From quantum cloning to quantum key distribution with continuous variables: a review (Invited)

Nicolas J. Cerf

QuIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium

Philippe Grangier*

Laboratoire Charles Fabry de l'Institut d'Optique, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France

Received October 4, 2006; revised October 17, 2006; accepted October 17, 2006;
posted October 19, 2006 (Doc. ID 75781); published January 26, 2007

Quantum information processing with continuous variables is a paradigm that has attracted a growing interest over the past years, partly as a consequence of the prospects for high-rate quantum communication systems based on standard optical telecommunication components. In this overview article, we introduce the concept of quantum continuous variables in optics and then turn to the fundamental impossibility of cloning continuous-variable light states, a result that lies at the heart of quantum key distribution. Then we present state-of-the-art quantum key distribution systems relying on continuous variables, focusing mainly on the protocols using Gaussian-modulated coherent light states and emphasizing the current experimental demonstration of these systems. Finally, we briefly review recent security proofs of these cryptographic protocols.

OCIS codes: 270.5570, 060.1660, 060.2920.

1. INTRODUCTION

Over the past years, there has been an increasing interest about the possibility of realizing quantum informational and computational tasks with so-called continuous variables (CVs).[1,2] The leading idea of this approach is to use, as quantum information carriers, physical quantities that have a continuous spectrum, such as the quadrature amplitudes of the quantized light field, instead of binary quantities, such as the polarization state of a single photon. As is well known, the central concepts of quantum information theory such as quantum teleportation, quantum cryptography, or quantum algorithms have initially been developed for binary quantum carriers (quantum bits or qubits). This is indeed the most natural way to go in order to build the quantum counterpart to classical informational processes. However, the use of CV quantum systems, which may involve many photons in one light mode, has some potential advantages over single-photon quantum systems. Such advantages lie in the prospect for higher optical data rates and simpler processing tools, based upon standard telecommunication techniques. More specifically, one defines a CV quantum communication system as a setup whose (main) measurement system is based on homodyne detection instead of single-photon detection. Using homodyne instead of single-photon detection comes with the advantage of producing a measurement outcome for each pulse; that is, CV protocols are, by essence, unconditional. In contrast, single-photon detectors typically have low efficiencies, resulting in a low probability of success. Another significant strength of the CV paradigm is that light–atoms quantum interfaces have been successfully designed and realized for CV, so that atomic systems can be used as a support for CV quantum information.

To illustrate the dramatic development of the field of CV quantum information processing, let us mention just some of the main recent achievements in this direction. On the experimental side, an important trigger was the successful demonstration of CV quantum teleportation.[3] It was then possible to demonstrate the entanglement of two atomic ensembles[4] and to realize a quantum memory for light.[5] Other implemented protocols include quantum erasing,[6] quantum cloning,[7] and the demonstration of CV coherent-state quantum key distribution[8] (QKD), which is the main topic of the present paper. Many groups have also been involved in theoretical developments, for example, about the characterization of CV entanglement,[9,10] CV entanglement purification with non-Gaussian operations,[11] bound entanglement with Gaussian states,[12,13] and, of direct interest for the present paper, CV quantum cloning[14] as well as QKD.[15,16]

2. OPTICAL QUANTUM CONTINUOUS VARIABLES

Let us consider the CV that naturally appear when one describes a light field. In classical electromagnetism, a light field can be written as an oscillatory function $x\cos(\omega t)+p\sin(\omega t)$, where ω is the angular frequency while x and p are the quadrature components of the field. If $\cos(\omega t)$ is viewed as a reference field, generally called the local oscillator (LO), then x is the amplitude of the

component of the field that is in phase with the LO, while p is the amplitude of the component that is in quadrature with the LO. Clearly, x and p make a pair of CV that completely characterize a single-mode optical field. When the quantum properties of light play a role, we have to turn to quantum optics, and the quadrature components x and p become noncommuting (yet continuous) observables associated with a quantum harmonic oscillator. One has then

$$[x,p] = 2i, \tag{1}$$

where the normalization is chosen so that the variance of the vacuum is unity. Hence, as a result of the Heisenberg uncertainty principle $\Delta x \Delta p \geqslant 1$, x and p cannot be known simultaneously, in contrast to the situation that prevails in classical optics: any measurement of x deletes the information on p and conversely. In some sense, the two quadrature components of light behave like the usual position–momentum pair in quantum mechanics, hence the notation. This suggests that we can build a whole set of quantum informational processes where the quadrature pair (x,p) carries some continuous information (i.e., real-valued data).

Although CV quantum information is conceptually less natural than the standard quantum information paradigm where a binary variable (a bit) is encoded into a dichotomic degree of freedom of a single photon (a qubit), it comes with several advantages: (i) it is sufficient to process simple nonclassical states of the light, known as single-mode squeezed states, into linear-optics circuits to perform a large variety of CV multipartite informational processes (although more sophisticated ingredients such as cat states are needed[17] for the implementation of universal CV quantum computing); (ii) the Bell measurement, a cornerstone of quantum information processing, can be realized deterministically with a balanced beam splitter followed by homodyne measurement; (iii) the measurement technique, namely, homodyne detection, may work at a high rate. By comparison, quantum-bit-based quantum information processes using photons suffer the following problems: (i) multipartite quantum circuits require two-body interaction between quantum bits, which either requires often unrealistic nonlinear optical effects, or can be achieved via linear-optics quantum computing techniques[18] but at the price of a strong postselection; (ii) the Bell measurement achieved with a beam splitter is fundamentally restricted to a probabilistic measurement (it succeeds with a probability of 50% at most); (iii) the measurement technique is based on avalanche photodiodes, which are comparatively slower and less efficient than homodyne detection.

3. CONTINUOUS-VARIABLE QUANTUM CLONING

Consider for a moment the case of qubits. As is well known, the duality between the computational basis $\{|0\rangle, |1\rangle\}$ and the dual basis $\{(|0\rangle+|1\rangle)/\sqrt{2}, 1/\sqrt{2}(|0\rangle-|1\rangle)/\sqrt{2}\}$ prohibits the simultaneous determination of the value of a state in both bases. This duality is at the heart of the quantum no-cloning theorem: it is impossible to duplicate perfectly the state of a quantum bit. Coming back to the case of CV, one notes that the canonical variables (x,p) are linked by a Fourier transform, just as the Hadamard transform maps the computational basis to the dual basis for qubits. The quantum no-cloning theorem then implies that it is not possible to clone position states $|x\rangle$ and momentum states $|p\rangle$ by the same process. By measuring x and preparing clones as x-localized states, one would make a perfect $|x\rangle$-states cloner, but this cloner would then fail at cloning p-localized states. Obviously, the converse holds, too, so we must turn to approximate cloning machines, which achieve the best possible imperfect copying of the state that is compatible with quantum mechanics.

A natural candidate for the optimal CV cloning machine is a transformation that adds the same noise to both quadrature components. By exploiting the connection between measurement and cloning theory, one can obtain a tight bound on this cloner from the well-known fact that the best joint measurement of x and p for a coherent state suffers from extra noise whose variance is equal to twice the shot-noise unit.[19] Intuitively, one of these units may be associated with the splitting process required for measuring both x and p, whereas the other unit is coming from the measurement process itself. Cloning the state and then measuring x on one clone and p on the other clone cannot beat this optimal measurement, which makes it understandable that the cloning process comes itself with a price of one shot-noise unit.

Actually, it is possible to build a Gaussian cloning machine that exactly saturates this bound.[14] The quantum circuit of this cloner consists of four CV controlled-NOT gates preceded by a preparation stage [see Fig. 1(a)]. The two auxiliary input modes need to be initially prepared in the vacuum state, and each contributes half a shot-noise unit to the cloning noise. As a result, this cloner adds a Gaussian-distributed noise to both quadrature components x and p with a variance of one shot-noise unit, which implies that the cloning fidelity is equal to 2/3 for all coherent states. It may be realized using a phase-insensitive amplifier of gain 2 followed by a balanced beam splitter[20,21] [see Fig. 1(b)]. A variant of this setup

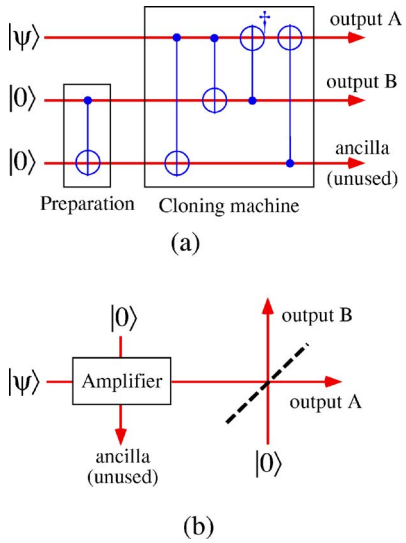

Fig. 1. (Color online) Quantum cloning for CV: (a) quantum circuit model and (b) a simple implementation using a phase-insensitive optical amplifier followed by a beam splitter.

has been experimentally implemented recently.[7] Interestingly, the physical origin of the cloning noise becomes much more evident in the case of CV than with quantum bits: it is indeed clear from Fig. 1 that the noise affecting the clones can be traced back to (half of) the vacuum fluctuations that unavoidably enter via the two auxiliary modes of the cloner.

4. CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

A. From Squeezed to Coherent States

The investigation of quantum cloning is of a particular significance given the strong connection between quantum cloning and quantum key distribution. Indeed, it is the impossibility of realizing a perfect cloning transformation that makes it possible to detect any potential eavesdropper in a quantum cryptographic scheme. More specifically, the use of an optimal quantum cloner generally makes it possible to derive a tight upper bound on the information acquired by the potential eavesdropper. This connection provides a strong incentive to devise QKD schemes that are linked to the quantum cloner of Fig. 1 and thus are specifically designed for CVs.

Let us show how to exploit this impossibility to perfectly clone the x and p states by turning it into a problem for the eavesdropper (Eve). The first proposal for CV-QKD relying on a continuous modulation of key carriers together with homodyne detection was made in Ref. 15 and independently in Ref. 22 (this latter protocol was demonstrated to be unconditionally secure). This protocol, which can be viewed as the direct continuous analogue of BB84, requires squeezed states of light (in Ref. 23 an earlier BB84-like protocol using homodyne detection had been proposed, but it remained intrinsically binary). In the protocol of Ref. 15 the sender (Alice) chooses to encode a Gaussian value into the x displacement of an x-squeezed state or similarly for the p quadrature. The squeezing parameter and the modulation variance are chosen in such a way that these two mixtures are indistinguishable and correspond to a thermal state. Then the receiver (Bob) measures one of the two quadratures by homodyne detection and publicly discloses whether x or p was measured. If the encoded and measured quadratures coincide, then Alice and Bob know that they share correlated Gaussian data, from which they can distill a secret key by using appropriate techniques (otherwise they simply discard their data). This protocol was shown to be secure against Gaussian individual attacks (defined in Subsection 4.C), provided that the squeezing parameter is nonzero. However, it has not been implemented as such because the need for squeezed states makes it rather impractical. Several other groups have proposed CV-QKD schemes based on Einstein–Podolsky–Rosen-like correlations.[24–27] Although some preliminary implementations have been carried out,[28,29] this approach is presently not mature enough for practical QKD purposes.

Important progress was made in Ref. 16 in which a coherent-state CV-QKD protocol was proposed, building upon the above squeezed-state protocol. The breakthrough here was to explicitly establish a secure protocol using states of light that can be easily generated with a laser. In this protocol, Alice modulates both x and p quadratures of a coherent state with a bivariate Gaussian distribution. Thus, she sends the same thermal state as before, but it is now realized as a mixture of coherent states. Bob again measures one of the two quadratures and publicly discloses which one, so that the corresponding quadrature is kept by Alice to make a correlated pair (the other quadrature is simply ignored). The security of the protocol against individual Gaussian attacks (defined in Subsection 4.C) was proven by using the concept of equivalent noise referred to the input,[8] which is common in electronics and has been used previously in the context of quantum nondemolition measurements in optics. The security criterion is then simple: the equivalent noise variance N of the transmission line, evaluated at the line input, cannot be larger than one shot-noise unit:

$$N < 1. \tag{2}$$

This condition is actually equivalent to the limit on CV quantum cloning; that is, the best attack (if the channel is lossless) is simply the optimal Gaussian cloning machine that is depicted in Fig. 1.

An important observation is that the equivalent noise variance can be split into two different contributions:

$$N = \frac{1-T}{T} + \epsilon, \tag{3}$$

where $(1-T)/T$ corresponds to the vacuum noise (referred to the input) due to the losses in the line of transmission $T<1$ and ϵ is the so-called excess noise, which may be due, for instance, to spontaneous emission from an in-line amplifier. The security criterion $N<1$ can then be equivalently written as $\epsilon<2-1/T$ or $T>1/(2+\epsilon)$. In the best possible case of a lossy but noiseless line, security thus requires that $T>1/2$; that is, more than half the intensity has to reach the receiver. This limit, known as the 3 dB loss limit, was first thought to be generic to CV-QKD.

B. Beating the 3 dB Loss Limit

It was realized, however, that this limit is protocol dependent and can be beaten just like in photon-counting QKD, where no loss limit applies because only the photons that are received by Bob are taken into account. The technique of reverse reconciliation[30] was shown to be applicable to CVs, so that the key distribution remains secure for any value of the line transmission.[8] To achieve this, the secret key must be made out of the (noisy) data received by Bob instead of the data sent by Alice. Since it is harder for Eve to infer Bob's errors than to guess Alice's data, this reverse protocol provides a definite informational advantage to Alice and Bob.

An alternative technique proposed at the same time to beat the 3 dB loss limit is to carry out a postselection by putting some threshold on Bob's data.[31–34] In this type of protocol, some sort of discretization of the states prepared by the sender is involved, followed by a state discrimination and postselection procedure by the receiver. Although these protocols seem to be promising in terms of tolerable losses and excess noise,[35–40] their security has unfortu-

nately not been firmly established because the best eavesdropping strategy is still unknown (see also Section 6).

Another fully continuous QKD protocol has been proposed in Refs. 41 and 42, in which Alice sends the same mixture of coherent states as in Ref. 16, but Bob measures both quadratures (with a beam splitter) instead of choosing one quadrature. This protocol has the advantage that Bob does not need to generate a random bit to choose a basis. An experimental implementation was presented in Ref. 43, but the quoted key rates were based on a less general security proof, restricted to beam-splitting attacks ($\epsilon=0$ in our notation). Other schemes, using coherent states but related to quantum encryption rather than QKD, have also been introduced.[44]

C. Classification of Attacks

Let us start by recalling the hierarchy of attacks against QKD that is generally adopted in the literature and that we adapt here to CV-QKD.

- Individual attacks. Eve can couple each pulse with an individual ancilla and store the resulting state of the ancilla in a quantum memory until Bob reveals his measurement basis. She then measures each ancilla in the appropriate basis and exploits here data classically. Some restricted classes of individual attacks are also considered:

  (i) Individual Gaussian attacks. Eve can perform any individual Gaussian operation; that is, she can use squeezing, entanglement, amplifiers, beam-splitting, etc.

  (ii) Beam-splitting attacks without added noise ($\epsilon=0$). Here squeezing, entanglement, amplifiers, intercept–resend attacks are forbidden. Though this case has been often considered in the literature, it is a restrictive class of attacks, based on the so-called no-excess noise hypothesis. It corresponds to Eve simulating a lossy but noiseless line, which is equivalent to an errorless line in photon-counting QKD.
- Collective attacks. Eve can again couple each pulse with an individual ancilla and store the state of a long block of ancillae in a quantum memory until Bob reveals his measurement basis and performs error correction and privacy amplification for the entire block. Then she measures coherently all ancillae (with a quantum computer) in order to optimize her information on the block.
- Coherent attacks. Eve can couple a pre-entangled multipulse ancilla with all pulses exchanged by Alice and Bob to make the key and store the state of the ancilla in a high-dimensional quantum memory until Bob reveals his measurement basis for the entire key and performs error correction and privacy amplification. She then measures coherently the ancilla (with a quantum computer) in order to optimize her information on the key. This should be the most general (and most practically infeasible) attack. It is often conjectured that coherent attacks are not really better than collective ones.

Note that collective or coherent attacks can be specified as finite size, which means that Alice and Bob are able to (classically) process blocks that are much larger than those Eve can process (in her quantum computer). Finite-size security with typical blocks with size of 10^5 bits for Alice and Bob is usually considered reliable, although not unconditional.

D. Secret Rates Achieved by the Gaussian-modulated Coherent-State Protocol

Here we give the secret bit rates that are obtained with the CV-QKD protocol based on Gaussian-modulated coherent states and reverse reconciliation, as described in Refs. 8 and 45. Alice sends Bob a train of coherent states $|x+ip\rangle$ where the quadratures (x,p) are randomly chosen from a bivariate Gaussian distribution with variance V_A. Bob randomly measures either x or p and publicly announces his choice. A binary secret key is then extracted from the correlated continuous data by reverse reconciliation: Bob sends Alice some parity bits on a classical (authenticated) side channel, so that she can correct her data to match Bob's data. For consistency, this reconciliation protocol must be one way (from Bob to Alice).

The processing of the coherent states sent by Alice in the transmission channel can be described in the following way: its amplitude is multiplied by $\sqrt{T}$, where $T\leqslant 1$ is the channel transmission, while its noise variance (normalized to the shot-noise level) is increased to $(1+T\epsilon)$ at the output, where ϵ is the so-called excess noise referred to the input as used in all formulas below. We assume that Bob's homodyne detector, with limited efficiency $\eta<1$ and electronic noise v_{el}, deteriorates Bob's reception but does not contribute to Eve's information (so-called realistic mode[8,45]). Denoting by V_A the variance of Alice's modulation in shot-noise units, we can write the information rates that are relevant for individual Gaussian attacks as

$$I_{AB}=\frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{\text{tot}}}\right), \tag{4}$$

$$I_{BE}=\frac{1}{2}\log_2\left[\frac{T^2(1+\chi_{\text{tot}}+V_A)\left(\chi_{\text{line}}+\frac{1}{1+V_A}\right)}{1+T\chi_{\text{hom}}\left(\chi_{\text{line}}+\frac{1}{1+V_A}\right)}\right]. \tag{5}$$

The total noise χ_{tot} (referred to the input) can be split as $\chi_{\text{tot}}=\chi_{\text{line}}+\chi_{\text{hom}}/T$, where $\chi_{\text{line}}=(1-T)/T+\epsilon$ is the noise due to line losses and excess noise during the transmission and $\chi_{\text{hom}}=(1-\eta)/\eta+v_{\text{el}}/\eta$ is the noise from Bob's homodyne detection. All the quantities appearing in these formulas are known or can be measured by Alice and Bob.

Using Eqs. (4) and (5) and the Csiszar–Körner theorem, we conclude that the raw secret key rate

$$K_{\text{raw}}=I_{AB}-I_{BE} \tag{6}$$

can be attained in reverse reconciliation. This rate was proven to be secure against Gaussian individual attacks[8,30] and finite-size non-Gaussian attacks.[46] For collective attacks, the value of Eve's information, given here as the Shannon mutual information I_{BE}, has to be changed into a Holevo quantity χ_{BE} (see details in Section 6).

An essential ingredient to make CV-QKD protocols practical lies in the ability to efficiently extract common secret bits on Alice's and Bob's sides from the correlated strings of continuous data provided by the quantum protocol and simultaneously to correct errors without revealing too much information to Eve. A method for achieving this goal, named sliced reconciliation, was proposed in Ref. 47. By alternating bit-extraction and error-correction steps over successive bit slices, it is possible to extract a number of common bits that reaches typically 80% to 85% of Shannon's limit. Thus, the above value of K_{raw} is not really relevant in practice, as one must take into account the efficiency β of the reconciliation algorithm with respect to Shannon's limit. The practical net secret key rate is then

$$K_{\mathrm{net}} = \beta I_{AB} - I_{BE}, \tag{7}$$

where the value of β depends on the quality of the reconciliation algorithm. It was recently shown that this quality can be significantly improved by using low-density parity-check (LDPC) codes.[48] A typical value obtained using LDPC codes is $\beta = 0.87$, but further optimization is certainly possible. Let us note that LDPC codes are fully one-way protocols (as required by reverse reconciliation) and that almost all the computing effort takes place at Alice's site; i.e., the costs of syndrome computation and transmission by Bob are negligible.

In practice, Alice and Bob must carefully evaluate T and ϵ in order to infer the optimal attack Eve can perform and therefore to upper bound I_{BE}. This is done by statistical evaluation over a random subset of the raw data.[45] This finite set size introduces statistical fluctuations that can alter the excess noise estimate, and security margins have to be considered when information rates are computed. Optimizing the channel evaluation without sacrificing too many secret bits is a generic question in QKD, which is not specific to CV implementations and deserves further attention.[49]

5. EXPERIMENTAL DEMONSTRATIONS

A. Proof-of-Principle Experiments

A tabletop experimental demonstration of the Gaussian-modulated coherent-state protocol with reverse reconciliation was reported in Ref. 8 (see Fig. 2). A significant advantage of this setup is that it does not need sophisticated devices such as single-photon sources or counters. It uses a laser diode at 780 nm to generate pulses at a repetition rate of 800 kHz. These coherent light pulses are modulated in amplitude and phase by Alice and then measured by Bob with homodyne detection. Finally, the resulting data are processed, together with Alice's data, by an appropriate sliced (multilevel) reconciliation algorithm.[47] This method was applied to the experimental data obtained with a variance ranging between 25 and 40 shot-noise units. The obtained net secret key bit rate was 1.7 Mbit/s for a lossless line and 75 kbit/s for a line with a 3.1 dB loss (these rates include privacy amplification but not the computing time as the calculations were actually carried out off-line). Given that this experiment was a first demonstration with off-the-shelf components and no optimization for speed, these rates are quite significant when compared with photon-counting QKD and open interesting perspectives for coherent-state CV-QKD.

Let us summarize here the pros and cons of such an implementation of CV-QKD, by comparison with photon-counting-based QKD.

- Pros

—The coherent states are produced and measured unconditionally, that is, at each repetition period. This feature is hard to obtain for single-photon sources and detectors. Of course, single-photon protocols may be run with weak coherent pulses instead, but in the standard security approach the number of photons per pulse must be much smaller than 1 (note that new protocols involving, e.g., decoy states[50] can increase the average photon number per pulse to around 1). In 1550 nm experiments,

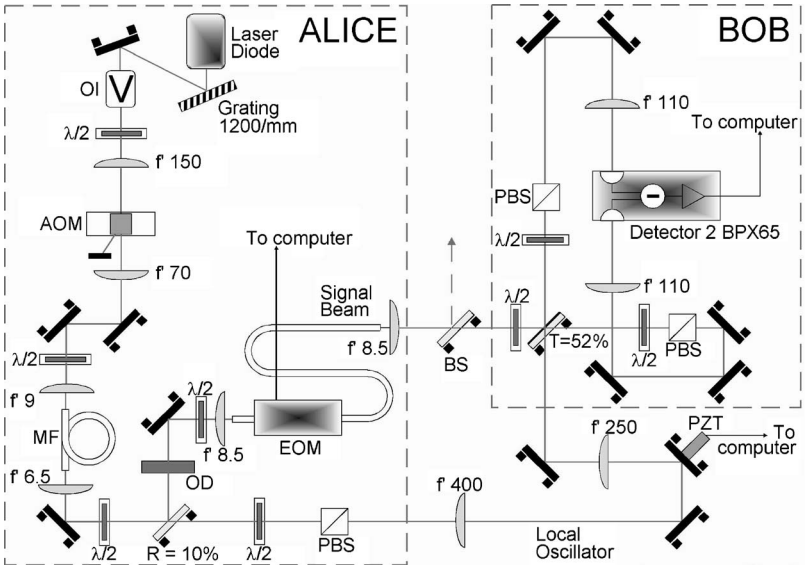

Fig. 2. First experimental implementation of CV-QKD using a modulated coherent-state protocol.[8] The operating wavelength is 780 nm. OI, optical isolator; λ/2, half-wave plate; AOM, acousto-optic modulator; MF, polarization-maintaining single-mode fiber; OD, optical density; EOM, electro-optic amplitude modulator; PBS, polarizer; BS, beam splitter; R and T, reflection transmission coefficients; PZT, piezoelectric transducer. Focal lengths are given in millimeters.

the limited quantum efficiency of the detectors also represents an important limitation of single-photon protocols. A possible solution to this may be to turn to 800 nm experiments, e.g., by using upconversion detectors.[51,52] But the high efficiency of homodyne detection, as used in CV-QKD, remains an advantage.

—Homodyne detection can, in principle, reach high bit rates. In contrast, single-photon detectors, which are based on avalanche photodiodes, are more limited in frequency, largely owing to afterpulsing. Again, recent developments in photon-counting QKD have tried to fight this effect and succeeded in reaching clock rates in the gigahertz range.[53,54] However, if its inherent data processing bottleneck can be overcome, CV-QKD has the potential of enhancing the repetition rates by orders of magnitude.

—CV-QKD requires only off-the-shelf telecom components and well-known techniques of coherent optical telecommunication, which have been extensively studied in the 1980's. It is then relatively simple to reach secret key rates in the megabits per second range for low transmission losses. Specific components (mostly dedicated electronics) should allow one to reach much higher rates, typically in the 100 Mbits/s range.

- Cons

—Although it does not require any specific component development, a homodyne detector is a rather sophisticated device that must be implemented with care to warrant the claimed security.

—The inherent presence of vacuum noise, even for a perfect line without eavesdropping, makes it such that powerful error-correction techniques are needed for an efficient key extraction. Physically, this is because the homodyne measurement of vacuum gives a Gaussian-distributed noise (the shot noise), while, in principle, vacuum never gives rise to a click with an ideal single-photon detector.

—A CV-QKD system is more vulnerable to channel losses. This is a consequence of the previous point: it is necessary to eliminate a larger amount of noise (intrinsic vacuum noise as well as loss-induced additional vacuum noise), which requires more computing effort than for photon-counting-based QKD.

It is worthwhile discussing a bit further this last issue, namely, that line losses create errors (due to vacuum noise) in CV-QKD, while they do not in photon-counting-based QKD (because the photon is simply not detected). First, let us stress again that this loss-induced noise does not limit the range: CV-QKD is, in principle, secure regardless of the line loss, just like photon-counting-based QKD in the absence of dark counts. However, this loss-induced noise must be actively suppressed in CV-QKD by classical postprocessing of the noisy data, whereas this is done "for free" in photon-counting-based QKD by the physics of the avalanche photodiode. CV-QKD is therefore more sensitive to the line loss because it puts a stringent constraint on the reconciliation procedure. It is also important to emphasize that the CV-QKD analogue of errors in photon-counting-based QKD [i.e., of a nonzero quantum bit error rate (QBER)] is the excess noise ϵ and not the vacuum noise $(1-T)/T$ [see Eq. (3)]. As a consequence, security studies of CV-QKD must take the excess noise ϵ into account, just as security studies of photon-counting QKD must be based on the QBER.

B. Experiments Using Fiber Transmission

The tabletop experiment shown in Fig. 2 can be transposed to telecom wavelength by using only standard telecom components, which makes it possible to transmit the light signals in an optical fiber, making the setup ready for field applications. This direction has been followed by the Institut d'Optique, in collaboration with Thales, and the first results have been presented in Ref. 45. A similar setup has been implemented at the University of Geneva.[55] The present setup of Ref. 45, depicted in Fig. 3, is a fiber-based system working at a wavelength of $\sim$1550 nm. The local oscillator (LO) for Bob's homodyne detection is transmitted in the same fiber as the signal, by using time multiplexing. The pulse rate is $\sim$1 MHz, and the pulse duration is 100 ns. These values are essentially limited by the technology of the personal computer–driven data acquisition system, for which the repetition rates cannot exceed a few megahertz. Repetition rates in the 100 MHz range would be compatible with the modulation and detection systems but would require the use of dedicated electronics for data acquisition, processing, and storage. The present efficiency of the homodyne detection is around 60%, which can be decomposed into 80% for the selected InGaAs photodiodes and 75% for the connectors and optical components, including a passive demultiplexer. The noise of the modulators is measured to be typically around 0.05 shot-noise units. This includes the noise due to the three modulators (Gaussian modulation at Alice's station and binary modulation at Bob's station), phase noise, and electronic noise.

Typical secret key rates expected from this setup are displayed on Fig. 4. The curves are drawn for $V_A=12$ and for noise levels measured on the experiment ($\epsilon=0.025$, $\eta=0.6$, $v_{el}=0.05$). The net secret key rate $K_{\mathrm{net}}=\beta I_{AB}-I_{BE}$ is software dependent and is typically a few tens of kilobits per second as shown on Fig. 4, depending on the value of β (one currently obtains $\beta\sim 0.87$ with LDPC codes). In the present implementation, the rate is further reduced down to a few kilobits per second because of the limited speed of the computer, which is not able to process the data as fast as the data come. These two last points, which rely basically on classical LDPC (or turbo) codes, are presently under optimization. These results clearly illustrate that CV-QKD trades off some hardware difficulty (getting good photon counters) against some software difficulty (getting fast and efficient multilevel error-correcting codes).

6. STATUS OF THE SECURITY PROOFS

A. Individual Gaussian Attacks and Shannon Formula

The first security proof on direct[15,16] and reverse[8,30] reconciliation protocols considered only individual Gaussian attacks. This certainly does not mean easy attacks because such attacks already imply that Eve must have a long-lived quantum memory for storing light states and

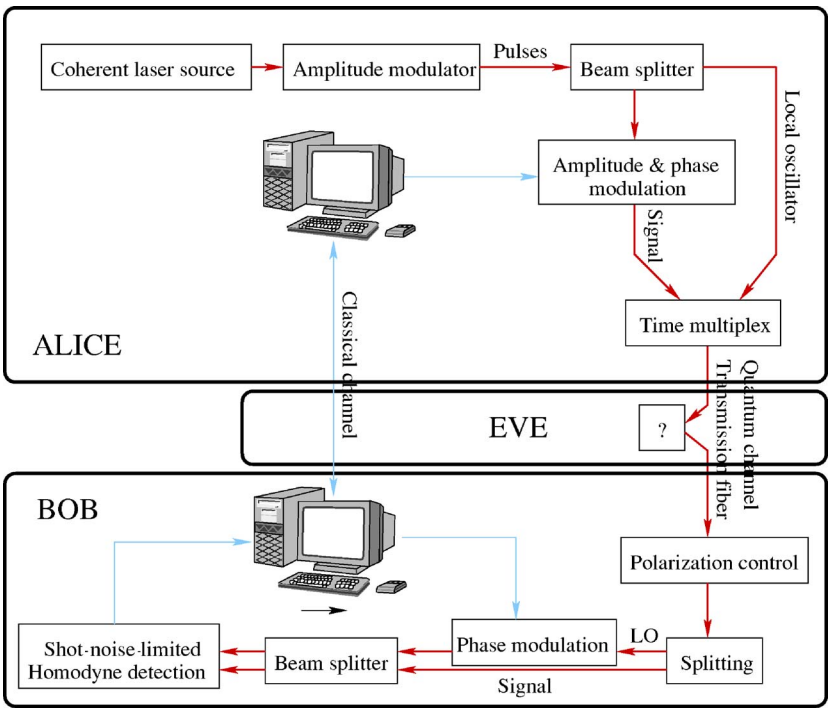

Fig. 3. (Color online) CV-QKD platform (Institut d'Optique and Thales Research and Technology). The operating wavelength is 1550 nm, and the setup uses only standard optical telecommunication components (distributed feedback laser, integrated amplitude and phase modulators, p-i-n photodiodes). The transmission channel is currently a coil of 25 km standard optical fiber.

also must produce pairs of light beams with arbitrary entanglement. Nevertheless, such attacks are not the most general ones, and, more recently, several new security proofs of coherent-state CV-QKD have appeared (see Subsections 6.B and 6.C).

An important first step is to realize that these protocols are actually equivalent to entangled-based protocols, where Alice measures simultaneously both quadratures on her entangled beam so to prepare a Gaussian-modulated coherent state at Bob's side.[56] This virtual entanglement, also known for photon-counting QKD, is useful for establishing security proofs. It also implies that there is an entanglement-breaking limit in CV protocols,[35–40] corresponding to an intercept-and-resend attack, which gives $\epsilon<2$. This means that when the excess noise exceeds two shot-noise units (referred to the input), no secure key distribution is possible.

More restrictive security limits can actually be established. The underlying proofs are based upon inequalities for added noise and conditional variances, similar to the ones introduced for QND measurements,[57] which are then plugged into Shannon's formula for a Gaussian channel. In principle, the key extraction (from the continuous data) should be performed up to the Shannon limit for a Gaussian channel, in which case the security is ensured for arbitrary high losses. Otherwise, the secret key rate decreases and vanishes at some finite loss, even if some secret bits are in principle available. The result is that, for an entanglement-based protocol using reverse reconciliation, the security bound becomes

$$\epsilon = 1. \tag{8}$$

For a coherent-state protocol, the bound is

$$\epsilon < 2 - 1/T \tag{9}$$

for direct reconciliation (as already seen in Subsection 4.A) and

$$\epsilon < 1/2 - 1/T + \sqrt{1/T^2 + 1/4} \tag{10}$$

for reverse reconciliation, provided that the variance of Alice's modulation is large enough. The relation between the excess noise ϵ and the maximum distance for secure QKD is shown in Fig. 5, assuming fiber losses of 0.2 dB/km. Curve (a) is the entanglement-breaking attack ($\epsilon=2$), curve (b) is obtained with the entangled-beam reverse reconciliation protocol ($\epsilon=1$), while the last two curves correspond to coherent-state protocols using either direct (c) or reverse (d) reconciliation.

B. Non-Gaussian Attacks and Entropic Heisenberg Relations

An important achievement in the quest for security proofs is the demonstration, based on replacing the QND-type inequalities by entropic Heisenberg relations, that the individual Gaussian attacks are actually the best possible attacks against reverse reconciliation protocols.[46] This proof covers all non-Gaussian attacks and even collective attacks, provided that their size remains smaller than the key size and provided that Eve does not delay her measurement until after the key distillation procedure. It means that the above limits, which were derived for individual Gaussian attacks, are actually valid in a much more general framework. It is worth emphasizing that, according to this proof, Alice and Bob should use a Gaussian modulation for exchanging data because it maximizes the information flow (for a given modulation variance) in

the Gaussian additive-noise channel that is effected by Eve. In that respect, using any kind of discrete modulation of the signal will be less efficient, a fact that further justifies the Gaussian encoding scheme.

C. Collective and Coherent Attacks

More recent progress has also been made in the direction of finding unconditional security proofs for coherent-state protocols. The first attempt consisted of extending the unconditional security proof of the squeezed-state protocol of Ref. 22, which itself is an extension of the Shor–Preskill proof for BB84. In short, the idea is to show that squeezing, which is required in the proof of Ref. 22, is used only to evaluate the channel's error rate and can actually be replaced by a channel tomography procedure using only coherent states.[58] This approach shows that the unconditional security of Gaussian-modulated coherent-state protocols is achievable, provided that the number of bits to sacrifice is specifically evaluated.[59] However, this evaluation requires a huge precision in the channel tomography, which currently makes this approach impractical. Finally, let us note that this proof yields the same theoretical rate as the one from the information-theoretic proofs presented below, when Eve is restricted to Gaussian collective attacks (which are actually optimal, see below).

Still another approach to the security consisted of adapting the concept of advantage distillation to an appropriately designed CV-QKD protocol, different from the ones considered above.[60] It was shown that the security threshold of this protocol against individual Gaussian attacks is identical to the channel entanglement-breaking limit [curve (a) on Fig. 5], and a quantitative threshold against collective attacks could be derived. Let us note that present advantage-distillation protocols yield a positive secret rate in regions where the protocols of Refs. 15 and 16 do not work any more, but they are only existence proofs and do not provide an explicit value of the secret key rate.

A more practical approach is to use general information-theoretic arguments in order to address the security with respect to collective Gaussian attacks.[61,62] In short, the idea is to apply the Devetak–Winter[63] security proof (where the Shannon information is replaced by the Holevo quantity) to the CV protocols. Eve is now authorized to make a delayed measurement, after the key distillation process, but she is restricted to use Gaussian attacks. Interestingly, up to some apparently minor restrictions, the previous results on individual attacks can be generalized to collective attacks. In particular, the loss behavior of direct reconciliation (3 dB limit) and reverse reconciliation (no loss limit) is recovered. Interestingly, although it may look similar to other protocols,[15,16] the protocol in which Bob measures both quadratures[41,42] happens to be slightly less secure against collective attacks.[61]

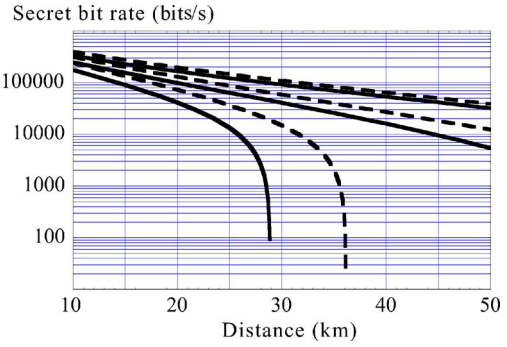

Fig. 4. (Color online) Typical secret key rates expected from the fiber CV-QKD setup, assuming a 1 MHz pulse rate. Dashed curves show the rate $K_{net}=\beta I_{AB}-I_{BE}$ (secure against arbitrary individual attacks) for $\beta=1$ (upper), $\beta=0.93$ (middle), $\beta=0.87$ (lower curve). Solid curves show the rate $H_{net}=\beta I_{AB}-\chi_{BE}$ (secure against arbitrary collective attacks; see Subsection 6.C) for the same values of β.

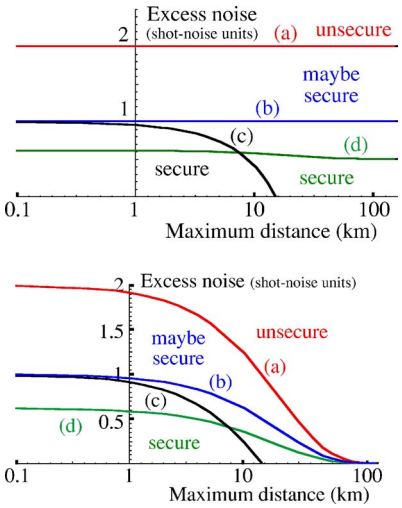

Fig. 5. (Color online) Two different views of the tolerable excess noise as a function of the distance. In the upper panel we plot the maximum value of the excess noise ϵ referred to the input (as used in the present paper and in other publications by our groups), and in the lower panel we plot the maximum value of the product ϵT effectively measured by Bob (as used, e.g., in Refs. 35–40). The various curves refer to (a) entanglement-breaking limit, (b) two-mode squeezed states and reverse reconciliation, (c) coherent states and direct reconciliation, and (d) coherent states and reverse reconciliation.

The latest development in the security analysis of CV-QKD is the proof that the above-derived bounds for collective attacks[61,62] are actually much more general than expected because Gaussian attacks are optimal against all collective attacks.[64,65] This further step on the way to unconditional security can be summarized simply and represents the current state of the art: to warrant security against collective (Gaussian or non-Gaussian) attacks, it is enough to replace the previous Shannon secret bit rates $K_{raw}=I_{AB}-I_{BE}$ or $K_{net}=\beta I_{AB}-I_{BE}$ by Holevo secret bit rates, $H_{raw}=I_{AB}-\chi_{BE}$ or $H_{net}=\beta I_{AB}-\chi_{BE}$. Here, χ_{BE} is the Holevo quantity for a Gaussian state, which can be computed analytically from the von Neumann entropy of a thermal state. In practice, the values of the Holevo rates are only slightly smaller than the Shannon rates (see Fig. 4), so that the secret key bit rates are not reduced much while they become secure in a much stronger sense.

For fully coherent attacks, it can be concluded that the security can most probably be warranted with some restrictions, e.g., on channel transmission. This is at present still a conjecture, but it can be made plausible given the recent result that, for BB84, coherent attacks do not outperform collective attacks.[49] This work is still in progress, but it seems so far that the reverse-

reconciliation coherent-state protocol with Gaussian modulation and homodyne measurement is remarkably resistant against more and more powerful attacks.

7. CONCLUSION

Coherent-state CV-QKD can be implemented by using only standard optical telecommunication equipment, without the need for dedicated photon sources or single-photon counters. Let us emphasize again that, in principle, secure CV-QKD can be achieved for arbitrarily high channel losses. The theoretical long-distance secret key bit rate of the reverse-reconciliation coherent-state Gaussian-modulated protocol (with ideal error correction) is roughly equal to that of an ideal BB84 (with a perfect single-photon source and detector). A basic lesson we can draw from reverse reconciliation is that the errors due to line losses can be eliminated, in principle, to the same extent as the line losses do not compromise the security of photon-counting protocols. In some sense, the role of errors in photon-counting QKD is played by the excess noise in CV-QKD, and both of them lead to a fundamental decrease in the secret bit rate. As illustrated in Fig. 5, the maximum tolerable excess noise for coherent-state CV-QKD decreases with the distance, which is what eventually puts a limit on the achievable security over long distances.

The first experimental demonstration,[8] as reported on in this paper, was a tabletop proof-of-principle experiment only. Several experiments have since then been completed (or are under way) to characterize such systems in the telecom domain. As with photon-counting QKD, several options are available: the pulses may be sent one way in an optical fiber using a time-multiplexing technique,[45] may be retroreflected using Faraday mirrors,[55] or may be sent in free space by using a polarization variant of the basic scheme.[32] These various possibilities are presently investigated in several laboratories in the framework of the European Integrated Project on the Development of a Global Network for Secure Communication Based on Quantum Cryptography[66] (SECOQC).

Ultimately, losses will be a limitation for CV-QKD protocols for practical reasons, just as they are for photon-counting protocols. One may then consider building quantum repeaters, based on CV entanglement distillation procedures. A first step in this direction is to learn how to manipulate non-Gaussian states, which are a required ingredient for CV entanglement distillation. This was recently achieved both for light fields[67,68] and for atomic variables.[69] All these recent developments, on both the theoretical and the experimental sides, clearly indicate that quantum CV may play a key role in the future of QKD.

ACKNOWLEDGMENTS

We thank our coworkers T. Debuisschert, R. Garcia-Patron, F. Grosshans, S. Iblisdir, J. Lodewyck, R. Tualle-Brouri, G. Van Assche, and J. Wenger for essential contributions to this work. This research is supported by the European Commission within the Information Society Technologies–Future and Emerging Technologies program under the Integrated Project SECOQC and the Specific Targeted Research Project Continuous Variable Quantum Information with Atoms and Light (COVAQIAL).

The corresponding author, P. Grangier, can be reached by e-mail at philippe.grangier@institutoptique.fr.

*Laboratoire Charles Fabry is an Unité Mixte de Recherche of the Institut d'Optique Graduate School, Centre National de la Recherche Scientifique, and Université Paris-Sud.

REFERENCES

1. S. L. Braunstein and A. K. Pati, eds., *Quantum Information with Continuous Variables* (Kluwer Academic, 2003).
2. N. J. Cerf, G. Leuchs, and E. S. Polzik, eds., *Quantum Information with Continuous Variables of Atoms and Light* (Imperial College, 2006).
3. A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," Science **282**, 706–709 (1998).
4. B. Julsgaard, A. Kozhekin, and E. S. Polzik, "Experimental long-lived entanglement of two macroscopic objects," Nature **413**, 400–403 (2001).
5. B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurasek, and E. S. Polzik, "Experimental demonstration of quantum memory for light," Nature **432**, 482–486 (2004).
6. U. L. Andersen, O. Glöckl, S. Lorenz, G. Leuchs, and R. Filip, "Experimental demonstration of continuous variable quantum erasing," Phys. Rev. Lett. **93**, 100403 (2004).
7. U. L. Andersen, V. Josse, and G. Leuchs, "Unconditional quantum cloning of coherent states with linear optics," Phys. Rev. Lett. **94**, 240503 (2005).
8. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
9. L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, "Inseparability criterion for continuous variable systems," Phys. Rev. Lett. **84**, 2722–2725 (2000).
10. R. Simon, "Peres–Horodecki separability criterion for continuous variable systems," Phys. Rev. Lett. **84**, 2726–2729 (2000).
11. J. Eisert, S. Scheel, and M. B. Plenio, "On the impossibility of distilling Gaussian states with Gaussian operations," Phys. Rev. Lett. **89**, 137903 (2002).
12. P. Horodecki and M. Lewenstein, "Bound entanglement and continuous variables," Phys. Rev. Lett. **85**, 2657–2660 (2000).
13. R. F. Werner and M. M. Wolf, "Bound entangled Gaussian states," Phys. Rev. Lett. **86**, 3658–3661 (2001).
14. N. J. Cerf, A. Ipe, and X. Rottenberg, "Cloning of continuous quantum variables," Phys. Rev. Lett. **85**, 1754–1757 (2000).
15. N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).
16. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
17. T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, "Quantum computation with optical coherent states," Phys. Rev. A **68**, 042319 (2003).
18. P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing," arXiv: quant-ph/0512071 (2005).
19. N. J. Cerf and S. Iblisdir, "Optimal *N*-to-*M* cloning of

conjugate quantum variables," Phys. Rev. A **62**, 040301(R) (2000).
20. S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, "Optimal cloning of coherent states with a linear amplifier and beam splitters," Phys. Rev. Lett. **86**, 4938–4941 (2001).
21. J. Fiurasek, "Optical implementation of continuous-variable quantum cloning machines," Phys. Rev. Lett. **86**, 4942–4945 (2001).
22. D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001).
23. M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**, 022309 (2000).
24. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303(R) (2000).
25. M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein–Podolsky–Rosen correlations," Phys. Rev. A **62**, 062308 (2000).
26. K. Bencheikh, Th. Symul, A. Jankovic, and J. A. Levenson, "Quantum key distribution with continuous variables," J. Mod. Opt. **48**, 1903–1920 (2001).
27. Ch. Silberhorn, N. Korolkova, and G. Leuchs, "Quantum key distribution with bright entangled beams," Phys. Rev. Lett. **88**, 167902 (2002).
28. A. C. Funk and M. G. Raymer, "Quantum key distribution using nonclassical photon-number correlations in macroscopic light pulses," Phys. Rev. A **65**, 042307 (2002).
29. J. Jing, Q. Pan, C. Xie, and K. Peng, "Quantum cryptography using Einstein–Podolsky–Rosen correlations of continuous variables," arXiv.org: quant-ph/0204111 (2002).
30. F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," arXiv: quant-ph/0204127 (2002).
31. C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: beating the 3 dB loss limit," Phys. Rev. Lett. **89**, 167901 (2002).
32. S. Lorenz, N. Korolkova, and G. Leuchs, "Continuous-variable quantum key distribution using polarization encoding and post selection," Appl. Phys. B **79**, 273–277 (2004).
33. R. Namiki and T. Hirano, "Security of quantum cryptography using balanced homodyne detection," Phys. Rev. A **67**, 022308 (2003).
34. T. Hirano, H. Yamanaka, M. Ashikaga, I. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," Phys. Rev. A **68**, 042331 (2003).
35. R. Namiki and T. Hirano, "Practical limitation for continuous-variable quantum cryptography using coherent states," Phys. Rev. Lett. **92**, 117901 (2004).
36. R. Namiki and T. Hirano, "Security of continuous-variable quantum cryptography using coherent states: decline of postselection advantage," Phys. Rev. A **72**, 024301 (2005).
37. M. Heid and N. Lütkenhaus, "Efficiency of coherent-state quantum cryptography in the presence of loss: influence of realistic error correction," Phys. Rev. A **73**, 052316 (2006).
38. M. Curty, M. Lewenstein, and N. Lütkenhaus, "Entanglement as a precondition for secure quantum key distribution," Phys. Rev. Lett. **92**, 217903 (2004).
39. M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, "Detecting two-party quantum correlations in quantum-key-distribution protocols," Phys. Rev. A **71**, 022306 (2005).
40. M. Heid and N. Lütkenhaus, "Security of coherent state quantum cryptography in the presence of Gaussian noise," arXiv: quant-ph/0608015 (2006).
41. Ch. Weedbrook, A. M. Lance, W. P. Bowen, Th. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
42. Ch. Weedbrook, A. M. Lance, W. P. Bowen, Th. Symul, T. C. Ralph, and P. K. Lam, "Coherent-state quantum key distribution without random basis switching," Phys. Rev. A **73**, 022316 (2006).
43. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-switching quantum key distribution using broadband modulated coherent light," Phys. Rev. Lett. **95**, 180503 (2005).
44. G. A. Barbosa, E. Corndorf, and P. Kumar, "Quantum cryptography with coherent-state light: demonstration of a secure data encryption scheme operating at 100 kb/s," in *Quantum Electronics and Laser Science (QELS)*, Vol. 74 of OSA Trends in Optics and Photonics Series (Optical Society of America, 2002), pp. 189–190.
45. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**, 050303(R) (2005).
46. F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-Gaussian attacks," Phys. Rev. Lett. **92**, 047905 (2004).
47. G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," IEEE Trans. Inf. Theory **50**, 394–400 (2004).
48. M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using LDPC codes," arXiv: cs.IT/0509041 (2005).
49. R. Renner, "Security of quantum key distribution," Ph.D. thesis (ETH Zurich 2005).
50. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," Phys. Rev. Lett. **96**, 070502 (2006).
51. E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, "Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors," Phys. Rev. A **72**, 052311 (2005).
52. R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, "Low jitter up-conversion detectors for telecom wavelength GHz QKD," New J. Phys. **8**, 32 (2006).
53. J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," Opt. Express **12**, 2011–2016 (2004).
54. K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," Opt. Express **13**, 3015–3020 (2005).
55. M. Legré, H. Zbinden, and N. Gisin, "Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration," Quantum Inf. Comput. **6**, 326–335 (2006).
56. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quantum Inf. Comput. **3**, 535–552 (2003).
57. P. Grangier, J.-A. Levenson, and J.-Ph. Poizat, "Quantum demolition measurements in optics," Nature **396**, 537–542 (1998).
58. S. Iblisdir, G. Van Assche, and N. J. Cerf, "Security of quantum key distribution with coherent states and homodyne detection," Phys. Rev. Lett. **93**, 170502 (2004).
59. G. Van Assche, S. Iblisdir, and N. J. Cerf, "Secure coherent-state quantum key distribution protocols with efficient reconciliation," Phys. Rev. A **71**, 052304 (2005).
60. M. Navascués, J. Bae, J. I. Cirac, M. Levenstein, A. Sapera, and A. Acín, "Quantum key distillation from Gaussian states by Gaussian operations," Phys. Rev. Lett. **94**, 010502 (2005).
61. F. Grosshans, "Collective attacks and unconditional security in continuous variable quantum key distribution," Phys. Rev. Lett. **94**, 020504 (2005).
62. M. Navascués and A. Acín, "Security bounds for continuous variables quantum key distribution," Phys. Rev. Lett. **94**, 020505 (2005).
63. I. Devetak and A. Winter, "Relating quantum privacy and quantum coherence: an operational approach," Phys. Rev. Lett. **93**, 080501 (2004).
64. R. García-Patrón and N. J. Cerf, "Unconditional optimality

of Gaussian attacks against continuous-variable QKD," Phys. Rev. Lett. **97**, 190503 (2006).
65. M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
66. See http://www.secoqc.net/.
67. J. Wenger, R. Brouri, and P. Grangier, "Non-Gaussian statistics from individual pulses of squeezed light," Phys. Rev. Lett. **92**, 153601 (2004).
68. A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier, "Generating optical Schrödinger kittens for quantum information processing," Science **312**, 83–86 (2006).
69. J. S. Neergaard-Nielsen, B. Melholt Nielsen, C. Hettich, K. Moelmer, and E. S. Polzik, "Generation of a superposition of odd photon number states for quantum information networks," Phys. Rev. Lett. **97**, 083604 (2006).