Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber

Paul Jouguet,[1,2] Sébastien Kunz-Jacques,[2] Anthony Leverrier,[3] Philippe Grangier,[4] and Eleni Diamanti[1]

[1]*LTCI, CNRS - Telecom ParisTech, 46 rue Barrault, 75013 Paris, France*
[2]*SeQureNet, 23 avenue d'Italie, 75013 Paris, France*
[3]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[4]*Laboratoire Charles Fabry de l'Institut d'Optique - CNRS - Univ. Paris-Sud 11, 2 avenue Augustin Fresnel, Campus Polytechnique, 91127 Palaiseau, France*

Introduction – Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications [1]. The rapid progress in this field has allowed for tests of quantum key distribution (QKD) systems in real-world conditions, bringing the entire field one step closer to practical applications. Furthermore, the theoretical and experimental tools that have been developed for these demonstrations have played or are expected to play a crucial role in further advancements in quantum cryptography and quantum communications.

In this work, we are interested in quantum key distribution based on continuous variables (CV), which offers a promising alternative to the most commonly employed discrete-variable protocols (see [2] for a recent review). The main advantage of CVQKD systems is that they only require standard telecommunication technology, and, in particular, that they do not use photon counters. Furthermore, recent work emphasized their potential compatibility with standard wavelength division multiplexed telecommunication networks [3]. However, these systems were considered up till now unsuitable for long-distance communication. Indeed, issues mainly related to the complex reconciliation codes required in these systems have hindered their operation over more than 25 km of optical fiber [4, 5].

Here, we overcome all previous limitations and demonstrate for the first time continuous-variable secret key distribution over up to 80 km of optical fiber. The demonstration includes all aspects of a real-world scenario, with real-time generation of secret keys and stable long-term operation in a regular environment with standard optical fibers. Moreover, this is the first QKD demonstration that takes into account the use of finite-size blocks of data for secret information computation and secret key distillation.

Security considerations – The protocol investigated here is the standard GG02 [6] with reverse reconciliation [7], where Alice prepares coherent states with a Gaussian modulation and sends them to Bob who measures either one of the quadratures with a homodyne detection. The security of this protocol is well established against collective attacks [8, 9], even in the finite-size regime [10]. The main remaining open question concerns its security against coherent attacks. In that case, an infinite-dimensional version of de Finetti's theorem shows that collective attacks are in fact optimal in the asymptotic limit [11]. Unfortunately, this result cannot directly be used in a practical scenario because the convergence to the asymptotic limit is too slow. This problem, however, can be solved with the use of the technique proposed by Christandl *et al* in [12], which was initially restricted to finite-dimensional protocols but can be efficiently adapted to continuous-variable protocols by exploiting their specific symmetries in phase space [13]. Using this approach, one can compute the secret key rate valid against arbitrary attacks in a finite-size scenario, which corresponds to the strongest level of security achievable with QKD. Another approach to prove the security of CV protocols is based on an entropic uncertainly relation, but only provides security for very short distances [14].

Experimental conditions – Our system is composed of a pair of optical devices, whose hardware description is given in Figure 1. This is a one-way implementation, where Alice sends to Bob coherent light pulses with a 100 ns duration and 500 kHz repetition rate generated by a 1550 nm pulsed telecom laser diode. These pulses are split into a weak signal and a strong local oscillator (LO) with an unbalanced coupler. The implemented protocol uses Gaussian modulation of coherent states [6]: the signal is randomly modulated following a centered Gaussian modulation in both quadratures, using an amplitude and a phase modulator. The signal pulses are then attenuated by a variable attenuator such that the signal power belongs to a range allowing to control the variance of the Gaussian distribution exiting Alice's device using a photodiode and an appropriate feedback algorithm. A second variable attenuator lowers the signal level to a few shot noise units.

The signal and LO are then transmitted through the optical fiber without overlap using time and polarization multiplexing. Delay lines of 200 ns, composed of a 20-m single-mode fibre followed by a Faraday mirror, are used for the time multiplexing. Polarization multiplexing is achieved using polarization beam splitters (PBS). After demultiplexing, the signal and LO interfere on a shot-noise limited balanced pulsed homodyne detector (HD). The electric signal coming from the HD is proportional to the signal quadrature X_ϕ , where ϕ 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 protocol [6].

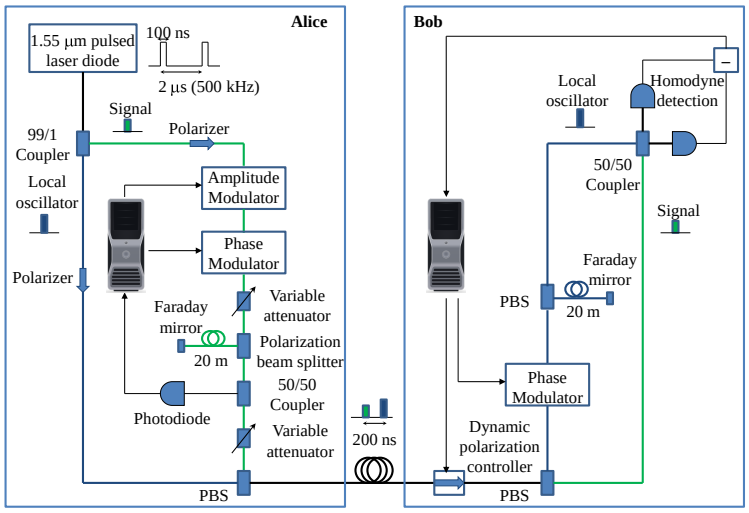

Figure 1: Optical layout of the long-distance CVQKD prototype.

Feedback controls are implemented to allow for a stable operation of the system over large number ($\geq 10^8$) of pulses. Polarization drifts occurring in the quantum channel are corrected using a dynamic polarization controller that finds an optimal polarization state at the output of the channel. The photodiode on Alice's signal path is used for the feedback control of Alice's amplitude modulator. 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.

Some of the required parameters to compute the secret key rate, namely the modulation variance V_A, the transmission T, and the excess noise ξ, are estimated in real time during a Parameter Estimation (PE) step during which half of the samples are randomly chosen and revealed. The other parameters used to compute an estimate of the secret information that can be extracted from the shared data, namely the electronic noise v_{el} and the efficiency of the homodyne detection η, are measured during a calibration procedure that takes place before the deployment of the system and that is assumed to be performed in a secure environment. In practice, since we are given a finite set of high-efficiency error-correction codes at some fixed signal-to-noise ratios (SNRs), we adjust the modulation variance V_A in order to be as close as possible to the SNR corresponding to the threshold of a code.

Long-distance CVQKD results – The Gaussian modulation used in the implemented protocol maximizes the mutual information between Alice and Bob, thus offering an optimal theoretical key rate against collective attacks. However, it is hard to reconcile correlated Gaussian variables, especially at low SNR. The secure distance of previous demonstrations of fiber-based CVQKD [4, 5] was limited to about 25 km because no efficient error-correction procedure was available at low SNR. In this work, we use the multidimensional reconciliation protocol of [15] that transforms a Gaussian channel into a 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 (BIAWGNC) whose typical efficiencies for arbitrarily low SNRs are of 0.95 extracted bit per bit theoretically available [16]. In this way, the secure distance can be considerably extended.

For a fixed transmission, several codes yield a positive secret key rate [16]. We choose the code with the best efficiency compatible with the observed transmission and the allowed range for the variance modulation (roughly between 1 and 10 shot noise units on Alice's side). The privacy amplification step allows us to extract the secret information from the identical strings shared by Alice and Bob after the error-correction procedure. In addition to the amount of data revealed during the error-correction step, we compute an upper bound on Eve's information on the corrected string against collective attacks in both the asymptotic regime, where we assume that all the parameters are known with an infinite precision, and in the finite-size regime [10], where the transmission and the excess noise are estimated over large data pulse sets ($\geq 10^8$ pulses). The stability of our system allows us to obtain a positive secret key rate at long distances in both regimes.

Figure 2 gives the secret key rate produced by the system operating during 16.5 hours with 100 km of standard optical fiber (21.4 dB losses). The mutual information I_{AB} is measured at 100 km, and for any distance the secret key size is calculated by keeping Bob's measured signal and noise both constant. This means that I_{AB} is not changed

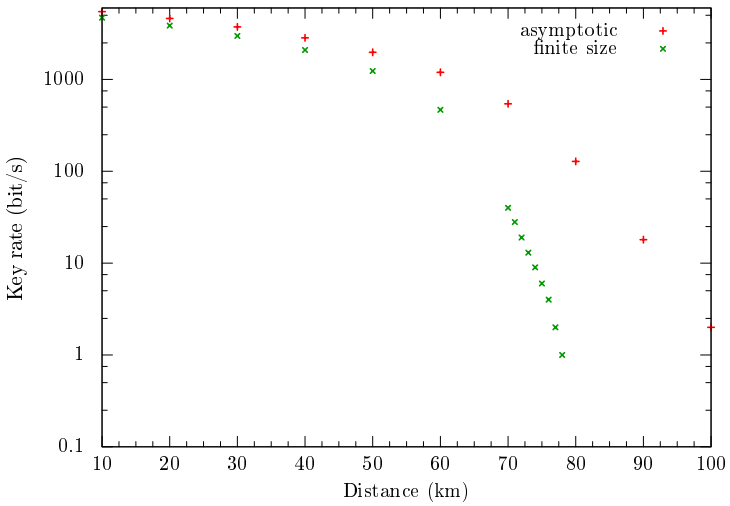

Figure 2: Key rate produced by the system after error correction and privacy amplification during 16.5 hours with a SNR of 0.075 on Bob's side. We used 100 km of standard optical fiber corresponding to 21.4 dB losses. In red, the rate is calculated assuming an eavesdropper able to perform collective attacks in the asymptotic regime. In green, the rate is calculated assuming an eavesdropper able to perform collective attacks taking into account finite-size effects with blocksize 10^8 and epsilon security parameter $\epsilon = 10^{-10}$.

either, and only the estimate of the amount of data known to the attacker changes with the distance. Note that this means that Alice's variance is implicitly readjusted with distance, as well as the excess noise referred to the input. This procedure will generally under-evaluate the number of secret bits, with respect to what would be obtained by a "real" experiment, performed at distances below 100 km. A sifting procedure reveals 50% of the raw key for parameter estimation. The failure probability of the error correction is about 0.3, which means that roughly 30% of the sifted key must be discarded. These results show that the system is reliable and the excess noise is low in the very low SNR regime, as required by the security proof.

Conclusion – We have demonstrated for the first time that long-distance quantum key distribution can be achieved with continuous variables, using only standard telecommunication components. Furthermore, we obtain a positive secret key rate over long distances even when taking into account finite-size effects. These results correspond to a practical implementation guaranteeing the strongest level of security achievable with QKD and show that continuous-variable quantum key distribution is a technology of choice for near-future secure quantum communications.

[1] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010).
[4] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).
[5] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, *arXiv:*1201.3744 [quant-ph] (2012).
[6] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[7] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[8] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[9] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[10] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[11] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[12] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[13] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, submitted to QCrypt 2012.
[14] F. Furrer, T. Franz, M. Berta, V. B. Scholtz, M. Tomamichel, and R. F. Werner, *arXiv:*1112.2179 [quant-ph] (2011).
[15] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[16] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).