Quantum cloning and key distribution with continuous variables

Nicolas Cerf
Nicolas Cerf is Associate Professor at ULB, where he heads the Centre for Quantum Information and Communication (QUIC). After having earned a Ph.D. in Physics at ULB in 1993, he was awarded a Marie Curie fellowship from the EC, and worked for two years as a post-doctoral research associate at the Division of Theoretical Physics in Orsay, France. His research then mainly concerned quantum many-body systems and quantum Monte Carlo methods. In 1995, he joined the California Institute of Technology, USA, to work on quantum computation and information theory, which then became his main research interest. In 1998, he was appointed as an Associate Professor at ULB, where he now teaches information and communication theory. He earned the Caltech President's Fund 1997 award, the Alcatel-Bell 1999 prize awarded by the Belgian National Fund for Scientific Research (FNRS), and a Fulbright award in 1999. He was member of the steering committee of the 5-year quantum information theory programme funded by the European Science Foundation, and is (or has been) involved in several QIPC projects under the EU-funded IST programme (EQUIP, QUIPROCONE, RESQ, SECOQC, COVAQIAL).

Philippe Grangier
Philippe Grangier is Directeur de Recherche at CNRS, and he is leading the Quantum Optics group in Institut d'Optique, Orsay. He got a Thèse de 3e Cycle in 1982 on Experimental Tests of Bell's Inequalities (under the supervision of Alain Aspect), and a Thèse d'Etat in 1986 on Experimental Studies on Non-Classical Properties of the Light, such as the production of single-photon states. After a post-doc in Bell Laboratories on squeezed states interferometry in 1987, he conducted many researches in quantum optics, and then in quantum information. He has been awarded prizes by Académie des Sciences (1987), French Physical Society (1988), Ernst-Abbe foundation (Carl Zeiss Award, 1990), and CNRS (Médaille d'Argent, 2002). Since the beginning of the 90's he has been involved in many European RTD projects, in the ESPRIT and then in the IST programs, as well as in Human Potential networks. He was the coordinator of two Research Training Networks, "Non-Classical Light" (1993-1996) and "QUEST" (2000-2004), and now he is in charge of the EU-funded IST FP6 Integrated Project "SCALA" (Scalable Quantum Computing with Light and Atoms). His research activities presently include various aspects of quantum cryptography, and the manipulation of single trapped atoms for quantum information processing.

Abstract
Quantum information with continuous variables is a paradigm which has attracted a growing interest lately, as a consequence of the prospect for high-rate quantum communication systems that may result from the use of standard telecommunication components. After introducing the concept of quantum continuous variables in optics, we turn to the fundamental impossibility of cloning continuous-variable light states, a result which is at the heart of quantum key distribution. We then present state-of-the-art quantum key distribution systems relying on continuous variables, with a special emphasis on the experimental demonstration of protocols using coherent light states. Finally, we briefly review the recent security proofs of these cryptographic protocols.

Introduction
Over the last years, there has been a lot of interest about the possibility to realize quantum informational and computational tasks with so-called **continuous variables**. In short, the idea 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). This research direction was triggered by the theoretical proposal for continuous-variable quantum teleportation, which was quickly followed by its experimental demonstration [1].

As is well known, the central concepts of quantum information theory such as quantum teleportation, quantum cryptography, or quantum algorithms have been initially developed for binary quantum carriers (quantum bits). This is indeed the most natural way to go in order to build the quantum counterpart to classical informational processes. However, the use of continuous-variable quantum systems, which may involve many photons in a light field, has some potential advantages over single-particle quantum systems. Such advantages lie in the prospect for higher optical data rates and simpler processing tools, based upon standard telecommunication techniques. Another significant strength of this paradigm is that the light-atoms quantum interface can be designed for continuous variables, so that distant atomic continuous-variable systems can be entangled.

The European Union has been at the forefront of the dramatic development of the field of **continuous-variable quantum information processing and communications** (CV-QIPC). A great deal of the main achievements in this direction, both theoretical and experimental, is due to European teams. To mention just a few, on the experimental side the group of Eugene Polzik (Niels Bohr Institute, Copenhagen, Denmark) was the first to entangle two atomic ensembles, and to realize a quantum memory for light [2]. The group of Gerd Leuchs (University of Erlangen, Germany) realized continuous-variable quantum cryptography, quantum erasing, and quantum cloning [3], and the group of one of the authors (PG) was the first to demonstrate continuous-variable coherent-state quantum cryptography [4], as well as de-gaussification operations. On the theoretical side, many groups have been involved in these developments, for example the group of Ignacio Cirac (Max-Planck Institute, Garching, Germany) who contributed to the characterization of continuous-variable entanglement, the group of Martin Plenio (Imperial College, London, UK) who investigated continuous-variable entanglement purification with non-Gaussian operations, the group of Reinhard Werner (Technical University of Braunschweig, Germany) who initiated the study of bound entanglement with Gaussian states, or the group of one of the authors (NC) who initiated the study of continuous-variable quantum cloning [5] as well as quantum cryptography.

This illustrates with no doubt that Europe has been a leading actor in CV-QIPC. **Two European projects are (or have been) entirely devoted to exploring this research direction, namely**

QUICOV (IST-1999-13071) and COVAQIAL (FP6-511004). This research effort is, to our knowledge, unmatched worldwide. In addition, an annual series of European workshops solely focused on this topic, funded by the European Science Foundation, has been organized since 2002.

Optical quantum continuous variables

Let us consider the continuous variables that naturally appear when describing 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 **continuous variables** that completely characterize the optical field.

When the quantum properties of light become of interest, such a classical description is not valid any more and we have to quantize the light field, that is, we have to turn to quantum optics. Then, the "granularity" of the light field becomes important and gives rise to photon counting processes, while the quadrature components x and p become non-commuting (but still continuous) observables. As a result of the Heisenberg uncertainty principle, x and p cannot be known together, in contrast to the situation in classical optics: any measurement of x deletes the information on p, and conversely. In some sense, the two quadrature components of light behave exactly as 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 the information. This departs from the standard QIPC paradigm where a binary variable (a bit) is encoded into a dichotomic degree of freedom of a single photon (a quantum bit), e.g., its polarization.

Although dealing with continuous-variable quantum information is conceptually less natural, it comes with several advantages: (i) the measurement technique, called **homodyne detection**, works at a very high rate; (ii) it is sufficient to process simple non-classical states of the light, known as single-mode squeezed states, into linear optics circuits in order to perform a large variety of multipartite informational processes over continuous variables; (iii) the Bell measurement, a corner stone of QIPC, can be realized deterministically with a balanced beam splitter followed by homodyne measurement. By comparison, quantum-bit based QIPC processes suffer the following problems: (i) the measurement technique is based on comparatively slower avalanche photodiodes; (ii) multipartite quantum circuits typically require two-body interaction between quantum bits; (iii) the Bell measurement achieved with a beam splitter is fundamentally restricted to a probabilistic measurement (it succeeds with a probability of 50% at most).

Continuous-variable quantum cloning

Consider for a moment the case of quantum bits. As is well known, the duality between the computational basis $\{|0\rangle, |1\rangle\}$ and the dual basis $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$ 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 case of continuous variables, one notes that the canonical variables (x, p) are linked by a Fourier transform, just as the Hadamard transform maps the computational to the dual basis for qubits. The quantum no-cloning theorem then implies that it is not possible to clone position states (x-states) and momentum states (p-states) by a same process. By measuring x and preparing clones as x-localized states, one would make a perfect x-states cloner; but this cloner would then fail at cloning

p-localized states. Obviously, the converse holds too, so that we must turn to **approximate** optimal cloning machines, which achieve the best possible imperfect copying of the state that is compatible with quantum mechanics.

A very natural candidate for continuous-variable cloning is a transformation that adds the same noise on both quadrature components. By exploiting the connection between measurement and cloning theory, a tight bound on this cloner can be obtained by exploiting the well-known fact that the best joint measurement of x and p for a coherent state suffers from an extra noise whose variance is equal to twice the shot-noise unit. Clearly, cloning the state and then measuring x on one clone and p on the other clone cannot beat this optimal measurement, so that the cloning process comes itself with a "price" of one shot-noise unit, the other unit simply coming from the measurement process. As was shown by the group of one of the authors (NC), one can build a Gaussian cloning machine that exactly saturates this bound [5]. The quantum circuit of this cloner (see **Figure 1a**) consists of four continuous-variable controlled-NOT gates preceded by a preparation stage. The two auxiliary input modes need to be initially prepared in the vacuum state, and they contribute each for half a shot-noise unit to the cloning noise. As a result, this cloner adds a Gaussian-distributed noise on 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 (see **Figure 1b**). A variant of this setup has been experimentally implemented very recently by the group of Gerd Leuchs [3]. Interestingly, the physical origin of the cloning noise becomes much more evident in the case of continuous variables than with quantum bits: it is indeed clear from **Figure 1** that the noise affecting the clones can be traced back to the vacuum fluctuations that unavoidably enter via the two auxiliary modes of the cloner.

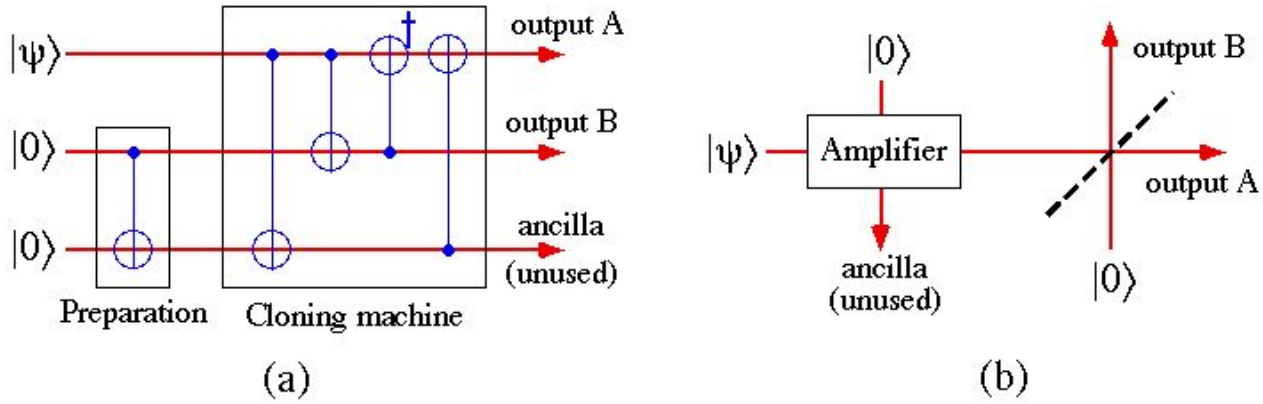

Figure 1

Continuous-variable quantum key distribution

The investigation of quantum cloning is of a particular significance given the strong connection between quantum cloning and quantum cryptography: it is indeed the impossibility to make a perfect cloning that makes it possible to detect a 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 devising quantum cryptographic schemes specifically designed for continuous variable.

More precisely, the idea is 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 was made by the team of one of the authors (NC), and independently by Gottesman and Preskill. This protocol, which can be viewed as the direct continuous analogue of BB84, requires squeezed states of light. The sender (Alice) chooses to encode a Gaussian value into the x-displacement of an x-squeezed state, or similarly for the quadrature p. 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, however, has never been implemented in the laboratory because the need for squeezed states makes it impractical.

An important progress was then made by the group of one of the authors (PG), who proposed a **coherent-state** CV-QKD protocol building upon these previous squeezed-state proposals [6]. The breakthrough was to explicitly establish a secure protocol using Gaussian-modulated coherent states of light, which can be easily generated with a laser. In this protocol, Alice modulates both x and p quadratures of a coherent state. Bob again measures one of them, and publicly discloses which one, so the corresponding quadrature is kept by Alice to make a correlated pair. The security of the protocol against individual Gaussian attacks was proven by using the concept of "equivalent noise" referred to the input, which is common in electronics and has been used previously in the context of quantum non-demolition measurements in optics (see [4]). The security criterion is then very simple: the equivalent noise variance N of the transmission line, evaluated at the line input, cannot exceed one shot-noise unit: $N < 1$. This condition is actually equivalent to limit on CV quantum cloning, that is, the best attack would be the optimal Gaussian cloning machine that is depicted in **Figure 1**.

An important observation is that the equivalent noise variance includes two contributions, namely the "vacuum noise" $(1–T)/T$, which is due to the losses in a line of transmission T, and the "excess noise" $\varepsilon = N – (1–T)/T$, which may be due for instance to spontaneous emission from an in-line amplifier. The security criterion $N \leq 1$ can then be equivalently written as $\varepsilon < 2 – 1/T$. In the ideal case of a lossy but noiseless line, the security thus requires that $T > 1/2$ (i.e., more than half the intensity has to reach the receiver). This limit, known as the **3dB-loss limit,** was first thought to be generic to CV-QKD. It was quickly realized, however, that it 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). A similar technique, known as **reverse reconciliation**, was shown to be applicable to continuous variables, so that the key distribution remains secure for any value of the line transmission [4]. 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 advantage to Alice and Bob. A related technique to beat the 3-dB loss limit is to carry out a post-selection by putting a threshold on Bob's data. However, the security of such post-selection protocols is not well established yet, since the best eavesdropping strategy has not been studied so far.

Experimental demonstration

A table-top experimental demonstration of this coherent-state continuous-variable protocol with reverse reconciliation was reported in [4] (see **Figure 2**). The setup 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 an homodyne detection. An essential ingredient to make this protocol practical lies in the ability to efficiently extract secret bits from correlated strings of continuous data, and simultaneously to correct errors without revealing

too much information to Eve. A method for achieving this goal, named **sliced reconciliation,** was proposed by the group of one of the authors (NC). 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 90% of Shannon's limit. 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 3.1dB loss. These rates are quite significant when compared to photon-counting QKD, and they open very interesting perspectives for coherent states CV-QKD. The table-top experiment shown in **Figure 2** may straightforwardly be transposed to telecom wavelength (1550 nm) by using only standard telecom components. A significant advantage is that the setup does not need sophisticated devices such as single-photon sources or counters.

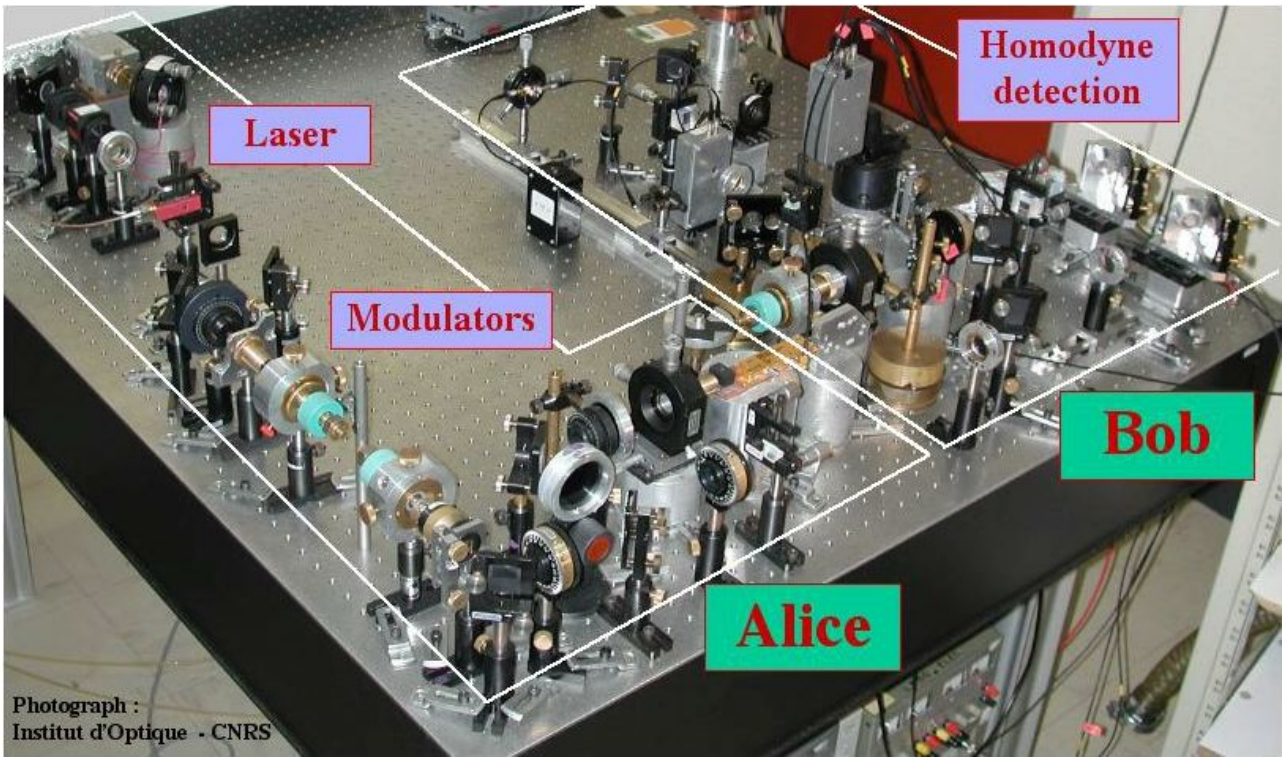

Figure 2

Security proofs

The first security proof on direct [6] and reverse [4] reconciliation protocols only considered 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 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. 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. This **virtual entanglement**, also known for photon-counting QKD, is very useful for establishing security proofs. In particular, it implies that there is an **entanglement-breaking limit** in continuous-variable protocols, corresponding to an intercept-and-resend attack, which gives $\varepsilon < 2$. This means that when the excess noise exceeds two shot-noise units, no secure communication is possible

More restrictive security limits can actually be established. For an entanglement-based protocol using reverse reconciliation, the security bound becomes $\varepsilon < 1$. For a coherent-state protocol, the bound is $\varepsilon < 2 - 1/T$ for direct reconciliation, and $\varepsilon < 1/2 - 1/T + (1/T^2 + 1/4)^{1/2}$ 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 **Figure 3**, assuming fiber losses of 0.2 dB/km. Curve (a) is the entanglement-breaking attack ($\varepsilon = 2$), curve (b) is obtained with the entangled-beam reverse-reconciled protocol ($\varepsilon=1$), while the last two curves correspond to coherent-state protocols using either direct (c) or reverse (d) reconciliation.

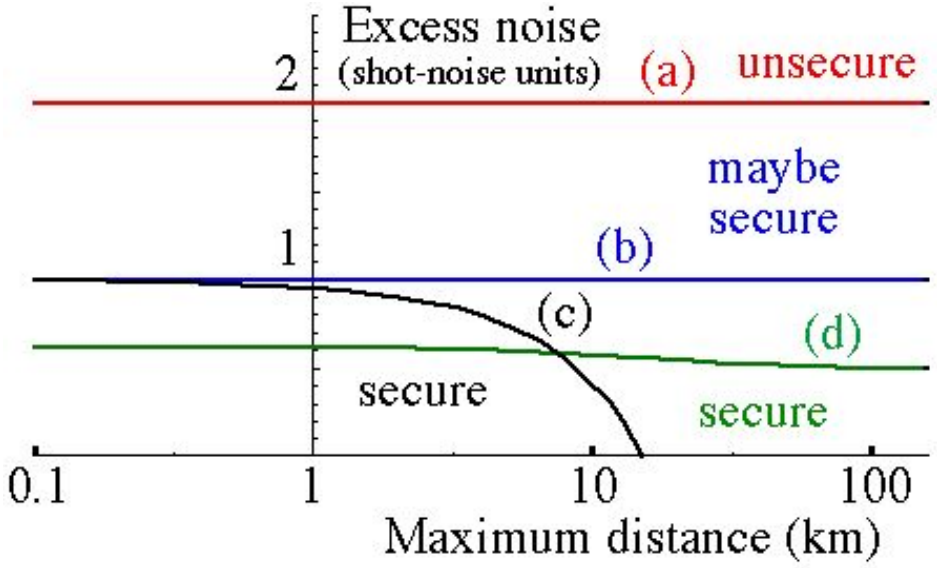

Figure 3

Interestingly, it can be shown by using entropic Heisenberg relations that the individual Gaussian attacks are actually the best possible attacks against reverse-reconciled protocols [7]. 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 that 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 must use a Gaussian modulation for exchanging data because this modulation maximizes the entropy for a given variance. In that respect, using any kind of discrete modulation of the signal will be less efficient, a fact which further justifies the Gaussian encoding scheme.

Progresses have also been made in the direction of **unconditional security**, first by extending the well-known unconditional security proof of Gottesman and Preskill. In short, the idea is to show that squeezing, which is required in the Gottesman-Preskill proof, is used only to evaluate the channel's error rate, and can actually be replaced by a channel tomography procedure using only coherent states [8]. This approach shows that unconditional security of coherent-state QKD is achievable, although it guarantees a much lower secret bit rate than in [4] because the used encoding scheme is far less efficient than a Gaussian modulation. Other security proofs, based upon general information-theoretic arguments, have also been published very recently.

Conclusions

As a conclusion, 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-reconciled coherent-state protocols 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 for reverse-reconciled CV-QKD, and they both lead to a fundamental decrease in the secret bit rate. As illustrated in **Figure 3**, the maximum tolerable excess noise for coherent-states CV-QKD decreases with the distance, which is what eventually puts a limit on the achievable security on long distances.

The experiments realized so far are table-top proof-of-principle experiments. Nevertheless, it must be pointed out that coherent-state CV-QKD can be implemented by using only standard optical telecommunications equipment, without the need for dedicated photon sources or single photon counters. Several experiments are presently under way to characterize such systems in the telecom domain. Like with photon-counting QKD, several options are available: the pulses can be sent one way in an optical fiber, or may be retro-reflected using Faraday mirrors, or may be sent in free space by using a polarization variant of the basic scheme. These various possibilities are presently investigated in several European laboratories (namely Orsay, Geneva, and Erlangen) in the framework of the **Integrated Project SECOQC**.

Ultimately, losses will be a limitation for CV-QKD protocols for practical reasons, just like they are for photon-counting protocols. One may then consider building "quantum repeaters", based on CV entanglement distillation procedures. A first step in that direction is to learn how to manipulate CV non-Gaussian states, which are a required ingredient for CV entanglement distillation. This was recently achieved by the group of one of the authors (PG) [9]. All these recent developments, both on the theoretical and experimental side, clearly indicate that quantum continuous variables are a promising tool for the future of Quantum Information Processing and Communications.

List of terms and acronyms

CV: continuous variable
QIPC: quantum information processing and communication
CV-QIPC: continuous-variable quantum information processing and communication
QKD: quantum key distribution
CV-QKD: continuous-variable quantum key distribution
LO: local oscillator
BB84: quantum key distribution protocol due to Bennett and Brassard in1984

References

[1] A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science 282, 706 (1998).
[2] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurasek, and E.S. Polzik, Nature 432, 482 (2004).
[3] U.L. Andersen, V. Josse, and G. Leuchs, http://arxiv.org/abs/quant-ph/0501005
[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, Nature 421, 238 (2003).
[5] N.J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. 85, 1754 (2000).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).
[7] F. Grosshans and N.J. Cerf, Phys. Rev. Lett. 92, 047905 (2004).
[8] S. Iblisdir, G. Van Assche, and N.J. Cerf, Phys. Rev. Lett. 93, 170502 (2004).

[9] J. Wenger, R. Brouri, and P. Grangier, Phys. Rev. Lett. 92, 153601 (2004).

Projects funded by the European Commission and related to the work in this article:

QUICOV
Quantum Information with Continuous Variables
Start date: 01/01/2000
End date: 31/06/2003
Project web site: http://kerr.physik.uni-erlangen.de/quicov/
Contact Person: Gerd Leuchs, Universität Erlangen-Nurnberg, leuchs@physik.uni-erlangen.de

COVAQIAL
Continuous Variable Quantum Information with Atoms and Light
Start date: 01/09/2004
End date: 31/08/2007
Project web site: http://www.ulb.ac.be/project/covaqial/
Contact Person: Nicolas Cerf, Université Libre de Bruxelles, nicolas.cerf@ulb.ac.be

SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography
Start date: 01/04/2004
End date: 31/03/2008
Project web site: http://www.secoqc.net/
Contact Person: Christian Monyk, ARC Seibersdorf research GmbH, christian.monyk@arcs.ac.at

Contact information of the authors of this article:
Nicolas Cerf
Ecole Polytechnique
Université Libre de Bruxelles
50 avenue F. D. Roosevelt, CP 165
1050 Bruxelles
Belgium
Email: nicolas.cerf@ulb.ac.be
Web page: http://quic.ulb.ac.be

Philippe Grangier
Quantum Optics Group
Laboratoire Charles Fabry de l'Institut d'Optique
Bâtiment 503, Centre Universitaire
91403 Orsay
France
Email: philippe.grangier@iota.u-psud.fr
Web page: http://www.iota.u-psud.fr/~grangier/Optique_quantique.html