Experimental demonstration of long-distance continuous-variable quantum key distribution

Paul Jouguet1,2, Sébastien Kunz-Jacques2, Anthony Leverrier3,4, Philippe Grangier5 and Eleni Diamanti6

Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications1. The rapid progress in this field has enabled quantum key distribution in real-world conditions2,3 and commercial devices are now readily available. Quantum key distribution systems based on continuous variables4 provide the major advantage that they only require standard telecommunication technology. However, to date, these systems have been considered unsuitable for long-distance communication5–7. Here, we overcome all previous limitations and demonstrate for the first time continuous-variable quantum key distribution over 80 km of optical fibre. All aspects of a practical scenario are considered, including the use of finite-size data blocks for secret information computation and key distillation. Our results correspond to an implementation guaranteeing the strongest level of security for quantum key distribution reported so far for such long distances and pave the way to practical applications of secure quantum communications.

Long-distance experiments in quantum information science, and in particular featuring quantum key distribution (QKD), are of the utmost importance for future technological applications. Such experiments will allow the integration of quantum devices in current secure infrastructures and in future networks based on quantum repeaters8. The quest for long-distance QKD in recent years has led to several successful demonstrations9–12; however, improving security guarantees and performance in practical conditions in these implementations remains an issue. These experiments use discrete-variable or distributed-phase-reference protocols1, where key information is encoded on the properties of single photons. Alternatively, in continuous-variable (CV) QKD protocols, light carries continuous information such as the value of a quadrature component of a coherent state. Such protocols have been implemented in various situations9–13,14–17. Their key feature is that dedicated photon-counting technology can be replaced by the homodyne detection techniques that are widely used in classical optical communications. However, CVQKD schemes require complex post-processing procedures, mostly related to error correction. These have limited their operation to less than 25 km of optical fibre9–7, a communication span that may be insufficient for network cryptographic applications. Furthermore, implementations so far have been based on security proofs valid in the limit of infinitely large data blocks, but the finite size of real data must be taken into account according to state-of-the-art security analysis18,19.

Here, we demonstrate the distribution of secret keys over a distance of 80 km, using continuous variables and security proofs compatible with the use of finite-size data blocks for the generation of the secret key. This remarkable range improvement was made possible by system operation in a regime of signal-to-noise ratios (SNRs) between one and two orders of magnitude lower than in earlier implementations. It was previously overlooked that techniques developed for error correction of Gaussian signals can perform close to the optimal bounds for low SNR. Implementing such error-correction codes at high speed and in an optical environment featuring excellent stability, which enables the acquisition of large data blocks, allowed us to access previously inaccessible parameter regions. This was a key element for the present experiments.

In the experimental set-up, shown in Fig. 1, we implement the standard GG02 coherent-state CVQKD protocol20. The sender, Alice, prepares coherent states with a Gaussian modulation and sends them to the receiver, Bob, who measures one of the quadratures with a homodyne detection system. A reverse reconciliation scheme is used in which Alice and Bob use Bob’s data to establish the secret key13. In practice, coherent light pulses are generated by a 1.550 nm laser diode at a repetition rate of 1 MHz, and split into a weak signal and a strong local oscillator (LO), which provides the required phase reference. The signal pulses are then randomly modulated in both quadratures and transmitted together with the LO pulses in a single fibre using time- and polarization-multiplexing techniques. At the receiver side, the pulses interfere on a homodyne detector, the output of which is proportional to the signal quadrature selected by a phase modulator placed at Bob’s LO path. Owing to the improved design with respect to previous implementations, the set-up presents excellent stability, ensured by several feedback controls (see Methods for details).

The security of the implemented protocol is well established against collective attacks, both in the asymptotic21,22 and finite-size regimes23. Moreover, collective attacks have been shown to be asymptotically optimal23,24. Here, we consider security proofs pertaining to such attacks, also taking into account finite-size effects. The Gaussian modulation used in the implemented protocol maximizes the mutual information between Alice and Bob, thus offering an optimal theoretical key rate. However, it is hard to reconcile correlated Gaussian variables, especially at low SNRs, which are inherent in long-distance experiments. Indeed, the secure distance of previous demonstrations of fibre-based CVQKD25 was limited to 25 km because no efficient error-correction procedure was available at low SNRs. Here, we use a multidimensional reconciliation protocol25, which transforms a channel with a Gaussian modulation into a virtual binary modulation channel, with a capacity loss that is very low at low SNR. This enables the use of error-correction codes designed for the binary input additive white Gaussian noise...
channel, which has typical efficiencies, for an arbitrarily low SNR, of 0.95 extracted bits per theoretically available bit. This leads to a significant extension of the secure distance.

Let us now look at the parameters that are relevant for the extraction of the secret key. As a result of the Gaussian optimality theorem, Alice and Bob’s two-mode state at the output of the quantum channel is fully characterized by Alice’s modulation variance $V_A$, channel transmission $T$ and excess noise $\xi$, which is added by the channel. Both $V_A$ and $\xi$ are expressed in shot noise units. These parameters, together with the shot noise, are estimated in real time using a parameter estimation process, during which a fraction of the samples is randomly revealed. The other parameters used to compute an estimate of the homodyne detection $\eta$, are assumed not to be accessible to Eve and are measured during a secure calibration procedure that takes place before the deployment of the system. For simplicity, we make the standard assumption that Eve does not tamper with the local oscillator, but we emphasize that countermeasures against such tampering have been proposed (see Supplementary section, ‘Local oscillator manipulation’, for details). The modulation variance is adjusted in real time so as to be at all times as close as possible to the threshold of the available code.

Privacy amplification allows extracting the secret information from the identical strings shared by Alice and Bob after error correction. In addition to the amount of data revealed during error correction, we compute an upper bound on the eavesdropper’s information on the corrected string for collective attacks in both the asymptotic regime, where all the experimental parameters are assumed to be known with infinite precision, and in the finite-size regime, where the parameters are estimated over large data pulse sets. The stability of our system allows us to obtain a positive secret key rate at long distances in both regimes.

**Figure 1** | Optical layout of the long-distance CVQKD prototype. Alice sends Bob 100 ns coherent light pulses generated by a 1,550 nm telecom laser diode pulsed with a frequency of 1 MHz. These pulses are split into a weak signal and a strong LO with an unbalanced coupler. The signal pulse is modulated with a centred Gaussian distribution using an amplitude and phase modulator. The variance is controlled using a coarse variable attenuator and the amplitude modulator. The signal pulse is 200 ns delayed with respect to the LO pulse using a 20 m delay line and a Faraday mirror. Both pulses are multiplexed with orthogonal polarization using a polarizing beamsplitter (PBS). The time- and polarization-multiplexed pulses are then sent through the channel. They are demultiplexed on Bob’s side with another PBS combined with active polarization control. A second delay line on Bob’s side allows for time superposition of the signal and LO pulses. After demultiplexing, the signal and LO interfere on a shot-noise-limited balanced pulsed homodyne detector. A phase modulator on the LO path allows for random choice of the measured signal quadrature. Alice and Bob are located in the same laboratory and separated by fibre spools. The maximum operating distance of the experiment is 80 km.

**Figure 2** | Key rate produced by the system after error correction and privacy amplification over 24 h. There is a SNR of 1.1 on Bob’s side at 25 km (5.0 dB losses), a SNR of 0.17 at 53 km (10.6 dB losses), and a SNR of 0.08 on Bob’s side at 80.5 km (16.1 dB losses). In red, the rate is calculated assuming an eavesdropper is able to perform collective attacks in the asymptotic regime. This rate is also valid against arbitrary attacks. In green (blue), the rate is calculated assuming an eavesdropper is able to perform collective attacks taking into account finite-size effects with block size of $1\times10^8$ ($1\times10^9$) and security parameter $e = 1\times10^{-10}$. The odd shape of the curves results from the use of a small set of error-correcting codes optimized to perform data reconciliation in specific ranges of SNR. The homodyne detection is characterized by an efficiency of $\eta = 0.552$, known with an uncertainty of $\Delta \eta = 0.025$, and an electronic noise variance $\nu_{el} = 0.015$, known with an uncertainty of $\Delta \nu_{el} = 0.002$. For comparison, previous state-of-the-art experimental results are shown: these are all restricted to distances below 25 km and do not take finite-size effects into account.
Long-distance secret key generation results are shown in Fig. 2. Secret keys were produced by the experimental system at 25 km, 53 km and 80.5 km of standard optical fibre. The key rate was computed over 24 h for all distances. A fitting procedure revealed 50% of the raw key for parameter estimation, while 50% of the optical pulses were also discarded for shot noise estimation. The fraction of light pulses effectively used for generating the key was thus 25%. Error correction was performed using low density parity check codes with a graphic processing unit (GPU) decoder (see Supplementary section, ‘Post-processing performance’, for details). The obtained secret key rates are lower than those obtained with discrete-variable QKD25. This is mainly a result of the lower clock rate of our experiment. The results corresponding to the finite-size regime are of particular interest because of their relevance for practical applications. Indeed, obtaining an infinite precision in parameter estimation as required in the asymptotic case is, in practice, impossible. We can further elucidate these results by investigating the impact on the secret key rate of the uncertainty on the excess noise value. Figure 3 shows the experimental excess noise measured on blocks of size $1 \times 10^8$ over 24 h for a distance of 53 km. For each data point, a worst-case estimator of the excess noise compatible with the experimental data is also indicated. For comparison, the worst-case estimator for a block size of $1 \times 10^6$ is displayed and is clearly incompatible with the extraction of a secret key rate, thus showing that a very large block size is required to achieve long-distance QKD. These results illustrate the significance of the excess noise estimation for system performance. They also confirm the excellent stability of our system, because the excess noise maintains low values, even in this very low SNR regime required by the security proof, and with very large data blocks.

To conclude, let us discuss possible further improvements to our implementation. The current repetition rate of 1 MHz can be increased by shortening the pulse duration and the time-multiplexing period, as well as the homodyne detection data sampling period, using high-speed and high-precision data acquisition cards. Current error-correction techniques can deal with raw key rates of up to 10 Mbits s$^{-1}$, and better rates are possible using multiple devices. However, both the fitting procedure and the multidimensional reconciliation scheme require a large amount of classical data to be transmitted between Alice and Bob, so increasing the optical rate too much would lead to network link saturation. Finally, the ultimate secure distance that can be reached by our system is determined by the excess noise present in the setup. In this respect, recent protocols using ‘noiseless amplification’27 or its ‘virtual’ implementation28,29 might be promising.

Methods

Experimental details. Our experiment is a one-way implementation, where Alice sends Bob coherent light pulses with a 100 ns duration and 1 MHz repetition rate, generated by a 1,550 nm pulsed telecom laser diode. These pulses are split into a weak signal and a strong LO with an unbalanced coupler. The implemented protocol uses Gaussian modulation of coherent states20, whereby the signal and LO interfere on a shot-noise-limited balanced homodyne detector. The electric signal coming from the detector is proportional to the signal quadrature $X_r$, where $X_r$ is the relative phase between the signal and the LO, which can be controlled using the phase modulator on Bob’s LO path according to the Gaussian protocol20.

Feedback controls are implemented to allow for stable operation of the system over a large number of pulses ($\geq 1 \times 10^9$). Polarization drifts occurring in the quantum channel are corrected using a dynamic polarization controller. The beamsplitter placed at the entrance of Bob’s apparatus aims to generate, from the LO pulse, a clock signal that is independent of polarization state. The homodyne detection statistics and an appropriate algorithm then allow us to maintain an optimal polarization state at the output of the channel. The photodiode on Alice’s signal path is used for amplitude modulator feedback to correct alterations of the required voltage settings induced by temperature variations. On Bob’s side, the homodyne detection output is sensitive to phase and can be used to control Alice’s and Bob’s phase modulators.

Security conditions. Collective attacks against the implemented protocol have been shown to be asymptotically optimal, thanks to an infinite-dimensional version of de Finetti’s theorem23. Furthermore, security proofs combining arbitrary attacks and finite-size effects are presently under active study23,24.

The implemented protocol requires an exact Gaussian modulation, which is impossible to achieve. In practice, this is approximated by a truncated discretized modulation with parameters compatible with a security proof against collective attacks. This is performed with almost optimal randomness consumption using source coding techniques.

Efficiency and variance of the electronic noise of the homodyne detection are assumed to be calibrated in a secure laboratory. This corresponds to the standard realistic assumption for CVQKD implementations, according to which Eve cannot entangle herself with the losses or electronic noise of the homodyne detection. Under this assumption, we evaluate confidence intervals for these values and we compute the eavesdropper’s corresponding information taking calibrated value uncertainties into account25. Note that in the so-called ‘paranoid’ or ‘uncalibrated-device’ scenario26, where Eve can exploit the homodyne detection parameters, no secret key would be obtained beyond 35 km.

Multidimensional reconciliation. The error-correction step is divided into two parts. First, Bob divides his data into vectors of size 8 and for each, draws a binary vector $u$ of the same size at random; $u$ is the reference for the key after error correction. Bob then computes $r = yu$ (where the vectors are interpreted as matrices ref. 25 for details) and sends it to Alice who obtains $r = x^{-1}r = x^{-1}yu$, which is a noisy version of Bob’s binary modulated vector $u$, with a noise close to a Gaussian noise. Interestingly, it can be shown that the classical data $r$, available to Eve, does not leak any information about the binary vector $u$ ref. 25. The second step of the error-correction protocol consists in forming vectors of size...
20 on Alice’s and Bob’s sides (corresponding to $2^2$ pairs of such vectors $u, v$) and to use multi-edge low-density parity check (LDPC) codes to correct all the errors20. The amount of data revealed during this step is subtracted from the secret information previously computed. We use GPU decoding to obtain a decoding speed compatible with real-time data processing.

Received 2 October 2012; accepted 17 February 2013; published online 14 April 2013

References
1. Scarani, V. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301–1350 (2009).
2. Peev, M. et al. The SECOQC quantum key distribution in Vienna. New J. Phys. 11, 075001 (2009).
3. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. Opt. Express 19, 10387–10409 (2011).
4. Weedbrook, C. et al. Gaussian quantum information. Rev. Mod. Phys. 84, 621–669 (2012).
5. Fossier, S. et al. Field test of a continuous-variable quantum key distribution prototype. New J. Phys. 11, 045023 (2009).
6. Dinh Xuan, Q., Zhang, Z. & Voss, P. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. Opt. Express 17, 24244–24249 (2009).
7. Jouguet, P. et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. Opt. Express 20, 14030–14041 (2012).
8. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. Phys. Rev. Lett. 81, 5932–5935 (1998).
9. Takekura, H. et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nature Photon. 1, 343–348 (2007).
10. Rosenberg, D. et al. Practical long-distance quantum key distribution system using decoy levels. New J. Phys. 11, 045009 (2009).
11. Stucki, D. et al. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. New J. Phys. 11, 075003 (2009).
12. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Continuous operation of high bit rate quantum key distribution. Appl. Phys. Lett. 96, 161102 (2010).
13. Grosshans, F. et al. Quantum key distribution using Gaussian-modulated coherent states. Nature 421, 238–241 (2003).
14. Qi, B., Huang, L-L., Qian, L. & Lo, H-K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. Phys. Rev. A 76, 052323 (2007).
15. Lodewyck, J. et al. Quantum key distribution over 23 km with an all-fiber continuous-variable system. Phys. Rev. A 76, 030303 (2007).
16. Symul, T. et al. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. Phys. Rev. A 76, 030303 (2007).
17. Shen, Y., Zou, H., Tian, L., Chen, P. & Yuan, J. Experimental study on discretely modulated continuous-variable quantum key distribution. Phys. Rev. A 82, 022317 (2010).
18. 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).
19. 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).
20. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88, 057902 (2002).
21. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. 97, 190503 (2006).
22. Navascués, M., Grosshans, F. & Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys. Rev. Lett. 97, 190502 (2006).
23. Renner, R. & Cirac, J. I. De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. 102, 110504 (2009).
24. Leverrier, A., García-Patrón, R., Renner, R. & Cerf, N. J. Security of continuous-variable quantum key distribution against general attacks. Phys. Rev. Lett. 110, 030502 (2013).
25. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G. & Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. A 77, 042325 (2008).
26. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys. Rev. A 84, 062317 (2011).
27. Blandino, R. et al. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. Phys. Rev. A 86, 012327 (2012).
28. Fiurasek, J. & Cerf, N. J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys. Rev. A 86, 060302(R) (2012).
29. Walk, N., Symul, T., Lam, P-K. & Ralph, T. C. Security of continuous-variable quantum cryptography with Gaussian postselection. Phys. Rev. A 87, 020303(R) (2013).
30. Furrer, F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. Phys. Rev. Lett. 109, 100502 (2012).

Acknowledgements
This research was supported by the French National Research Agency, through the FREQUENCY (Fundamental Research in Quantum Networks and Cryptography, ANR-09-BLAN-0410) and HIPERCOM (High Performance Coherent Quantum Communications, 2011-CHRI-006) projects, and by the European Union through the project Q-CERT (Quantum Key Distribution Certification, FP7-PEOPLE-2009-IAPP). P.J. acknowledges support from the ANRT (Agence Nationale de la Recherche et de la Technologie). A.L. was supported by the SNF through the National Centre of Competence in Research ‘Quantum Science and Technology.’

Author contributions
P.J., S.K.-J. and E.D. conceived the project and developed the experimental setup. P.J. and S.K.-J. collected and analyzed the data. A.L. performed the security analysis. All authors contributed to writing the manuscript.

Additional information
Supplementary information is available in the online version of the paper. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to P.J.

Competing financial interests
The authors declare no competing financial interests.