For simplicity reasons, we will assume in the following that all equations are symmetric in Q and P, in particular $G_Q = G_P = G$ and $\chi_Q = \chi_P = \chi$,[a] so that these conditions simplify into:

$$(G\chi + Gs)(G\chi + G/V) < 1. \tag{43}$$

This condition can be rewritten by using the definition $\chi = \chi_0 + \varepsilon$, where $\chi_0 = \frac{1-G}{G}$ is the loss-induced "vacuum noise" and ε is the excess noise[b], giving

$$[1 - G(1 - s - \varepsilon)][1 - G(1 - \tfrac{1}{V} - \varepsilon)] < 1. \tag{44}$$

Since $s \leq 1$ and $V > 1$, this condition is always fulfilled for $\varepsilon = 0$, *i.e.* when the noise only originates from losses. This holds for arbitrary high losses ($G \to 0$) and even for coherent state protocols ($s = 1$). Therefore, reverse reconciliation provides a simple way to extend the coherent state protocol of ref. [3] into the high-loss regime.

Finally, one can show that squeezed state protocols are more robust against excess noise than coherent state protocols. Indeed, by solving Eq. (44), we get

$$\varepsilon < \varepsilon_{\max} \qquad \text{with} \qquad \varepsilon_{\max} = 1 - \tfrac{1}{V} \underbrace{-\tfrac{1}{G} - \tfrac{1}{2}(s - \tfrac{1}{V}) + \sqrt{\tfrac{1}{G^2} + \tfrac{1}{4}(s - \tfrac{1}{V})^2}}_{\leq 0} < 1 \tag{45}$$

It is easy to check that this upper limit on ε is less stringent for low values of s, *i.e.* for strong squeezing. When the squeezing is maximum ($s = \frac{1}{V}$), we get $\varepsilon_{\max} = 1 - \frac{1}{V}$. Note also that, in the limit of high losses ($G \to 0$), we have $\varepsilon_{\max} = 1 - \frac{1}{2}(s + \frac{1}{V})$. The maximum tolerable excess noise is shown in Fig. 6 as a function of the losses in the limiting case of high modulation ($V \to \infty$).

[a] Any experimental implementation of this protocol should however estimate these parameters from statistical tests, which are likely not to be exactly symmetric.

[b] Strictly speaking, ε corresponds to the excess noise only in the usual case of losses, where $G \leq 1$.

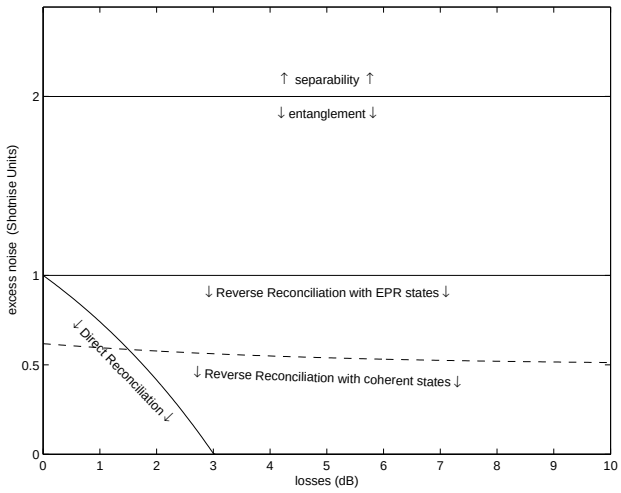

Fig. 6. **Tolerable excess noise ε as a function of the losses** at the high modulation limit ($V \gg 1$). The RR limit is given by Eq. (45). It reduces to $\varepsilon_{\max}^{\mathrm{EPR}} = 1$ for EPR states (or maximal squeezing) at the high modulation limit ($s = \frac{1}{V} \to 0$), and to Eq. (51) for coherent states (dashed line). The DR security limit defined in Eq. (60) implies that DR is more robust against excess noise than coherent state RR in the low losses regime. The entanglement limit given by Eq. (59), *i.e.* $\varepsilon = 2$, is well above the previous security limits. In the region $1 < \varepsilon < 2$, no QCV cryptographic protocol is known, although entanglement is present.

4.2 Secret information rates (EPR vs coherent beams)

The condition (43) can directly be translated into a secret information rate by using Shannon's formula (in the case where everything is symmetric in Q and P) [24]

$$I_{BA} = \tfrac{1}{2}\log_2 \frac{\langle Q_B^2 \rangle}{V_{B|A}} \qquad I_{BE} = \tfrac{1}{2}\log_2 \frac{\langle Q_B^2 \rangle}{V_{B|E}} \tag{46}$$

$$= \tfrac{1}{2}\log_2 \frac{V+\chi}{s+\chi} \qquad = \tfrac{1}{2}\log_2[(GV+G\chi)(G\chi+G\tfrac{1}{V})] \tag{47}$$

The RR secret information rate is therefore

$$\Delta I = I_{BA} - I_{BE} = \tfrac{1}{2}\log_2 \frac{V_{B|E}}{V_{B|A}} = \tfrac{1}{2}\log_2 \frac{1}{\left(G\chi + G\frac{1}{V}\right)(G\chi + Gs)} \tag{48}$$

and it is strictly positive if the security condition (43) is fulfilled.

Let us compare the cases where Alice uses EPR or coherent beams. If Alice measures only one quadrature of an EPR beam (or modulates a maximally squeezed beam compatible with the total variance V), we have $s = 1/V$ and $\varepsilon_{\max}^{\mathrm{EPR}} = 1 - \frac{1}{V}$. Alice and Bob gain shared information only every second transmission since they don't always choose the same

measurement basis[c]. Therefore,

$$\Delta I_{\mathrm{EPR}} = \frac{1}{4}\log_2 \frac{1}{\left(G\chi + G\frac{1}{V}\right)^2} = \frac{1}{2}\log_2 \frac{1}{G\chi + G\frac{1}{V}} \tag{49}$$

$$= \frac{1}{2}\log_2 \frac{1}{1 - G\left(1 - \frac{1}{V} - \varepsilon\right)} \tag{50}$$

In contrast, for coherent beams, we have $s = 1$ and

$$\varepsilon_{\max}^{\mathrm{coh}} = \tfrac{1}{2} - \tfrac{1}{2V} - \tfrac{1}{G} + \sqrt{\tfrac{1}{G^2} + \tfrac{1}{4}(1 - \tfrac{1}{V})^2}. \tag{51}$$

The mutual informations are not dependent of the basis choice (we do not get this prefactor $1/2$), so we have

$$\Delta I_{\mathrm{coh}} = \frac{1}{2}\log_2 \frac{1}{\left(G\chi + G\frac{1}{V}\right)(G\chi + G)} \tag{52}$$

$$= \Delta I_{\mathrm{EPR}} - \frac{1}{2}\log_2(1 + G\varepsilon) \tag{53}$$

Since the excess noise ε is positive, we obtain

$$\Delta I_{\mathrm{coh}} \leq \Delta I_{\mathrm{EPR}}. \tag{54}$$

Both secret rates become equal if and only if the noise only comes from losses ($\varepsilon = 0$ and $G \leq 1$). Therefore, the use of entanglement or squeezing does not improve the secret rate for losses only, and it becomes advantageous only in the presence of excess noise.

4.3 Strong losses limit

Assuming strong losses ($G \ll 1$), Eqs. (50) and (53) tend to

$$\Delta I_{\mathrm{EPR}} \simeq \frac{G}{2\ln 2}\left(1 - \tfrac{1}{V} - \varepsilon\right) \qquad \Delta I_{\mathrm{coh}} \simeq \frac{G}{2\ln 2}\left(1 - \tfrac{1}{V} - 2\varepsilon\right) \tag{55}$$

In the case where there is no excess noise ($\varepsilon = 0$), both rates are equal, as we just said, and we get $\Delta I_{\mathrm{EPR,losses}} = \Delta I_{\mathrm{coh,losses}}$. If there is some excess noise in the line, one sees that the reverse reconciliation protocol is secure as long as as $\varepsilon < \frac{1}{2}(1 - \frac{1}{V}) \sim 1/2$ for coherent states, and $\varepsilon < 1 - \frac{1}{V} \sim 1$ for EPR beams. This shows again that it is always possible to use coherent states regardless the line losses, though EPR beams make the scheme more robust against excess noise.

Now, we may compare the secret key rate of the RR coherent-state protocol with BB84's net key rate in the case of a lossy errorless channel, which is $\frac{1}{2}G\bar{n}$ with $\bar{n} = 1$ for single photons and $\bar{n} \ll 1$ for weak coherent pulses. Taking for instance a 100 km line with 20 dB loss ($G = 0.01$) and a reasonable modulation ($V \simeq 10$), the secret key rate is $\Delta I = 6.5 \cdot 10^{-3}$ bit/symbol for a RR coherent-state protocol. For the same parameters, the secret key rate for BB84 with an ideal single-photon source would be at best $5 \cdot 10^{-3}$ bit/time slot, and one order of magnitude smaller using attenuated light pulses with $\bar{n} = 0.1$, even with perfect detectors

[c] We suppose that Alice and Bob do not have a quantum memory available.

(this corresponds to a very recent experimental realization of BB84 [25]). Thus, our reversed-reconciliation QCV protocol has, in principle, a comparable efficiency to that of ideal BB84 (for strong losses and no excess noise). In particular, with a "symbol rate" of a few MHz, which should be easy to achieve, the theoretical QCV secret key rate after 100 km would be more than 10 kbits/sec.

We must stress, however, that in order to achieve this rate, better reconciliation protocols than those available today should be developed. In their current state, the reconciliation procedures cannot extract a single secret bit in such a high-loss regime (the highest loss that can be tolerated in the first experimental demonstration of QCV quantum cryptography is about 3.1 dB [4]). Indeed, for the values of the parameters above, the information between Alice and Bob is $I_{AB} = 6.2 \cdot 10^{-2}$ bit/symbol, which is one order of magnitude larger than ΔI. Hence, the required reconciliation efficiency should be larger than 90 percent in a regime where the information content (I_{AB}) is of a few hundredth of bit per symbol (or, in other words, when the signal-to-noise ratio does not exceed about -10 dB).

5 Entanglement versus security criteria

5.1 Virtual entanglement criterion

If the channel between Alice and Bob is too noisy, the *virtual entanglement* between (Q_B, P_B) and (Q', P') will be destroyed. The threshold at which this happens can be calculated using the Duan–Simon entanglement criterion for bivariate gaussian states[26, 27]. This criterion, expressed by the equation (17) of [26], is

$$(V-1)(V_B-1) < C^2, \tag{56}$$

where

$$V_B\, N_0 = \langle {Q_B}^2 \rangle = \langle {P_B}^2 \rangle = G(V+\chi)\, N_0 \tag{57}$$

$$C\, N_0 = \langle Q'\, Q_B \rangle = -\langle P'\, P_B \rangle = \sqrt{G(V^2-1)}\, N_0 \tag{58}$$

In our case, this leads to

$$G(V-1)(V-1+\varepsilon) < G(V-1)(V+1) \qquad \Leftrightarrow \qquad \varepsilon < 2 \tag{59}$$

Therefore, virtual entanglement is present as soon as there is non-zero modulation ($V > 1$) and non-zero transmission ($G > 0$), provided that the excess noise of the channel is smaller than twice the shot-noise limit.

5.2 Security criteria

The security limit against gaussian individual attacks of the QKD protocols discussed in [3, 4, 6, 7, 11] are simply obtained by comparing conditional variances. For direct protocols [3], an argument linked to cloning leads to the limit [3, 6, 7]

$$\chi < 1 \qquad \Leftrightarrow \qquad \varepsilon < 2 - \frac{1}{G}, \tag{60}$$

which ensures that the inequality (59) is fulfilled. For reverse protocols, the inequality (45) cannot be fulfilled if $\varepsilon > 1$ so that the entanglement condition $\varepsilon < 2$ is also always fulfilled

when reverse reconciliation is possible. This situation is summarized in Fig. 6, where the entanglement limit is compared with the DR and RR security limits. The figure makes clear that the DR and RR cryptographic security thresholds lie well within the entanglement region, where the channel is able to distribute quantum entanglement. This holds even if no entangled beams are physically implemented.

It is worth noting that the entanglement threshold is known to coincide, physically, with an intercept-and-resend attack [28]. In other words, at the point where the joint state of Alice and Bob becomes separable ($\varepsilon = 2$), there exists an explicit intercept-and-resend attack, so that obviously no protocol can be secure. The gap between the entanglement condition (59) and the security limits (60) and (44) corresponds to a region where the known DR and RR protocols are insecure with respect to gaussian attacks, though intercept-and-resend attacks cannot be used yet. It is presently unknown whether improved protocols may be devised, that would remain secure against gaussian attacks in this region.

6 Conclusion

In this paper we have shown that reverse reconciliation protocols can be used to extract a secret key from the exchange of coherent, squeezed or EPR beams between Alice and Bob. The key is secure against individual gaussian attacks regardless the transmission of the optical line between Alice and Bob, provided that the excess noise (*i.e.* the noise beyond the loss-induced vacuum noise) is not too large. Squeezing or entanglement allow these protocols to tolerate a larger amount of excess noise, but they are not absolutely required. We have also shown that the QCV protocols based on gaussian displaced squeezed or coherent states [3, 4, 6, 7, 11] are equivalent to entangled-beams based protocols, and that the security limits of these protocols are more severe than the entanglement limit of the equivalent entanglement-based protocol. This result is certainly compatible with—and even supports—the idea that they may be unconditionally secure [23].

The difference between the entanglement condition and the security limits in RR or DR shows that our protocols do not use the full available entanglement. In principle, procedures based either on quantum entanglement distillation [12, 22] or on classical advantage distillation [29] can exploit the entanglement up to its ultimate limit. However, it should be noticed that such protocols are either much more difficult to implement (quantum entanglement distillation) than the ones we have considered here, or have extremely low practical secret bit rates (classical advantage distillation).

Clearly, several questions remain open. First, one should determine whether the gap between our security threshold and the entanglement threshold is due to the restricted observables we can measure through homodyne detection, or to the reconciliation procedure used to extract the bits, or perhaps to another factor. Second, though individual gaussian attacks are clearly well suited to the encoding scheme that we are using, it remains to be shown either that these attacks are indeed optimal, or that the protocol is secure against any type of attacks (including non-gaussian collective attacks [22]). Work along these lines is in progress [30].

Acknowledgments

FG acknowledges support from the Belgian National Fund for Scientific Research. NJC

acknowledges financial support from the Communauté Française de Belgique under grant ARC 00/05-251, from the IUAP programme of the Belgian governement under grant V-18, and from the EU under project RESQ (IST-2001-35759). This work has been partly funded by the IST / FET / QIPC project "QUICOV".

References

1. S.L. Braunstein and A.K. Pati, *Quantum Information Theory with Continuous Variables*, (Kluwer Academic, Dordrecht, 2003).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
3. F. Grosshans and Ph. Grangier, Phys. Rev. Lett. **88** 057902 (2002); see also e-print quant-ph/0109084.
4. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf and Ph. Grangier, Nature **421**, 238 (2003).
5. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
6. N.J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001); see also e-print quant-ph/0008058.
7. N.J. Cerf, S. Iblisdir and G. Van Assche, Eur. Phys. J. D **18**, 211 (2002); see also e-print quant-ph/0107077.
8. N.J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000); see also e-print quant-ph/9909037.
9. N.J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000); see also e-print quant-ph/0005044.
10. F. Grosshans and Ph. Grangier, Phys. Rev. A **64** 010301(R) (2001); see also e-print quant-ph/0012121.
11. F. Grosshans and Ph. Grangier, Proc. 6^{th} Int. Conf. on Quantum Communications, Measurement, and Computing (QCMC'02), Rinton Press, December 2002; see also e-print quant-ph/0204127
12. L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000).
13. Ch. Silberhorn, T. C. Ralph, N. Luetkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
14. C. Bennett and G. Brassard, Proc. of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New-York, 1984), p. 175
15. A.K. Ekert, Phys. Rev. Let. **67**, 661 (1991).
16. C.H. Bennett, G. Brassard and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
17. G. Van Assche, J. Cardinal and N.J. Cerf, e-print cs.CR/0107030, to appear in IEEE Trans. Inf. Theory (2003)
18. I. Csiszar and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
19. U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
20. J.-Ph. Poizat, J.-F. Roch and Ph. Grangier, Ann. Phys. (Paris), **19**, 265 (1994).
21. Ph. Grangier, J.-A. Levenson and J.-Ph. Poizat, Nature **396**, 537 (1998).
22. D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001); see also e-print quant-ph/0008046.
23. S. Iblisdir, G. Van Assche, and N. J. Cerf, article in preparation.
24. C.E. Shannon, Bell Syst. Tech. J. **27** 623-656(1948).
25. H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, e-print quant-ph/0306066.
26. L.-M. Duan, G. Giedke, J. I. Cirac and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
27. R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
28. M. Horodecki, P. W. Shor, and M. B. Ruskai, to appear in Rev. Math. Phys.; see also quant-ph/0302031.
29. N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999); see also quant-ph/9902048.
30. Sofyan Iblisdir, PhD thesis, Université Libre de Bruxelles, 2003.