ISSN 2427-4577

BULLETIN N° 271
ACADÉMIE EUROPÉENNE INTERDISCIPLINAIRE DES SCIENCES
INTERDISCIPLINARY EUROPEAN ACADEMY OF SCIENCES

Lundi 13 novembre 2023 à 14h30

ASSEMBLÉE GÉNÉRALE ANNUELLE DE L'AEIS

Notre Prochaine séance aura lieu le lundi 4 Décembre 2023 de 15h à 17h
Salle Annexe Amphi Burg
Institut Curie, 12 rue Lhomond – 75005 Paris

Elle sera consacrée, à 15h précises à :

Conférence :

« COMMUNICATIONS SÉCURISÉES AVEC DES VARIABLES QUANTIQUES CONTINUES »

Par Philippe GRANGIER
Directeur de recherche CNRS
Laboratoire Charles Fabry, Institut d'Optique Graduate School,
CNRS, Université Paris-Saclay, Palaiseau, France

ACADÉMIE EUROPÉENNE INTERDISCIPLINAIRE DES SCIENCES

INTERDISCIPLINARY EUROPEAN ACADEMY OF SCIENCES

Novembre 2023

N°271

TABLE DES MATIERES

Prochaine séance : lundi 4 décembre 2023 à 15h précises

Conférence :

« COMMUNICATIONS SÉCURISÉES AVEC DES VARIABLES QUANTIQUES CONTINUES »

Par Philippe GRANGIER
Directeur de recherche CNRS
Laboratoire Charles Fabry, Institut d'Optique Graduate School,
CNRS, Université Paris-Saclay, Palaiseau, France

ACADÉMIE EUROPÉENNE INTERDISCIPLINAIRE DES SCIENCES
INTERDISCIPLINARY EUROPEAN ACADEMY OF SCIENCES

Séance du Lundi 13 novembre 2023

La séance est ouverte à 14h30, **sous la Présidence de Victor MASTRANGELO**

- **Étaient présents physiquement nos Collègues membres titulaires** de Paris Jean BERBINAU, Anne BURBAN**,** Eric CHENIN**,** Jean-Félix DURASTANTI, Françoise DUTHEIL, Michel GONDRAN, Irène HERPE-LITWIN, Paul Louis MEUNIER, Jean SCHMETS et Jean-Pierre TREUIL
- **Étaient excusés physiquement pour raisons de santé nos Collègues** Gilbert BELAUBRE et Gilles COHEN-TANNOUDJI,
- **Avaient donné leur procuration pour les élections :**

BELAUBRE Gilbert	à MASTRANGELO Victor
BOBIN Jean-Louis	à DUTHEIL Françoise
COHEN-TANNOUDJI Gilles	à MASTRANGELO Victor
ELSAESSER Wolfgang	à CHENIN Éric
OLIVERIO Alberto	à MASTRANGELO Victor
PERRIER Edith	à CHENIN Éric
PUMAIN Denise	à HERPE-LITWIN Irène

I. ASSEMBLÉE GÉNÉRALE DE l'AEIS pour l'Année 2023

Notre Président Victor MASTRANGELO procède à l'ouverture de l'Assemblée générale.

A. Rapports moraux et d'activités des diverses sections

Les sections de NANCY, REIMS et PARIS nous ont communiqué leurs rapports d'activités et moraux. Soumis au vote des Collègues présents et représentés, les rapports sont adoptés à l'unanimité des votants ou représentés. Il en a été de même du rapport financier fourni par notre Collègue Françoise DUTHEIL.

B. Election du nouveau bureau pour l'année 2023-2024

Se présentent comme candidats aux diverses fonctions :

Fonction	Candidat
Président	Victor MASTRANGELO
Vice-Présidente	Édith PERRIER
Secrétaire général	Éric CHENIN
Secrétaire générale adjointe	Irène HERPE-LITWIN
Trésorière générale	Françoise DUTHEIL
Edition	Robert FRANCK
Relations européennes	Jean SCHMETS
Relations avec l'AX	Gilbert BELAUBRE
Ville de Paris et Région IDF	Michel GONDRAN et Jean BERBINAU
Moyens Multimédias et Universités	Moyens Multimédia : Eric CHENIN Relations Universités : Victor MASTRANGELO

Recrutements	Paul-Louis MEUNIER coordinateur, Jean BERBINAU, Anne BURBAN, Christian GORINI, Jacques PRINTZ
Thèmes et Programmes de Colloque	Jean SCHMETS et Johanna HENRION-LATCHÉ
Synthèses scientifiques et Publications AEIS	Jean-Pierre TREUIL, Marie-Françoise PASSINI
Grands organismes de recherche nationaux et internationaux	Michel SPIRO
Mécénat	Jean Félix DURASTANTI coordinateur, Jean BERBINAU, Anne BURBAN

Se présentent comme Conseillers scientifiques au titre de l'année 2023-2024

Disciplines	**Candidats**
Sciences de la Matière	Gilles COHEN-TANNOUDJI
Sciences de la Vie-Biotechnologies	Ernesto Di MAURO

L'ensemble des candidatures est adopté à l'unanimité des présents et représentés.

C. Elections des membres consultatifs du CONSEIL D'ADMINISTRATION

Se présentent en tant que membres consultatifs du Conseil d'Administration

Membres consultatifs du Conseil d'Administration	Gilbert BELAUBRE Michel GONDRAN

D. Présidents de section élus (appartenant statutairement au bureau)

Section	**Élu**
Nancy-Luxembourg	Sylvie PIERRE
Reims	Johanna HENRION-LATCHÉ
Section associée Athènes (Grèce)	Anastassios METAXAS

REMERCIEMENTS
Nous tenons à remercier vivement Mr Yann TRAN et Mme Annabelle POIRIER de l'Institut Curie pour la qualité de leur accueil.

Documents

Communications sécurisées avec des variables quantiques continues.

Philippe Grangier
Laboratoire Charles Fabry, Institut d'Optique Graduate School,
CNRS, Université Paris-Saclay, Palaiseau, France
philippe.grangier@institutoptique.fr

Résumé

Comme on le sait depuis Planck et Einstein au début du 20e siècle, la lumière doit être décrite par la physique quantique, et elle possède des propriétés à la fois discrètes et continues. Nous résumerons d'abord notre description actuelle de ces propriétés la lumière, et présenterons un outil intéressant pour les représenter intuitivement, la fonction de Wigner.

Une application bien connue de la lumière quantique est la distribution quantique de clés secrètes (QKD), ou cryptographie quantique, qui s'est beaucoup développée ces dernières années. Cependant, la QKD reste une technologie techniquement exigeante et coûteuse, et plusieurs directions sont actuellement explorées pour résoudre ces difficultés. Nous présenterons en détail l'une d'entre elles, la cryptographie quantique à variables continues (CVQKD) [1-4], qui est beaucoup plus proche des techniques de télécommunication optique standard que la QKD à variables discrètes (DV). En particulier, la CVQKD n'utilise pas de compteurs de photons, mais des détections cohérentes (homodynes ou hétérodynes), qui sont désormais très courantes dans les systèmes de télécommunications commerciaux à haut débit [4].

Finalement, nous présenterons quelques tentatives actuelles de mise en place de réseaux quantiques, qui visent à surmonter les pertes de canaux de transmission, notamment par des nœuds de confiance, des satellites ou des répéteurs quantiques. Dans une perspective à plus long terme, nous discuterons également la possibilité de réaliser des interactions déterministes entre photons individuels [5].

References

[1] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, P. Grangier, Nature 421, 238 (2003).
[2] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Nature Photon. 7, 378 (2013).
[3] E. Diamanti and A. Leverrier, Entropy 17, 6072 (2016).
[4] F. Roumestan et al, https://arxiv.org/abs/2207.11702 (2022)
[5] J. Vaneecloo, S. Garcia, A. Ourjoumtsev, Phys. Rev. X 12, 021034 (2022)

Secure communications with quantum continuous variables.

As it has been known since the beginning of the 20th century, light must be described by quantum physics, and it has both discrete and continuous properties. We will first summarize our current description of these properties, and introduce a nice tool for representing them intuitively, that is the Wigner function.

A well-known application of quantum light is quantum key distribution (QKD), which has been developing quite a lot in the recent years. However, QKD remains a technically demanding and costly technology, and various directions are currently explored to improve on this issue. In particular, we will present in details one of them, continuous variable (CV) QKD [1-4], which is much closer to standard optical telecommunication techniques than discrete variable (DV) QKD. In particular, CVQKD does not use photon counters, but coherent (homodyne or heterodyne) detections, which are now very usual in high-speed commercial telecom systems [4].

In a last part we will present current attempts towards quantum networks, which aim at overcoming channel losses by various ways including trusted nodes, satellites, or quantum repeaters. As a look to the future, we will also discuss the possibility to achieve deterministic photon-photon interactions [5].

Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution

Francois Roumestan,[1,2] Amirhossein Ghazisaeidi,[1] Jérémie Renaudier,[1] Luis Trigo Vidarte,[3] Anthony Leverrier,[4] Eleni Diamanti,[2] and Philippe Grangier[5]

[1]*Nokia Bell Labs, Paris-Saclay, route de Villejust, F-91620 Nozay, France*
[2]*Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France*
[3]*ICFO - Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, Castelldefels (Barcelona) 08860, Spain*
[4]*Inria Paris, 2 rue Simone Iff, F75589 Paris Cedex 12, France*
[5]*Université Paris-Saclay, IOGS, CNRS, Laboratoire Charles Fabry, F-91127 Palaiseau, France*

Quantum key distribution (QKD) enables the establishment of secret keys between users connected via a channel vulnerable to eavesdropping, with information-theoretic security, that is, independently of the power of a malevolent party[1]. QKD systems based on the encoding of the key information on continuous variables (CV), such as the values of the quadrature components of coherent states[2,3], present the major advantage that they only require standard telecommunication technology. However, the most general security proofs for CV-QKD required until now the use of Gaussian modulation by the transmitter, complicating practical implementations[4–6]. Here, we experimentally implement a protocol that allows for arbitrary, Gaussian-like, discrete modulations, whose security is based on a theoretical proof that applies very generally to such situations[7]. These modulation formats are compatible with the use of powerful tools of coherent optical telecommunication, allowing our system to reach a performance of tens of megabit per second secret key rates over 25 km.

Driven by the pressing need for high-security solutions to address risks to cybersecurity posed by rapid technological progress, the development of quantum key distribution (QKD) systems has advanced significantly in recent years[8–10]. A major challenge in this direction is to leverage the high potential of techniques that have been developed with great success for the classical telecommunication industry, with the goal of both enhancing the performance of QKD systems and assuring their smooth integration into deployed fibre optic network infrastructures. Continuous-variable (CV) QKD schemes[3,11] are particularly well suited for this purpose. The key feature of such schemes is that dedicated photon-counting technology required in standard single-photon based schemes can be replaced by coherent detection techniques that are widely used in classical optical communications. This hardware simplification, however, comes at the price of a more involved theoretical analysis, and security proofs typically require the transmitter, commonly called Alice, to prepare coherent states with a Gaussian modulation to be sent to the receiver, Bob. Such a modulation has been used for advanced experimental implementations[4–6], but is not a common industrial practice; a more practical approach is to send coherent states chosen from a finite constellation in phase space. Although such discrete modulations were considered early in CV-QKD[12–14], sound security proofs have been developed only recently, for protocols with either very large constellation sizes[15] or very small ones[16–19], with some experimental implementations in the latter case[20,21]. But the most interesting format of medium-size quadrature amplitude modulation (QAM) used in classical optical communications remained out of reach for these methods, which rely on solving huge convex optimization problems. This outstanding issue was solved in Ref.[7], which provided an analytical bound for the asymptotic secret key rate of protocols with arbitrary modulation schemes, including probabilistic constellation shaping (PCS) QAM[22]. Strictly speaking, this bound is not tight, but it becomes essentially so for any QAM of size greater than 64.

Here, we experimentally demonstrate CV-QKD with PCS 64-QAM and 256-QAM that can reach very high peak secret key rate (SKR) with standard hardware and software compatible with current telecommunication systems[23,24]. We emphasize that our choice of modulation format presents a number of advantages in practice: the use of QAM ensures the need for a smaller number of random numbers and leads in principle to more efficient post-processing, pulse shaping requires a smaller bandwidth, and PCS optimizes the mutual information bringing it closer to Shannon channel capacity. Our results thus open the way towards integrating CV-QKD in standard optical communication systems, in an efficient, transparent, and cost-efficient way.

CV-QKD protocol and security proof. In the Prepare-and-Measure (PM) coherent state CV-QKD protocol with discrete modulation, Alice prepares coherent states $|\alpha\rangle = |(p+iq)/2\rangle$, chosen at random from a discrete constellation. She sends them through an optical link to Bob who measures them using coherent detection.This quantum transmission phase is followed by classical post-processing, in which Alice and Bob compare a randomly

chosen fraction of their data to estimate the channel parameters and thus the length of the final key. Then they correct errors through a reconciliation step and finally turn their identical data set into a shorter secret key via privacy amplification.

The security of this PM protocol is analysed through an equivalent Entanglement-Based (EB) protocol[3], where Alice (virtually) prepares an initial entangled state, measures one mode and transmits the second mode to Bob through the quantum channel. Exploiting the property that Gaussian states maximize the Holevo information between Bob's measurement outcome and the eavesdropper quantum memory[25–27], it is sufficient to compute the covariance matrix of the bipartite state shared by Alice and Bob before measurement. The difficulty is that this virtual state is never prepared nor measured in the true PM protocol. Rather, the goal is for Alice and Bob to infer this covariance matrix from the data they observe in the PM protocol.

While this task is straightforward when the modulation is Gaussian[4,6,11], it is much more involved in the case of a discrete modulation. There, one needs to solve a semidefinite program whose dimension scales both with the constellation size and the dimension of the relevant Hilbert space – infinite for CV protocols. Even if it is possible to truncate the Fock space to a relevant subspace[28], this numerical approach quickly becomes untractable as soon as the constellation size exceeds 10. The main contribution of Ref.[7] is to provide an analytical formula for the covariance matrix, depending only on easily measurable quantities in the PM protocol, namely the variance of Bob's measurement result and two correlation coefficients between Alice and Bob's data. This will be analyzed further below.

PCS QAM for CV-QKD. The probabilistic constellation shaping with quadrature amplitude modulation (PCS QAM) is a standard modulation method[29], involving a discretized Gaussian probability distribution $\pi_{k,l}$ given by

$$\alpha_{k,l} = \alpha_0(k + il) \tag{1}$$

$$\pi_{k,l} = \frac{\exp(-\nu|\alpha_{k,l}|^2)}{\sum_{k,l}\exp(-\nu|\alpha_{k,l}|^2)}, \tag{2}$$

where $k + il$ are the points of a standard QAM constellation, and $\nu > 0$ and $\alpha_0 > 0$ are free parameters such that $\sum_{k,l}\pi_{k,l}|\alpha_{k,l}|^2 = V_A/2$. Here, V_A is the variance of Alice's modulation, measured in shot-noise units (SNU), *i.e.*, such that the variance of the shot noise equals one. Since PCS QAM are commonly used in modern high-rate coherent optical transmission systems, very efficient digital signal processing techniques have been developed. Moreover, PCS QAM are good candidates for discrete modulation with near optimal SKR, thanks to their Gaussian-like distribution[30]. When using PCS QAM, it is crucial to optimize the free parameter ν to maximize the SKR. Using numerical calculation, we observed that the optimal value depends only on Alice's modulation variance V_A. In the following, both V_A and ν are chosen to maximize the SKR for either 64-QAM or 256-QAM modulations, as displayed on Fig. 1.

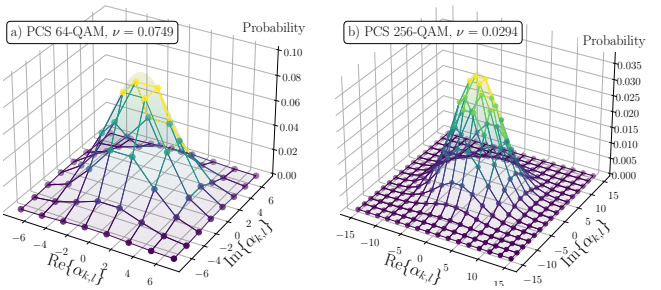

Figure 1: Constellation probability distributions for (a) PCS 64-QAM with $\nu = 0.0749$, and (b) PCS 256-QAM with $\nu = 0.0294$. In both cases bottom units are $\sqrt{SNU}$ and $\alpha_0 = 2\sqrt{SNU}$. Connecting lines and equivalent Gaussian distributions are depicted for clarity. The free parameter ν appears in the discretized Gaussian probability distribution describing the constellation, and its optimization is crucial for the maximization of the SKR.

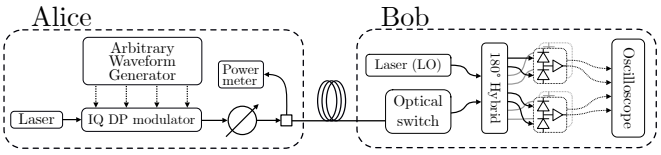

Figure 2: Experimental setup. The setup only involves off-the-shelf, state-of-the-art telecom equipment. The 1550-nm laser has a 10 kHz nominal linewidth. The Arbitrary Waveform Generator feeds the dual-polarization in-phase-and-quadrature (DP-IQ) modulator with four 600 MBaud signals with Root Raised Cosine (RRC) pulse shape. An optical power meter and an attenuator at the output of Alice are used to monitor V_A. Bob uses a 180 degrees hybrid to interfere the signal with the local oscillator (LO) and a set of four amplified balanced photodetectors, whose outputs are sampled using a real-time oscilloscope and processed by offline digital signal processing. At the input of Bob, a microelectromechanical optical switch is used to periodically turn off the signal to perform shot noise measurements for noise calibration.

Experimental implementation. The main idea behind the development of the experimental system in our work is to use only commercially available, latest generation telecom equipment in order to provide a convenient cost-efficient solution. Important requirements that we sought for were high resolution, low noise and a bandwidth of at least 1 GHz. The setup is shown in Fig. 2. Alice generates coherent states using a 1550 nm tunable laser source with nominal 10 kHz linewidth (Pure Photonics). A dual polarization (DP) in-phase-and-quadrature (IQ) modulator (Fujitsu) is used to modulate the phase and amplitude of the laser beam. The analog inputs of the

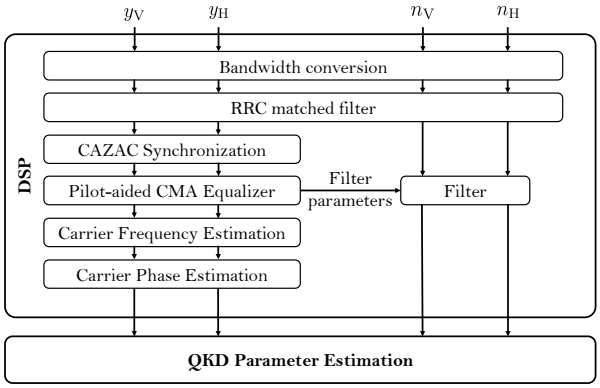

Figure 3: Bob's digital signal processing building blocks. DSP consists in a combination of digital filter matching the pulse shape of input symbols y_H, y_V, auto-correlation for retrieving the time-multiplexed pilots used in our experiments, a pilot-aided adaptive equalizer technique, and finally carrier frequency and phase estimation algorithms. It is then possible, by using the transmitted data together with noise calibration data n_H, n_V that have undergone the same processing, to estimate the secret key rate.

DP-IQ modulator are fed with the output of an Arbitrary Waveform Generator (AWG) with 5 GS/s sampling rate and 14 bits nominal resolution. The AWG outputs four 600 MBaud signals with Root Raised Cosine (RRC) pulse shape[29]. At the output of Alice's lab, an optical power meter and an optical attenuator are used to monitor V_A. Bob uses a 180 degrees hybrid to interfere the signal with the phase reference (or local oscillator, LO), which is generated with a laser identical to Alice's. Four amplified balanced photodetectors convert the received optical signal to an analog electronic signal, which is then sampled using a 1 GHz real-time oscilloscope with 5 GS/s sampling rate and 12 bits nominal resolution. The sampled waveforms are stored for offline digital signal processing (DSP, see below). In the present experiment, the memory and writing speed of the oscilloscope impose to perform noise calibration and parameter estimation one acquisition at a time, but in a full-scale implementation the oscilloscope and offline DSP would be replaced by a continuously running receiver with real-time DSP.

Digital signal processing. The implementation of DSP suitable for CV-QKD is one of the most important practical challenges of this work. The main building blocks are shown in Fig. 3. The algorithm inputs four sampled waveforms $y_1(k)$, $y_2(k)$, $y_3(k)$, $y_4(k)$, with an average number of samples per transmitted symbol $\bar{n}_{\mathrm{sps}} = 8.3$ (calculated by dividing the 5 GS/s sampling rate with the 600 Mbaud symbol rate). The waveforms are then assembled into two complex waveforms $y_H(k) = y_1(k) + jy_2(k)$ and $y_V(k) = y_3(k) + jy_4(k)$. If the signal is single-side band (see details in Methods), it is converted into a baseband signal by a digital frequency shift, and a digital filter matching the pulse shape is applied; a root raised cosine (RRC) filter in our case. Then, we use a constant amplitude zero autocorrelation waveform (CAZAC) sequence[31] to compute the auto-correlation on the signal in order to retrieve the beginning of the time-multiplexed pilot sequence used in our implementation. The next steps are to correct linear impairments using a pilot-aided CMA adaptive equalizer[32] (see details in Methods), and to apply carrier frequency and carrier phase estimation algorithms. Finally, using the noise calibration symbols, denoted as n_H and n_V in Fig. 3, which undergo the same DSP operations, QKD parameters are estimated to compute the achievable secret key rate.

These algorithms are obviously unable to perfectly correct channel impairments, and the DSP imperfections may result in apparent channel excess noise. Therefore it is crucial to optimize the various DSP parameters to minimize excess noise, ideally for each individual run of the experiment producing a block of data. In this work, the optimization procedure has been performed offline, after signal acquisition, and is described in Methods.

Noise calibration measurements. Most of the CV-QKD parameters are expressed in SNU. However, Bob effectively measures samples U of an electrical tension expressed in volts; see Methods for a description of the required calibration procedure. We note that the LO intensity and thus the shot noise may vary during the experiment, making it necessary to periodically reiterate the procedure of recording shot noise samples as often as possible. For this purpose, Bob's setup includes an optical switch used to turn on and off the signal light coming from Alice. This procedure is repeated once every minute. Finally, the normalized value V_B of Bob's variance can be written as

$$V_B = 1 + \eta T V_A/2 + V_{\mathrm{el}} + \xi_B, \tag{3}$$

where T is the channel transmission efficiency, and ξ_B is the excess noise measured at Bob's site, to be evaluated by Alice and Bob. The quantum efficiency and electronic noise of Bob's detectors, which in our experiment take the values $\eta = 0.65$ and $V_{\mathrm{el}} = 0.1$, respectively, are supposed here to be known to the legitimate users and cannot be modified by Eve.

Non-Gaussian attacks. Recall that in our protocol, which follows the security proof of Ref.[7], Alice and Bob should not in fact evaluate T and ξ_B from the data, but rather three parameters, denoted as c_1, c_2 and n_B. Under the assumption of a Gaussian channel these parameters are simply related to T and ξ_B, and to the parameters defining the constellation[33]. However, the Gaussian channel assumption is not justified for an arbitrary attack by Eve on a discrete modulation, and c_1, c_2 and n_B must be evaluated directly. As a consequence, the SKR, related to the Holevo quantity, is a function $f(c_1, c_2, n_B)$, instead of the usual $g(T, \xi_B)$; see Ref.[33].

Fiber	Modulation	ν	V_A[SNU]	ξ_B[mSNU]	SKR[Mbps]
9.5 km SMF-28	64-QAM	0.0688	5.32	0.197	60.2
	256-QAM	0.0362	7.11	0.132	91.8
25 km EX3000	64-QAM	0.0460	4.20	1.170	0.0
	256-QAM	0.0380	6.53	0.900	24.0

Table I: Modulation variance V_A (in SNU), indicative excess noise ξ_B (in mSNU) and SKR calculated using the security proof of Ref.[7] including finite-size effects (in Mbps), for PCS 64-QAM and PCS 256-QAM, during 1 hour of experiment, with 9.5 km of SMF-28 and 25 km of EX3000 fiber. The block size is $N = 5 \times 10^6$.

Under our experimental conditions, we found the effective channel to be very well described by a Gaussian model, and we observe $f(\hat{c}_1, \hat{c}_2, \hat{n}_B) \simeq g(\hat{T}, \hat{\xi}_B)$. However, the direct evaluation of these formulas with the estimators ignores finite-size effects. In order to take them into account, we evaluate the formulas with worst-case estimators[7], *i.e.*, we rather compute $f(\hat{c}_1^{\min}, \hat{c}_2^{\min}, \hat{n}_B^{\max})$, which is less favorable than $g(\hat{T}^{\min}, \hat{\xi}_B^{\max})$ for a Gaussian channel. This is the procedure followed to obtain the results provided in Table I, which correspond to a rigorous implementation of the protocol with the security proof for a discrete modulation[33].

Results. Our experiment was performed with either 9.5 km of SMF-28 or 25 km of EX3000 fiber. The 25 km fiber link has a total loss of 4.3 dB. In each case the most critical DSP parameters are optimized to minimize the excess noise. In the present implementation the system operates with acquisitions of length 20 ms from which, after processing, $N = 5 \times 10^6$ QKD symbols are used for parameter estimation. Finally, the DSP optimization process is performed on a subset of 12 acquisitions.

Figure 4 shows the estimated SKR for the 9.5 km SMF-28 fiber, for PCS 64 and 256-QAM. The estimation is based on the proof for an arbitrary modulation protocol[7], assuming $\beta = 0.95$[34], and using worst-case estimators with $N = 5 \times 10^6$ and security parameter $\epsilon = 10^{-10}$, following Refs.[35–37]. Table I summarizes the results with modulation variance V_A values (in SNU), excess noise ξ_B values (in SNU), which are included as an indication of system performance, and SKR (in Mbps) calculated following the aforementioned procedure.

We can achieve a secret key rate of ~ 92 Mbps over 9.5 km and 24 Mbps over 25 km, using PCS 256-QAM format, averaged over 100 transmission blocks of $N = 5 \times 10^6$ QKD symbols. PCS 64-QAM gives lower performance, as theoretically expected. The expected behavior as a function of distance is shown in Fig. 5. By comparison with the current state of the art[5,6,9,10,24], these results confirm the high performance reached by our system by adopting techniques from standard optical communication and following the security proof for discrete modulation, including finite-size effects.

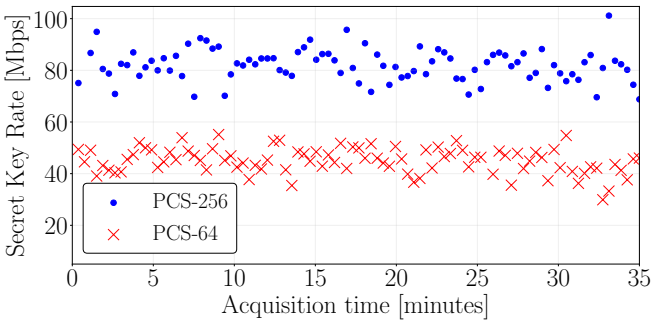

Figure 4: Estimated secret key rate for each block of acquired data, plotted as a function of the acquisition time, for PCS 64 and 256-QAM, with 9.5 km SMF-28 link.

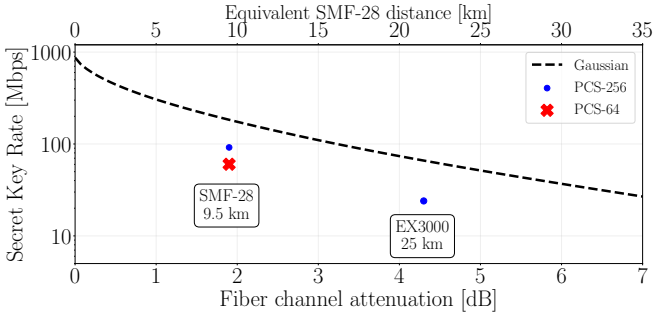

Figure 5: Experimental results of secret key rate as a function of the channel attenuation and distance considering finite-size effects and neglecting post-processing times. Two modulation formats (PCS-64 and PCS-256) and two fibers have been used in this experiment; a 9.5 km standard single mode fiber (SMF-28) with attenuation coefficient 0.2 dB/km and a 25 km EX3000 fiber with attenuation coefficient 0.172 dB/km. PCS-64 modulation at 25 km does not yield a positive key rate. The expected SKR of a setup with Gaussian modulation in the asymptotic regime is plotted for comparison, assuming the same repetition rate $R = 600$ MBaud, $\xi_B = 0.5$ mSNU, and Alice using the optimal V_A. The block size is $N = 5 \times 10^6$.

Conclusion. The laboratory experiment presented in this work opens interesting avenues towards faster and more flexible implementations of CV-QKD, within the standard environment of high bit rate coherent telecommunications. It leverages in particular industry-grade digital signal processing techniques that have been minimally modified for the CV-QKD implementation. To take full advantage of these improvements, it would be necessary to also improve the speed of data post-processing, which should be facilitated by the use of discrete constellations.

METHODS

Pilot amplitude and rate. To correctly retrieve the low signal-to-noise ratio QKD symbols, the DSP relies on QPSK (that is 4-QAM) pilot symbols with a higher

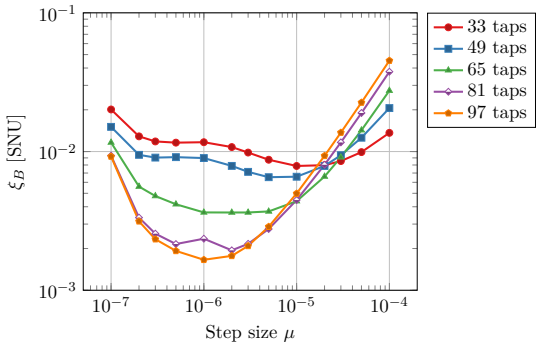

Figure 6: Excess noise ξ_B vs. step size μ and number of taps of adaptive equalizer, averaged over 12 acquisitions of PCS 256-QAM signal and 25 km of EX3000 fiber.

power, which needs to be optimized before signal acquisition. This is done by acquiring QKD signals with various values of the pilot amplitude, and applying the DSP to estimate the excess noise. Using such experimental tests, the pilot over QKD symbol power ratio was adjusted to 14 dB. The same optimization should be performed for the pilot rate. Contrary to pilot amplitude, the criterion to optimize the pilot rate is not the excess noise. In fact, if an increase of the pilot rate decreases the excess noise, it also decreases the rate of QKD symbols. Hence, we need to optimize directly the SKR. Using again an experimental optimization, we fixed the pilot rate to 4 pilots over 8 symbols, *i.e.*, half of the transmitted symbols are actually pilots.

Adaptive equalizer. For each experiment, we want to find the DSP parameters that minimize the excess noise. Since the DSP is performed offline, we can do a brute force optimization for the most relevant parameters, on a few acquisitions. To start with, we jointly optimize two parameters of the adaptive equalizer for polarization demultiplexing[38]: n_{taps}, number of taps, and μ, the step size. For each couple (n_{taps}, μ) under test, the DSP is applied to 12 different acquisitions. Figure 6 shows the average excess noise for all the tested (n_{taps}, μ), for experimental PCS 256-QAM data obtained in conditions slightly different than those presented in the main text. We observe that the lowest values of excess noise are achieved with 97 taps and a step size μ of 10^{-6}.

Signal conditioning. We observed the presence of low frequency components of the excess noise, below 20 MHz, that we attribute to cutoff frequencies of the hardware as well as additive noise stemming from the electrical line. To avoid these perturbations, the outputs of the AWG are digitally upshifted such that the signal has no frequency component in the noisy region. In particular, the 600 MBaud signal with RRC pulse shape and roll-off factor 0.4, corresponding to a bandwidth of 840 MHz, is upshifted by 500 MHz such that the useful bandwidth extends from 80 MHz to 920 MHz. The baudrate and roll-off factor have to be jointly optimized to minimize the excess noise. Furthermore, as noted above, the ratio of the QPSK pilots power relatively to the QAM symbols power has to be optimized to minimize the excess noise.

Noise calibration. Since Bob effectively measures samples U of an electrical tension expressed in volts, and obtains variances $\text{Var}(U)$ in V^2, he needs to estimate the quantity N_0, namely the variance of the shot noise expressed in V^2. When disconnecting the signal input of the receiver, the output of the receiver is the sum of the shot noise and the electronic noise; therefore Bob can measure $\text{Var}(U) = N_0(1 + V_{\text{el}})$, where V_{el} is the variance of the receiver's electronic noise in SNU. Then, disconnecting the LO input, Bob measures only the electronic noise, $\text{Var}(U') = N_0 V_{\text{el}}$ and $N_0 = \text{Var}(U) - \text{Var}(U')$.

This procedure gives four different values $N_0^{(1)}$, $N_0^{(2)}$, $N_0^{(3)}$, and $N_0^{(4)}$, one for each channel of the oscilloscope. In practice, the samples measured on a channel are a mixture of the quadratures of the coherent states sent by Alice, that are recovered only after the DSP. This comes from several channel impairments such as polarization rotation or carrier phase noise. As a consequence, if the $N_0^{(i)}$ are not all equal, they do not correspond to the variances of the shot noise on the quadratures effectively transmitted by Alice. To tackle this issue, we apply to the shot noise samples the same DSP correction as to the signal itself, and estimate the variances afterwards. In other words, the DSP operations applied to the signal samples are simultaneously applied to the noise samples.

Signal averaging. Our use of a worst-case estimator is justified if the fluctuations observed on the parameters are of a statistical nature. Given that all 5×10^6 data points within a data block are very close in time (total acquisition time 20 ms), the population variance can be considered sufficiently close to the theoretical variance to assume that fluctuations on the excess noise measurement are essentially of statistical nature. Therefore, the use of the worst-case estimator for the excess noise can be considered acceptable to take into account finite-size effects on the security of the protocol, although a more rigorous theoretical treatment of finite-size issues remains desirable.

ACKNOWLEDGMENTS

This research was supported by the E.C. projects CiViQ and OpenQKD, with a contribution by the Paris Region project ParisRegionQCI. F.R. was supported by a CIFRE PhD grant.

1. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

2. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
3. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **6072**, 17 (2015).
4. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photon.* **7**, 378 (2013).
5. Zhang, Y. *et al.* Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
6. Jain, N. *et al.* Practical continuous-variable quantum key distribution with composable security. *arXiv:2110.09262 [quant-ph]* (2021).
7. Denys, A., Brown, P. & Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* **5**, 540 (2021).
8. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quant. Inf.* **2**, 16025 (2016).
9. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012 (2020).
10. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
11. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238 (2003).
12. Lorenz, S. *et al.* Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using post-selection. *Phys. Rev. A* **74**, 042326 (2006).
13. Leverrier, A. & Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **102**, 180504 (2009).
14. Leverrier, A. & Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A* **83**, 042312 (2011).
15. Kaur, E., Guha, S. & Wilde, M. M. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Phys. Rev. A* **103**, 012412 (2021).
16. Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **9**, 021059 (2019).
17. Lin, J., Upadhyaya, T. & Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **9**, 041064 (2019).
18. Lin, J. & Lütkenhaus, N. Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. *Phys. Rev. Appl.* **14**, 064030 (2020).
19. Matsuura, T., Maeda, K., Sasaki, T. & Koashi, M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature Comm.* **12**, 252 (2021).
20. Hirano, T. *et al.* Implementation of continuous-variable quantum key distribution with discrete modulation. *Quant. Sci. Tech.* **2**, 024010 (2017).
21. Wang, P., Liu, J., Lu, Z., Wang, X. & Li, Y. Discrete-modulation continuous-variable quantum key distribution with high key rate. *arXiv:2112.00214 [quant-ph]* (2021).
22. Ghazisaeidi, A. *et al.* Advanced c+l-band transoceanic transmission systems based on probabilistically shaped pdm-64qam. *J. Lightwave Tech.* **35**, 1291 (2017).
23. Roumestan, F. *et al.* High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In *European Conference on Optical Communication (ECOC)* (Bordeaux, France, 2021). Doi:10.1109/ECOC52684.2021.9606013t.
24. Pan, Y. *et al.* Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Opt. Lett.* **47**, 3307 (2022).
25. Wolf, M. M., Giedke, G. & Cirac, J. I. Extremality of gaussian quantum states. *Phys. Rev. Lett.* **96**, 080502 (2006).
26. García-Patrón, R. & Cerf, N. J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
27. Navascués, M., Grosshans, F. & Acín, A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
28. Upadhyaya, T., van Himbeeck, T., Lin, J. & Lütkenhaus, N. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. *PRX Quantum* **2**, 020325 (2021).
29. Proakis, J. & Salehi, M. *Digital Communications* (McGraw-Hill Higher Education, 2007).
30. Roumestan, F. *et al.* Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution. In *Optical Fiber Communication (OFC)* (Washington, United States, 2021). Paper F4E.1.
31. Milewski, A. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM Journal of Research and Development* **27**, 426 (1983).
32. Faruk, M. S., Mori, Y., Zhang, C., Igarashi, K. & Kikuchi, K. Multiimpairment monitoring from adaptive finite-impulse-response filters in a digital coherent receiver,. *Opt. Express* **18**, 26929 (2010).
33. Roumestan, F. *Advanced signal processing techniques for optical fiber continuous-variable quantum key distribution systems.* Ph.D. thesis, Sorbonne Université (2022). Available online at https://tel.archives-ouvertes.fr/tel-03707442v1.
34. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
35. Scarani, V. & Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100**, 200501 (2008).
36. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).
37. Jouguet, P., Kunz-Jacques, S., Diamanti, E. & Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **86**, 032309 (2012).
38. Kikuchi, K. Fundamentals of coherent optical fiber communications. *J. Lightwave Technol.* **34**, 157–179 (2016).

Grosshans, F., Assche, G. V., Wenger, J., Cerf, R. B. J. & Grangier, P. Quantum key distribution using gaussian-modulated coherent states. Nature 421, 238-241

Article *in* Nature · February 2003

DOI: 10.1038/nature01289 · Source: PubMed

Quantum key distribution using gaussian-modulated coherent states*

Frédéric Grosshans,[a] Gilles Van Assche,[b] Jérôme Wenger,[a]
Rosa Brouri,[a] Nicolas J. Cerf,[b] and Philippe Grangier[a]

[a] *Laboratoire Charles Fabry de l'Institut d'Optique, CNRS UMR 8501, 91403 Orsay, France*
[b] *École Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

(Dated: 16 January 2003)

Quantum continuous variables [1] are being explored [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14] as an alternative means to implement quantum key distribution, which is usually based on single photon counting [15]. The former approach is potentially advantageous because it should enable higher key distribution rates. Here we propose and experimentally demonstrate a quantum key distribution protocol based on the transmission of gaussian-modulated coherent states (consisting of laser pulses containing a few hundred photons) and shot-noise-limited homodyne detection; squeezed or entangled beams are not required [13]. Complete secret key extraction is achieved using a reverse reconciliation [14] technique followed by privacy amplification. The reverse reconciliation technique is in principle secure for any value of the line transmission, against gaussian individual attacks based on entanglement and quantum memories. Our table-top experiment yields a net key transmission rate of about 1.7 megabits per second for a loss-free line, and 75 kilobits per second for a line with losses of 3.1 dB. We anticipate that the scheme should remain effective for lines with higher losses, particularly because the present limitations are essentially technical, so that significant margin for improvement is available on both the hardware and software.

Much interest has arisen recently in using the electromagnetic field amplitudes to obtain possibly more efficient quantum continuous variable (QCV) alternatives [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14] to the usual photon-counting quan tum key distribution (QKD) techniques (see ref. [15] and references therein) — for instance, by using "non-classical" light beams [2, 3, 4, 5, 6, 7, 8, 9, 10, 11]. In fact, it was shown in ref. [13] that squeezed or entangled light is not required to achieve this goal: an equivalent level of security may be obtained by transmitting "quasi-classical" coherent states. When the line transmission is larger than 50 % (line loss $\leq$ 3 dB), the physical limits on QCV cloning [16, 17, 18] ensure that this protocol is secure against individual attacks. This corroborates the fact that QKD only requires non-orthogonal states, and may well work with macroscopic signals instead of single photons [19]. There are in principle various way s for the partners Alice and Bob to distribute keys beyond this 3 dB limit, for instance by using entanglement purification [20] or post-selection [12]. Therefore these QCV schemes stimulate many fundamental questions about the physical origin of QKD security. As will be shown below, cryptographic security appears to have a strong relationship with entanglement, even though our protocol does not rely on entangled states.

Here we introduce and implement a coherent-state QKD protocol, and we demonstrate that it is, in principle, secure for any value of the line transmission. It relies on the distribution of a gaussian key [7] obtained by continuously modulating the phase and amplitude of coherent light pulses [13] at Alice's side, and subsequently performing homodyne detection at Bob's side. The continuous data are then converted into a common binary key via a specifically designed reconciliation algorithm [8, 10]. The security against arbitrarily high losses is achieved by reversing the reconciliation protocol, that is, Alice attempts to guess what was received by Bob rather than Bob guessing what was sent by Alice. Such a reverse reconciliation protocol [14] gives Alice an advantage over a potential eavesdropper Eve, regardless of the line loss. The practical limitations of our scheme are essentially technical, and appear to be due mostly to the limited efficiency of the reconciliation software.

The protocol runs as follows [13]. First, Alice draws two random numbers x_A and p_A from a gaussian distribution of mean zero and variance $V_A N_0$, where N_0 denotes the shot-noise variance. Then, she sends the coherent state $|x_A + ip_A\rangle$ to Bob, who randomly chooses to measure either quadrature x or p. Later, using a public authenticated channel, he informs Alice about which quadrature he measured, so she may discard the irrelevant data. After many similar exchanges, Alice and Bob (and possibly the eavesdropper Eve) share a set of correlated gaussian variables, which we call "key elements".

Classical data processing is then necessary for Alice and Bob to obtain a fully secret binary key. First, Alice and Bob publicly compare a random sample of their key elements to evaluate the error rate and transmission efficiency of the quantum channel. From the observed correlations, Alice and Bob evaluate the amount of information they share ($I_{AB} = I_{BA}$) and the maximum information Eve may have obtained (by eavesdropping) about their values (I_{AE} and I_{BE}). It is known that Alice and Bob can, in principle, distil from their data a common secret key of size $S > \sup(I_{AB} - I_{AE}, I_{BA} - I_{BE})$ bits per

*Published in *Nature (London)* **421**, 238-241 (16 January 2003).

key element [21, 22]. This requires classical communication over an authenticated public channel, and may be divided into two steps : reconciliation (that is, correcting the errors while minimizing the information revealed to Eve) and privacy amplification (that is, making the key secret). As we deal here with continuous data, we developed a "sliced" reconciliation algorithm [8, 10] to extract common bit strings from the correlated key elements. In order to reconcile Bob's measured data with Alice's sent data, the most natural way to proceed is that Bob gets R extra bits of information from Alice in order to correct the transmission errors. The corresponding direct reconciliation (DR) protocols, which have been used so far in QCV QKD [7, 13], allow the generation of a common string of $I_{AB} + R$ bits, of which Eve may know up to $I_{AE} + R$ bits. Here we rather consider reverse reconciliation (RR) protocols [14], where Bob sends R bits of information to Alice so that she incorporates the transmission errors in her initial data. These RR protocols allow the generation of a common string of $I_{BA} + R$ bits, of which Eve may know $I_{BE}+R$ bits. This turns out to be particularly well suited to QCV QKD, because it is more difficult for Eve to control the errors at Bob's side than to read Alice's modulation. The last step of key extraction, namely privacy amplification, consists of filtering out Eve's information by properly mixing the reconciled bits to spread Eve's uncertainty over the entire final key. This procedure requires an estimate of Eve's information on the reconciled key, so we need a bound on I_{AE} for DR, or I_{BE} for RR. In addition, Alice and Bob must keep track of the information publicly revealed during reconciliation. This knowledge is destroyed at the end of the privacy amplification procedure, reducing the key length by the same amount. The DR bound [13] on I_{AE} implies that the security cannot be warranted if the line transmission G is below 50%. We will now establish the RR bound on I_{BE}, and show that it is not associated with a minimum value of G.

In a RR scheme, Eve needs to guess Bob's measurement outcome without adding too much noise on his data. This can be done via an "entangling cloner", which creates two quantum-correlated copies of Alice's quantum state, so Eve simply keeps one of them while sending the other to Bob. Let $(x_{\rm in}, p_{\rm in})$ be the input field quadratures of the entangling cloner, and (x_B, p_B), (x_E, p_E) the quadratures of Bob's and Eve's output fields. To be safe, we must assume Eve uses the best possible entangling cloner compatible with the parameters of the Alice-Bob channel: Eve's cloner should minimize the conditional variances [23, 24] $V(x_B|x_E)$ and $V(p_B|p_E)$, that is, the variances of Eve's estimates of Bob's field quadratures (x_B, p_B). These variances are constrained by Heisenberg-type relations (see Appendix A), which limit what can be obtained by Eve:

$$\begin{aligned} V(x_B|x_A)V(p_B|p_E) &\geq N_0^2 \\ V(p_B|p_A)V(x_B|x_E) &\geq N_0^2 \end{aligned} \tag{1}$$

where $V(x_B|x_A)$ and $V(p_B|p_A)$ denote Alice's conditional variances. This means that Alice and Eve cannot jointly know more about Bob's conjugate quadratures than is allowed by the uncertainty principle. Now, Alice's variances can be bounded by using the measured parameters of the quantum channel, which in turn makes it possible to bound Eve's variances.

The channel is described by the linear relations $x_B = G_x^{1/2}(x_{\rm in} + B_x)$ and $p_B = G_p^{1/2}(p_{\rm in} + B_p)$, with $\langle x_{\rm in}^2 \rangle = \langle p_{\rm in}^2 \rangle = VN_0 \geq N_0$, $\langle B_{x,p}^2 \rangle = \chi_{x,p} N_0$, and $\langle x_{\rm in} B_x \rangle = \langle p_{\rm in} B_p \rangle = 0$. Here χ_x, χ_p represent the channel noises referred to its input, called equivalent input noises [23, 24], while G_x, G_p are the channel gains in x and p, and V is the variance of Alice's field quadratures in shot-noise units ($V = V_A + 1$). The output-output correlations of the entangling cloner, described by $V(x_B|x_E)$ and $V(p_B|p_E)$, depend only on the density matrix $D_{\rm in}$ of the input field $(x_{\rm in}, p_{\rm in})$, and not on the way it is produced, namely whether it is a gaussian mixture of coherent states or one of two entangled beams. Inequalities (1) thus have to be fulfilled for all physically allowed values of $V(x_B|x_A)$ and $V(p_B|p_A)$, given $D_{\rm in}$. Therefore, the values of $V(x_B|x_A)$ and $V(p_B|p_A)$ that should be used in inequalities (1) to limit Eve's knowledge are the minimum values Alice might achieve by using the maximal entanglement compatible with V, namely (see Appendix A)

$$\begin{aligned} V(x_B|x_A)_{\rm min} &= G_x(\chi_x + V^{-1})N_0 \\ V(p_B|p_A)_{\rm min} &= G_p(\chi_p + V^{-1})N_0 \end{aligned} \tag{2}$$

These lower bounds are thus directly connected with entanglement, even though Alice does not use it in practice. They may be compared with the actual values when Alice sends coherent states, that is, $V(x_B|x_A)_{\rm coh} = G_x(\chi_x + 1)N_0$ and $V(p_B|p_A)_{\rm coh} = G_p(\chi_p + 1)N_0$. The lower bounds on Eve's conditional variances are then obtained from equations (1) and (2), as:

$$\begin{aligned} V(p_B|p_E) &\geq N_0/\{G_x(\chi_x + V^{-1})\} \\ V(x_B|x_E) &\geq N_0/\{G_p(\chi_p + V^{-1})\} \end{aligned} \tag{3}$$

A physical realization of an entangling cloner reaching these bounds is sketched in ref. [14].

To assess the security of the RR scheme, one assumes that Eve's ability to infer Bob's measurement can reach the limit put by inequalities (3). For simplicity, we consider the channel gains and noises and the signal variances to be the same for x and p (in practice, deviations should be estimated by statistical tests). The information rates can be derived using Shannon's theory for gaussian additive-noise channels [25], giving

$$\begin{aligned} I_{BA} &= (1/2)\log_2[V_B/(V_{B|A})_{\rm coh}] \\ &= (1/2)\log_2[(V+\chi)/(1+\chi)] \qquad (4a) \\ I_{BE} &= (1/2)\log_2[V_B/(V_{B|E})_{\rm min}] \\ &= (1/2)\log_2[G^2(V+\chi)(V^{-1}+\chi)] \qquad (4b) \end{aligned}$$

expressed in bits per symbol (or per key element). Here $V_B = \langle x_B^2 \rangle = \langle p_B^2 \rangle = G(V + \chi)N_0$ is Bob's variance, $(V_{B|E})_{\rm min} = V(x_B|x_E)_{\rm min} = V(p_B|p_E)_{\rm min} =$

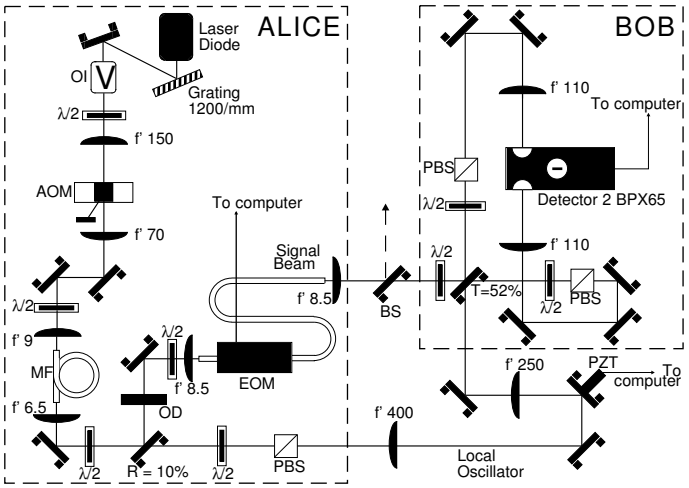

FIG. 1: Experimental set-up. Laser diode, SDL 5412 (780 nm); OI, optical isolator; $\lambda/2$, half-wave plate; AOM, acousto-optic modulator; MF, polarization maintaining single-mode fibre; OA, optical attenuator; EOM, electro-optic amplitude modulator; PBS, polarizer; BS, beam splitter; PZT, piezoelectric transducer. Focal lengths (f') are given in millimetres. R and T are reflection and transmission coefficients.

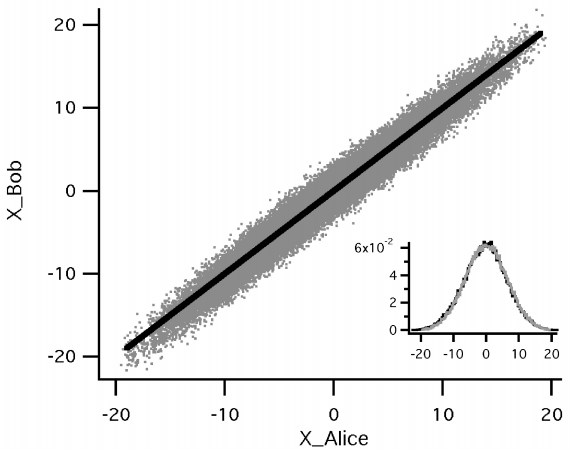

FIG. 2: Bob's measured quadrature as a function of the amplitude sent by Alice (in Bob's measurement basis) for a burst of 60,000 pulses. The line transmission is 100% and the modulation variance is V = 41.7. The solid line represents the expected unity slope. Inset, the corresponding histograms of Alice's (grey curve) and Bob's (black curve) data.

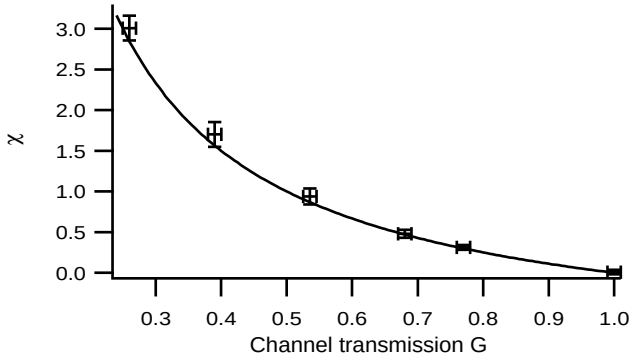

FIG. 3: Channel equivalent noise χ_{line} as a function of line transmission G. The curve is the theoretical prediction $\chi_{\text{vac}} = (1-G)/G$. The errors bars include two contributions with approximately the same size, from statistics (evaluated over blocks of 60,000 pulses) and systematics (calibration errors and drifts).

$N_0/\{G(\chi + V^{-1})\}$ is Eve's minimum conditional variance, and $(V_{B|A})_{\text{coh}} = V(x_B|x_A)_{\text{coh}} = V(p_B|p_A)_{\text{coh}} = G(\chi+1)N_0$ is Alice's conditional variance for a coherent-state protocol. The secret bit rate of a RR protocol is thus

$$\begin{aligned} \Delta I_{RR} &= I_{BA} - I_{BE} \\ &= -(1/2)\log_2[G^2(1+\chi)(V^{-1}+\chi)] \end{aligned} \quad (5)$$

and the security is guaranteed if $\Delta I_{RR} > 0$. The equivalent input noise χ can be split into a "vacuum noise" component due to the line losses, given by $\chi_{\text{vac}} = (1-G)/G$, and an "excess noise" component defined as $\epsilon = \chi - \chi_{\text{vac}}$. In the high-loss limit ($G \ll 1$), the RR protocol remains secure if $\epsilon < (V-1)/(2V) \approx 1/2$, that is, if the amount of excess noise ϵ is not too large. In contrast, a DR protocol requires low-loss lines, as the security is warranted only if $\chi < 1$, that is, if $G > 1/(2-\epsilon)$. Note that DR tolerates an excess noise up to $\epsilon \approx 1$, so it might be preferred to RR for low-loss but noisy channels.

Our experimental implementation (Fig. 1) of the quantum key exchange uses 120-ns coherent pulses at a 800-kHz repetition rate (wavelength of 780 nm, see Appendix A). Data bursts of 60,000 pulses have been analysed (Fig. 2). For each burst, a subset of the values are disclosed to evaluate the transmission G and the total added noise variance. The output noise has four contributions: the shot noise N_0, the channel noise $\chi_{\text{line}}N_0$, the electronics noise of Bob's detector ($N_{\text{el}} = 0.33N_0$), and the noise due to imperfect homodyne detection efficiency ($N_{\text{hom}} = 0.27N_0$). When introducing line losses using a variable attenuator, the measured χ_{line} increases as $(1-G)/G$, as shown in Fig. 3 ($\epsilon_{\text{line}} = 0$ here). The two detection noises N_{el} and N_{hom} originate from Bob's detection system, so they must be taken into account when estimating I_{BA}. In contrast, we may reasonably assume that Eve cannot know or control the corresponding fluctuations, so her attack is inferred on the basis of the line noise χ_{line} only (see Appendix B for details). Figure 4 shows explicitly the mutual information between all parties, which makes straightforward the comparison between the DR and RR protocols.

We wrote a computer program that implements the reconciliation algorithm followed by privacy amplification (see Appendices A and B). Although Alice and Bob are not spatially separated in the present set-up, the analysed data have the same structure as in a realistic cryp-

V	G_{line}	Losses (dB)	I_{BA} (bit)	I_{BE} (% I_{BA})	I_{rec} (% I_{BA})	Ideal RR rate (kbit s^{-1})	Practical RR rate (kbit s^{-1})	Ideal DR rate (kbit s^{-1})	Practical DR rate (kbit s^{-1})
41.7	1	0	2.39	0	88	1,920	1,690	1,910	1,660
38.6	0.79	1.0	2.17	58	85	730	470	540	270
32.3	0.68	1.7	1.93	67	79	510	185	190	–
27	0.49	3.1	1.66	72	78	370	75	0	–
43.7	0.26	5.9	1.48	93	71	85	–	0	–

TABLE I: **Ideal and practical net secret key rates.** The parameters of the quantum key exchange are measured for several values of the channel transmission G (the corresponding losses are also given in decibels). The variations of the variance V of Alice's field quadrature are due to different experimental adjustments. The information I_{BA} is given in bits per time slot. Also shown are the maximum information gained by Eve (I_{BE}) and the extracted information by reverse reconciliation (I_{rec}). The ideal secret key bit rates would be obtained from our measured data with perfect key distillation that yields exactly $I_{BA} - I_{BE}$ bits (RR) or $I_{AB} - I_{AE}$ bits (DR), whereas the practical secret key bit rates are the one achieved with our current key distillation procedure ("–" means that no secret key is generated). Both bit rates are calculated over bursts of about 60,000 pulses at 800 kHz, not taking into account the duty cycle ($\sim 5\%$) in the present set-up.

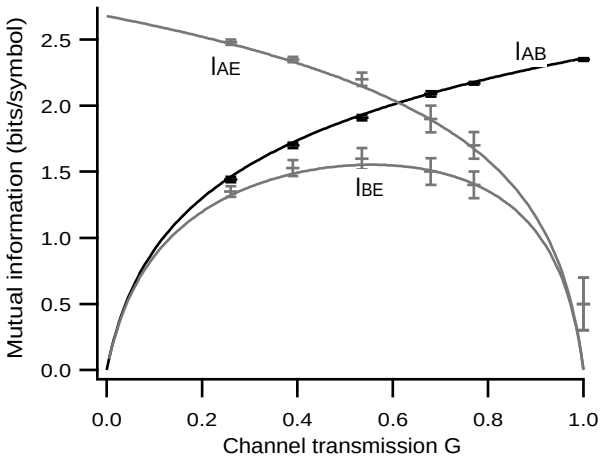

FIG. 4: Values of I_{BA}, I_{BE}, and I_{AE} as a function of the line transmission G for $V \approx 40$. Here, I_{BA} is given by equation (4a), including all transmission and detection noises for evaluating V_B and $(V_{B|A})_{\text{coh}}$. The expression for I_{BE} is given by equation (4b), using the same V_B and $(V_{B|E})_{\min} = N_0/\{G(\chi_{\text{line}} + V^{-1})\} + N_{\text{el}} + N_{\text{hom}}$. This expression realistically assumes that Eve cannot know the noises N_{el} and N_{hom}, which are internal to Bob's detection set-up. For comparison with DR, the value of I_{AE} is also plotted (the theoretical value of I_{AE} is obtained from ref. [13]).

tographic exchange. Table I shows the ideal and practical net key rates of our reverse QKD protocol, as well as the DR values for comparison. The RR scheme is efficient for any value of G provided that the reconciliation protocol achieves the limit given by I_{BA}. However, unavoidable deviations of the algorithm from Shannon's limit reduce the actual reconciled information I_{rec} between Alice and Bob, while I_{BE} is of course assumed unaffected. For high modulation ($V \approx 40$) and low losses, the reconciliation efficiency lies around 80%, which makes it possible to distribute a secret key at a rate of several hundreds of kilobits per second. However, the achievable reconciliation efficiency drops when the signal-to-noise ratio decreases, but this can be improved by reducing the modulation variance, which increases the ratio I_{BA}/I_{BE}. Although the ideal secret key rate is then lower, we could process the data with a reconciliation efficiency of 78% for $G = 0.49$ (3.1 dB) and $V = 27$, resulting in a net key rate of 75 kbits s^{-1} (see also Appendix A). This clearly demonstrates that RR continuous-variable protocols operate efficiently at and beyond the 3 dB loss limit of DR protocols. We emphasize that this result is obtained despite the fact that the evaluated reconciliation cost is higher for RR than for DR: the better result for RR is essentially due to its initial "quantum advantage".

In photon-counting QKD, the key rate is limited by the single-photon detectors, in which the avalanche processes are difficult to control reliably at very high counting rates. In contrast, homodyne detection may run at frequencies up to tens of MHz. In addition, a specific advantage of the high dimensionality of the QCV phase space is that the field quadratures can be modulated with a large dynamics, allowing the encoding of several key bits per pulse (see Table I). Very high secret bit rates are therefore attainable with our coherent-state protocol on low-loss lines. For high-loss lines, our protocol is at present limited by the reconciliation efficiency, but its intrinsic performances remain very high. Since most of the limitations of the present proof-of-principle experiment appear to be of a technical nature, there is still a considerable margin for improvement, both in the hardware (increased detection bandwidth, better homodyne efficiency, lower electronic noise), and in the software (better reconciliation algorithms [26] , see Appendix A). In conclusion, the way seems open for implementing the present proposal at telecommunications wavelengths as a practical, high bit-rate, quantum key distribution scheme over long distances.

Acknowledgements. The contributions of J. Gao to early stages of the experiment, and of K. Nguyen to the software development, are acknowledged. We thank S. Iblisdir for discussions, and Th. Debuisschert for the loan

of the 780 nm integrated modulator. This work was supported by the EU programme IST/FET/QIPC (projects "QUICOV" and "EQUIP"), the French programmes ACI Photonique and ASTRE, and by the Belgian programme ARC.

Correspondence and requests for materials should be addressed to Philippe Grangier (e-mail philippe.grangier@iota.u-psud.fr).

APPENDIX A: METHODS

Relevant Heisenberg relations

In a RR protocol, Alice's estimator for x_B and Eve's estimator for p_B can be denoted respectively as αx_A and βp_E, where α, β are real numbers. The corresponding errors are $x_{B|A,\alpha} = x_B - \alpha x_A$, and $p_{B|E,\beta} = p_B - \beta p_E$. Because Alice's, Bob's, and Eve's operators commute, we have $[x_{B|A,\alpha}, p_{B|E,\beta}] = [x_B, p_B]$, and thus the Heisenberg relation $\Delta x^2_{B|A,\alpha} \Delta p^2_{B|E,\beta} \geq N_0^2$. Defining the conditional variances as $V(x_B|x_A) = \min_\alpha\{\Delta x^2_{B|A,\alpha}\}$ and $V(p_B|p_E) = \min_\beta\{\Delta p^2_{B|E,\beta}\}$, we obtain $V(x_B|x_A)V(p_B|p_E) \geq N_0^2$, or, by exchanging x and p, $V(p_B|p_A)V(x_B|x_E) \geq N_0^2$.

Alice has the estimators (x_A, p_A) for the field $(x_{\rm in}, p_{\rm in}) = (x_A + A_x, p_A + A_p)$ that she sends, with $\langle A_x^2\rangle = \langle A_p^2\rangle = sN_0$. Here s measures the amount of squeezing possibly used by Alice in her state preparation [14], with $s \geq V^{-1}$ for consistency with Heisenberg's relations. By calculating $\langle p_A^2\rangle = (V - s)N_0$, $\langle p_B^2\rangle = G_p(V + \chi_p)N_0$, $\langle p_A p_B\rangle = G_p^{1/2}\langle p_A^2\rangle$, we obtain the conditional variance $V(p_B|p_A) = \langle p_B^2\rangle - |\langle p_A p_B\rangle|^2/\langle p_A^2\rangle = G_p(s + \chi_p)N_0$. This equation and the constraint $s \geq V^{-1}$ gives $V(p_B|p_A) \geq G_p(V^{-1} + \chi_p)N_0$, and similarly $V(x_B|x_A) \geq G_x(V^{-1} + \chi_x)N_0$. The bound on $V_{B|A}$ is thus obtained by assuming that Alice may use squeezed or entangled beams, while the bound on $V_{B|E}$ can only be achieved if Eve uses an entangling attack. This reflects the fact that squeezing or entanglement play a crucial role in our security demonstration, even though the protocol implies coherent states. Our security proof addresses individual gaussian attacks only, but as the entangling cloner attack saturates the Heisenberg uncertainty relations, we conjecture that it encompasses all incoherent (non-collective) eavesdropping strategies.

Experimental set-up

A continuous-wave laser diode at 780 nm wavelength associated with an acousto-optic modulator is used to emit 120-ns (full-width at half-maximum) pulses at a 800 kHz rate. The signal pulses contain up to 250 photons, while the local oscillator (LO) power is 1.3×10^8 photons per pulse. The amplitude of each pulse is arbitrarily modulated by an integrated electro-optic modulator. However, owing to the unavailability of a fast phase modulator at 780 nm, the phase is not randomly modulated but scanned continuously. No genuine secret key can be distributed, strictly speaking, but random permutations of Bob's data are used to provide realistic data (see Appendix B). The data are organized in bursts of 60,000 pulses, separated by synchronization periods also used to lock the phase of the LO. The overall homodyne detection efficiency is 0.81, due to the optical transmission (0.92), the mode-matching efficiency (0.96) and the photodiode quantum efficiency (0.92). For the critical data at 3 dB loss, the mode-matching efficiency was improved to 0.99, and thus the overall efficiency was 0.84. We also point out that many blocks of data were exchanged around the 3 dB loss point, with a typical rate above 55 kbit $\rm s^{-1}$.

Secret key distillation

A common bit string is extracted from the continuous data by sequentially reconciling several strings ("slices") of binary functions of the gaussian key elements, applying a binary reconciliation protocol successively on each bit [8, 10]. Here, we used five slices, each being corrected either by a trivial one-way protocol (communicating the bits) when the bit error rate (BER) is high, or by the two-way protocol Cascade [27, 28] when the BER is low. Note that the disclosed slices are useful for reconciling the remaining slices with less information leaking to Eve, even though they of course do not yield secret bits as such. In addition, Alice and Bob encrypt their classical messages using the one-time pad scheme with a fraction of the previous key bits, or a bootstrap key for the first block. For slices corrected with Cascade, the exchanged parities are encrypted with the same key bits on both sides [29], making Eve aware of the differences between Alice's and Bob's parities (that is, the error positions) but not of their individual values. Fully communicated slices are also encrypted, thereby revealing no information at all to Eve. Still, Eve may exploit the interactivity of Cascade and gain some information on the final key by combining her knowledge of the error positions with that of the correlations between Alice's and Bob's gaussian values. In the present protocol, this information is numerically calculated for an entangling cloner attack, and then destroyed by privacy amplification. This is achieved by appropriate "hashing" [30] functions (see Appendix B). The resulting net secret key rate is then obtained by subtracting, from the raw key rate, the cost of the one-time pad encryption and the error-position information. Finally, let us emphasize that sliced reconciliation can be made very close to a one-way protocol by increasing the number of key elements from which the bits are jointly extracted (multidimensional reconciliation [8]). This approach was not implemented here, but should deliver an improved secret key rate, approaching the value from the Csiszár-Körner formula [21, 22].

APPENDIX B: SUPPLEMENTARY INFORMATION

Experimental set-up

The source consists of a CW laser diode (SDL 5412) at 780 nm associated with an acousto-optic modulator, used to chop pulses with a duration 120 ns (full width at half-maximum), at a repetition rate 800 kHz. To reduce the excess noise, a grating-extended external cavity is used, and the beam is spatially filtered using a single mode fiber. Light pulses are then split onto a beam-splitter, one beam being the local oscillator (LO), the other Alice's signal beam. The data is organised in bursts of 60,000 pulses, separated by time periods used to lock the phase of the LO, and sequences of pulses to synchronize the parties. In the present experiment, there is a burst every 1.6 seconds, corresponding to a duty cycle of about 5%, which is obviously under-optimised but should be easy to improve in further experiments.

The coherent state distribution is generated by modulating both the amplitude and phase of the light pulses with the appropriate probability law. In the present experiment, the amplitude of each pulse is arbitrarily modulated at the nominal 800 kHz rate by an integrated electro-optic LiNbO3 Mach-Zehnder interferometer. In contrast, due to the unavailability of a fast phase modulator at 780 nm, the phase is not randomly modulated but scanned continuously from 0 to 2π using a piezoelectric transducer (PZT). For such a deterministic phase variation, the security of the protocol is not warranted, and thus no genuine secret key could be distributed strictly speaking. However, the experiment provides realistic data, having exactly the awaited structure provided that random phase permutation on Bob's data are performed.

Due to an imbalance between the paths of the interferometer which modulates the amplitude of the signal beam, the extinction is not strictly zero. In the present experiment that is only aimed at a proof of principle, we subtract the offset field from the data received by Bob. In a real cryptographic transmission, the offset field should be compensated by Alice, either by adding a zeroing field, or by using a better modulator.

All voltages for the electro-optic modulator or the PZT are generated by an acquisition board (National Instruments PCI6111E) connected to a computer. Although all discussions assume the modulation to be continuous, digitised voltages are used in practice. With our experimental parameters, a resolution of 8 bits is enough to hide the amplitude or phase steps under the shot noise. Since the modulation voltage is produced using a 16 bits converter, and the data is digitised over 12 bits, we may fairly assume the modulation and measurement to be continuous.

The homodyne detection was checked to be shot-noise limited for LO power up to 5×10^8 photons/pulse. In the present experiment, we used 1.3×10^8 photons/pulse for LO power, while each signal pulse contains up to 250 photons. Depending on the run, the overall detection efficiency is either 0.81 or 0.84, due to optical transmission (0.92), mode-matching visibility (0.96 or 0.99) and photodiode quantum efficiency (0.92).

The experiment is thus carried out in such a way that all useful parameters can be measured experimentally. Reconciliation and privacy amplification protocols can thus be performed in realistic – though not fully secret – conditions. The limitations of the present set-up are essentially due to the lack of appropriate fast amplitude and phase modulators at 780 nm. This should be easily solved by operating at telecom wavelengths (1540-1580 nm) where such equipment is readily available. Let us point out also that it is not convenient to transmit separately the signal and LO, so a better solution would be to use a frequency sideband technique similar to Mérolla et al. [31]. Then all light pulses are transmitted together along the same fibre, and a separate radio-frequency is sent from Alice to Bob in order to reconstruct the optical phase information.

Hypothesis about the detector's noise : "realistic" vs "paranoid" assumptions

After the quantum exchange, Alice and Bob reveal a subset of their values taken randomly to evaluate the transmission G and the total added noise variance. This variance has four contributions: the shot noise N_0, the channel noise $\chi_{\text{line}} N_0$, the electronics noise of Bob's detector ($N_{\text{el}} = 0.33 N_0$), and the noise due to imperfect homodyne detection efficiency ($N_{\text{hom}} = 0.27 N_0$). The two detection noises N_{el} and N_{hom} originate from Bob's detection system, so one may reasonably assume that they do not contribute to Eve's knowledge. This "realistic" assumption has been followed in the article. In that case, the noise from Bob's detection system also affects Eve's information so, in equation (4b), we take $(V_{B|E})_{\min} = N_0/\{G_{\text{line}}(\chi_{\text{line}}+V^{-1})\}+N_{\text{el}}+N_{\text{hom}}$, where G_{line} stands for the line transmission.

In contrast, in a "paranoid" approach, one should assume that the noises N_{el} and N_{hom} are also controlled by Eve, that gives her a supplementary advantage. In that case, $(V_{B|E})_{\min}$ will be given by $N_0/\{G(\chi+V^{-1})\}$, where G now includes both the line and detection efficiencies and χ includes both the line and detection noises. In all cases, the value of I_{BA} is given by equation (4a), where χ is the total equivalent noise including both transmission and detection.

Presently we are able to extract practically a key with up to 3.1 dB losses under the "realistic" approach with a reverse reconciliation protocol. Considering now the "paranoid" assumption and reverse reconciliation, the ideal secret key rate is 420 kbits s^{-1} for a lossless line, and 200 kbits s^{-1} for $G_{\text{line}} = 0.79$ (1.0 dB). However, secret bits could be delivered only in the lossless case, at a practical rate of 195 kbits s^{-1}. It is clear that an increase in the reconciliation efficiency would immediately trans-

late into a larger achievable range. Let us point out that we always assume in both the "realistic" or the "paranoid" approach that Eve has an ideal software, quantum memories, perfectly entangled beams, etc. If any of these hypotheses is relaxed, the practical secure range may be extended over the "threshold" presently set by the limited reconciliation efficiency. However, it is not the purpose of the present paper to discuss such "constrained attacks".

Implementation of secret key distillation

Secret key distillation was performed by a computer program written in standard C++ that implements the steps described in the paper. Although Alice's and Bob's data are both processed on the same computer, it is done in the same way as if the parties were distant and were using a network connection as classical channel. The particular platform used is a regular PC running Linux.

As bursts of data are input to the program, a part of the gaussian key elements are sacrificed and used to estimate the characteristics of the quantum channel. This includes the variances and the correlation coefficient between both sides, which would be exchanged between Alice and Bob over the public authenticated classical channel in a real-life setup.

Depending on the value of the estimated I_{AB}, the two parties agree on appropriate binary functions (slices [8, 10]) that will transform their gaussian values into bits. These bits are then reconciled, as described in the paper, with sliced error correction [8, 10] and an implementation [28] of Cascade [27] as a sub-routine. In our implementation, 5 binary functions are used per gaussian key elements, out of which 2 or 3 (depending on I_{AB}) are fully disclosed, while the remaining 3 or 2 are reconciled using Cascade.

Next, the data are moved to the privacy amplification routine. Excluding the bits that are fully disclosed and from which no secret key can be extracted, the reconciled bits are processed by use of a transformation randomly taken in a universal class of hash functions [30, 32], which in our case is the class of truncated linear functions in a finite field. First, we consider the reconciled bits as coefficients of a binary polynomial in a representation of the Galois field GF(2^{110503}), hereby called the reconciled polynomial. Then Alice and Bob publicly and randomly choose a random element of the same field and multiply the reconciled polynomial with this chosen element. Finally, they extract from the resulting polynomial the desired number of least significant bits. In our implementation, the representation of the field is GF(2)$[x]/(p)$, where $p = x^{110503} + x^{519} + 1$ is an irreducible polynomial over GF(2), see ref. [33]. The fact that this operation can be implemented efficiently [34] motivated our choice. The size of the field allows us to process up to 110503 bits at once, or equivalently blocks of about 55200 gaussian key elements when Cascade operates on 2 bits per gaussian key element or of 36800 elements with 3 bits per element. To produce a longer key, the gaussian key elements must thus be grouped into blocks.

As explained in the paper, the number of bits that are destroyed by privacy amplification depends on the amount of information that could be inferred by a potential eavesdropper. An easvesdropper Eve has two sources of knowledge. First, she may have attacked the quantum channel and second, she knows the error positions of the reconciled bits from listening to the execution of Cascade. Let K be the final key, E the ancilla Eve uses for quantum eavesdropping, and Δ the error positions revealed during reconciliation. We thus need to evaluate $I(K; E, \Delta) = I(K; E) + I(K; \Delta|E)$. The first term on the rhs is upper bounded by I_{BE} (in RR) or I_{AE} (in DR), while the second term is evaluated numerically for an entangling cloner attack.

This numerical evaluation of $I(K; \Delta|E)$ comes down to integrating $I(K; \Delta|E = e)$ for all possible outcomes e of E, weighted by the probability density function $p(e)$ of E. In the case of the entangling cloner attack, E refers both to the knowledge of Eve's half of the EPR state she injects and to her eavesdropping of the state being sent to Bob, so E denotes a bivariate gaussian variable whose covariance matrix can be calculated from the channel characteristics (i.e., attenuation and added noise amplitude). For a given outcome e of E, Eve can infer A and B, Alice's and Bob's key elements as a bivariate gaussian variable. Since K and Δ are discrete functions of only A and B, the probability distribution of $K(A, B)$ and $\Delta(A, B)$ conditionally on $E = e$ can be calculated, hence giving $I(K; \Delta|E = e)$.

Finally, a part of the generated key is used to encrypt [29] the execution of the reconciliation for the next block. The remaining bits, namely the net secret key, can be then used for instance to encrypt the classical communications between Alice and Bob using a one-time pad.

[1] Braunstein, S. L. & Pati, A. K. *Quantum information theory with continuous variables* (Kluwer Academic, Dordrecht, 2003).

[2] Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).

[3] Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303(R) (2000).

[4] Ralph, T. C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **62**, 062306 (2000).

[5] Reid, M. D. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A* **62**, 062308 (2000).

[6] Gottesman, D. & Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Rev. A* **63**, 022309

(2001).
[7] Cerf, N. J., Lévy, M. & Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).
[8] Van Assche, G., Cardinal, J. & Cerf, N. J. Reconciliation of a quantum-distributed Gaussian key. E-print arXiv:cs.CR/0107030. To appear in *IEEE Trans. Inform. Theory*.
[9] Bencheikh, K., Symul, Th., Jankovic, A. & Levenson, J.A. Quantum key distribution with continuous variables. *J. Mod. Optics* **48**, 1903-1920 (2001).
[10] Cerf, N. J., Iblisdir, S. & Van Assche, G. Cloning and cryptography with quantum continuous variables. *Eur. Phys. J. D* **18**, 211-218 (2002).
[11] Silberhorn, Ch., Korolkova, N. & Leuchs, G. Quantum key distribution with bright entangled beams. *Phys. Rev. Lett.* **88**, 167902 (2002).
[12] Silberhorn, Ch., Ralph, T.C., Lütkenhaus, N. & Leuchs, G. Continuous variable quantum cryptography beating the 3 dB loss limit. *Phys. Rev. Lett.* **89**, 167901 (2002).
[13] Grosshans, F. & Grangier, Ph. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
[14] Grosshans, F. & Grangier, Ph. Reverse reconciliation protocols for quantum cryptography with continuous variables. E-print arXiv:quant-ph/0204127. Proc. 6th Int. Conf. on Quantum Communications, Measurement, and Computing, (Rinton Press, Princeton, 2003).
[15] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145-195 (2002).
[16] Cerf, N. J., Ipe, A. & Rottenberg, X. Cloning of continuous variables. *Phys. Rev. Lett.* **85**, 1754-1757 (2000).
[17] Cerf, N. J. & Iblisdir, S. Optimal N-to-M cloning of conjugate quantum variables. *Phys. Rev. A* **62**, 040301(R) (2000).
[18] Grosshans, F. & Grangier, Ph. Quantum cloning and teleportation criteria for continuous quantum variables. *Phys. Rev. A* **64**, 010301(R) (2001).
[19] Bennett C.-H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121-3124 (1992).
[20] Duan, L.-M., Giedke, G., Cirac, J. I. & Zoller, P. Entanglement purification of gaussian continuous variable quantum states. *Phys. Rev. Lett.* **84**, 4002-4005 (2000).
[21] Csiszár I. & Körner J., Broadcast channel with confidential messages. *IEEE Trans. Inform. Theory* **24**, 339-348 (1978).
[22] Maurer, U. M. Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory* **39**, 733-742 (1993).
[23] Poizat, J.-Ph., Roch, J.-F. & Grangier, Ph. Characterization of quantum non-demolition measurements in optics. *Ann. Phys. (Paris)* **19**, 265- 297 (1994).
[24] Grangier, Ph., Levenson, J. A. & Poizat, J.-Ph. Quantum non-demolition measurements in optics. *Nature* **396**, 537-542 (1998).
[25] Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 623-656 (1948).
[26] Buttler,W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H. & Peterson, C.G. Fast, efficient error reconciliation for quantum cryptography. E-print arXiv:quant-ph/0203096.
[27] Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. *Advances in Cryptology - Eurocrypt'93* Lecture Notes in Computer Science (ed. Helleseth, T.) 411-423 (Springer, New York, 1993).
[28] Nguyen, K. *Extension des Protocoles de Réconciliation en Cryptographie Quantique*, Thesis, Univ. Libre de Bruxelles (2002).
[29] Lo, H.-K., Method for decoupling error correction from privacy amplification. Eprint arXiv: quant-ph/ 0201030.
[30] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inform. Theory* **41**, 1915-1935 (1995).
[31] Mérolla, J.-M., Mazurenko, Y., Goedgebuer, J.-P. & Rhodes, W. T. Single Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography, *Phys. Rev. Lett.* **82**, 1656-1659 (1999).
[32] Carter, J. L. & Wegman, M. N. Universal Classes of Hash Functions. *J. of Comp. and Syst. Sci.* **18**, 143-154 (1979).
[33] Brent, R. P. Larvala, S. & Zimmermann, P. A fast algorithm for testing irreductibility of trinomials mod 2. Tech. Rep., Oxford University Computing Laboratory, 1-16 (2000).
[34] Schönhage, A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* **7**, 395-398 (1977).