Quantum key distribution using gaussian-modulated coherent states

Frédéric Grosshans*, Gilles Van Assche†, Jérôme Wenger*, Rosa Brouri*, Nicolas J. Cerf† & Philippe Grangier*

** Laboratoire Charles Fabry de l'Institut d'Optique, CNRS UMR 8501, 91403 Orsay, France*
† Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium

Quantum continuous variables[1] are being explored[2–14] 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[2–14] to the usual photon-counting quantum key distribution (QKD) techniques (see ref. 15 and references therein)—for instance, by using 'non-classical' light beams[2–11]. 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[16–18] 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 ways for the partners Alice and Bob to distribute keys beyond this 3 dB limit, for instance by using entanglement purification[20] or postselection[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 current 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

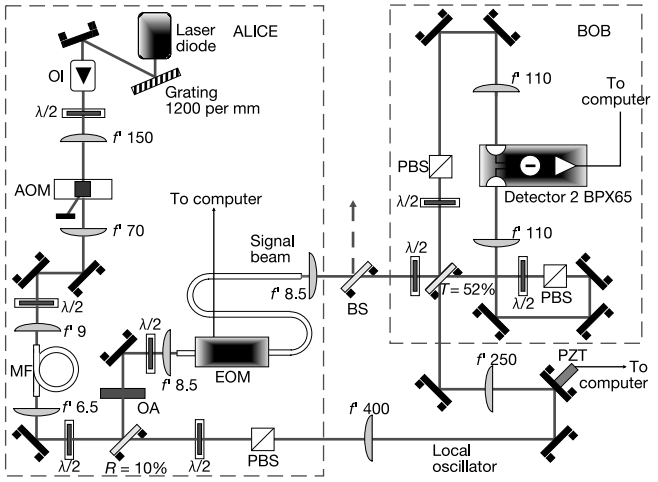

Figure 1 Experimental set-up. Laser diode, SDL 5412 (780 nm); OI, optical isolator; λ/2, half-wave plate; AOM, acousto-optic modulator; MF, polarization maintaining single-mode fibre; OA, optical attenuator; EOM, electro-optic amplitude modulator; PBS, polarizer; BS, beam splitter; PZT, piezoelectric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

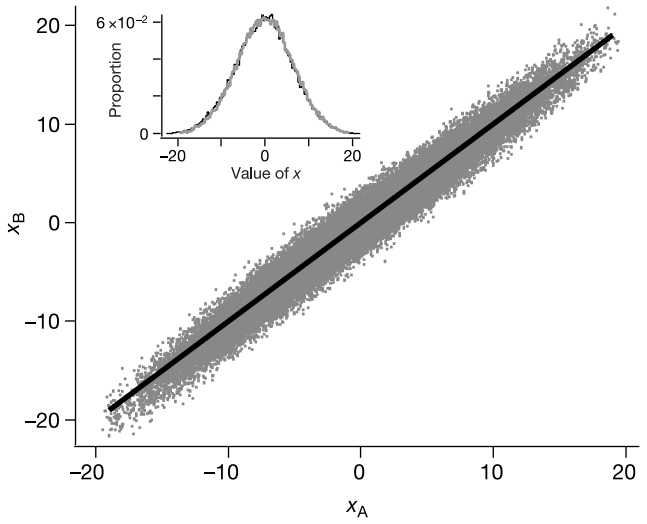

Figure 2 Bob's measured quadrature as a function of the amplitude sent by Alice (in Bob's measurement basis) for a burst of 60,000 pulses. The line transmission is 100% and the modulation variance is $V = 41.7$. The solid line represents the expected unity slope. Inset, the corresponding histograms of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

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 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_{in}, p_{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 Methods), which limit what can be obtained by Eve:

$$V(x_B|x_A)\,V(p_B|p_E) \geq N_0^2 \quad \text{and} \quad V(p_B|p_A)\,V(x_B|x_E) \geq N_0^2 \qquad (1)$$

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 $x_B = G_x^{1/2}(x_{in} + B_x)$ and $p_B = G_p^{1/2}(p_{in} + B_p)$, with $\langle x_{in}^2\rangle = \langle p_{in}^2\rangle = V N_0 \geq N_0$, $\langle B_{x,p}^2\rangle = \chi_{x,p} N_0$, and $\langle x_{in} B_x\rangle = \langle p_{in} B_p\rangle = 0$. 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_{in} of the input field (x_{in}, p_{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_{in}. Therefore, the values of $V(x_A|x_B)$ and $V(p_A|p_B)$ 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 Methods):

$$V(x_B|x_A)_{min} = G_x(\chi_x + V^{-1})N_0$$
$$V(p_B|p_A)_{min} = G_p(\chi_p + V^{-1})N_0 \qquad (2)$$

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, $V(x_B|x_A)_{coh} = G_x(\chi_x + 1)N_0$ and $V(p_B|p_A)_{coh} = G_p(\chi_p + 1)N_0$. The lower bounds on Eve's conditional variances are then obtained from equations (1) and (2), as:

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

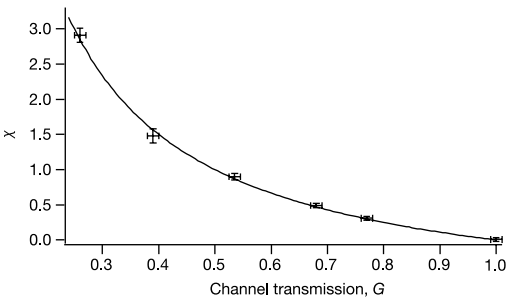

Figure 3 Channel equivalent noise χ_{line} as a function of line transmission G. The curve is the theoretical prediction $\chi_{vac} = (1 - G)/G$. The error bars include two contributions with approximately the same size, from statistics (evaluated over blocks of 60,000 pulses) and systematics (calibration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

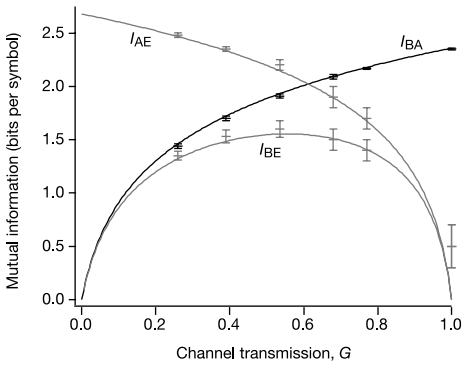

Figure 4 Values of I_{BA}, I_{BE} and I_{AE} as a function of the line transmission G for $V \approx 40$. Here, I_{BA} is given by equation (4a), including all transmission and detection noises for evaluating V_B and $(V_{B|A})_{coh}$. The expression for I_{BE} is given by equation (4b), using the same V_B and $(V_{B|E})_{min} = N_0/\{G(\chi_{line} + V^{-1})\} + N_{el} + N_{hom}$. 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).

Table 1 **Ideal and practical net secret key rates**

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	–

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 $I_{AB} - I_{BE}$ 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 (~5%) in the present set-up.

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

To assess the security of the RR scheme, we assume 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

$$I_{BA} = (1/2)\log_2[V_B/(V_{B|A})_{coh}] = (1/2)\log_2[(V+\chi)/(1+\chi)] \quad (4a)$$

$$I_{BE} = (1/2)\log_2[V_B/(V_{B|E})_{min}] = (1/2)\log_2[G^2(V+\chi)(V^{-1}+\chi)] \quad (4b)$$

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

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

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 $\chi_{vac} = (1-G)/G$, and an 'excess noise' component defined as $\varepsilon = \chi - \chi_{vac}$. In the high-loss limit ($G \ll 1$), the RR protocol remains secure if $\varepsilon < (V-1)/(2V) \approx 1/2$, 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 $\varepsilon \approx 1$, 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 Methods). 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 $\chi_{line}N_0$, the electronics noise of Bob's detector ($N_{el} = 0.33N_0$), and the noise due to imperfect homodyne detection efficiency ($N_{hom} = 0.27N_0$). When introducing line losses using a variable attenuator, the measured χ_{line} increases as $(1-G)/G$, as shown in Fig. 3 ($\varepsilon_{line} = 0$ 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 Supplementary Information 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 Methods and Supplementary Information). Although Alice and Bob are not spatially separated in the present set-up, the analysed data have the same structure as in a realistic cryptographic exchange. Table 1 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 kbit s^{-1} (see also Methods). 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 1). 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. Because 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 Methods). 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. □

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 $(x_{in}, p_{in}) = (x_A + A_x, p_A + A_p)$ that she sends, with $\langle A_x^2\rangle = \langle A_p^2\rangle = s N_0$. 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 Supplementary Information). 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 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 Supplementary Information). 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, we 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].

Received 8 July; accepted 30 October 2002; doi:10.1038/nature01289.

1. Braunstein, S. L. & Pati, A. K. *Quantum Information Theory with Continuous Variables* (Kluwer Academic, Dordrecht, in the press).
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. Preprint cs.CR/0107030 at ⟨http://arxiv.org⟩ (2001).
9. Bencheikh, K., Symul, Th., Jankovic, A. & Levenson, J. A. Quantum key distribution with continuous variables. *J. Mod. Opt.* **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. Preprint quant-ph/0204127 at ⟨http://arxiv.org⟩ (2002).
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. Preprint quant-ph/0203096 at ⟨http://arxiv.org⟩ (2002).
27. Brassard, G. & Salvail, L. *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. Preprint quant-ph/0201030 at ⟨http://arxiv.org⟩ (2002)
30. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inform. Theory* **41,** 1915–1935 (1995).

Supplementary Information accompanies the paper on *Nature*'s website (**http://www.nature.com/nature**).

Acknowledgements The contributions of J. Gao to the 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.

Competing interests statement The authors declare that they have no competing financial interests.

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

Single-nanowire electrically driven lasers

Xiangfeng Duan*†, Yu Huang*†, Ritesh Agarwal* & Charles M. Lieber*‡

** Department of Chemistry and Chemical Biology, ‡ Division of Engineering and Applied Sciences, Harvard University, Cambridge, Massachusetts 02138, USA*
† These authors contributed equally to this work

Electrically driven semiconductor lasers are used in technologies ranging from telecommunications and information storage to medical diagnostics and therapeutics[1]. The success of this class of lasers is due in part to well-developed planar semiconductor growth and processing, which enables reproducible fabrication of integrated, electrically driven devices[2,3]. Yet this approach to device fabrication is also costly and difficult to integrate directly with other technologies such as silicon microelectronics. To overcome these issues for future applications, there has been considerable interest in using organic molecules[4,5], polymers[6,7],