Field test of a continuous-variable quantum key distribution prototype

Simon Fossier, Eleni Diamanti, Thierry Debuisschert, André Villing, Rosa Tualle-Brouri, Philippe Grangier

Field test of a continuous-variable quantum key distribution prototype

2009 New J. Phys. 11 045023

(http://iopscience.iop.org/1367-2630/11/4/045023)

New Journal of Physics
The open-access journal for physics

Field test of a continuous-variable quantum key distribution prototype

S Fossier[1,2,3], E Diamanti[2], T Debuisschert[1], A Villing[2], R Tualle-Brouri[2] and P Grangier[2]

[1] Thales Research & Technology France, RD 128, 91767 Palaiseau Cedex, France
[2] Laboratoire Charles Fabry de l'Institut d'Optique–CNRS–Univ. Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France
E-mail: simon.fossier@institutoptique.fr

New Journal of Physics **11** (2009) 045023 (14pp)
Received 17 December 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045023

Abstract. We have designed and realized a prototype that implements a continuous-variable quantum key distribution (QKD) protocol based on coherent states and reverse reconciliation. The system uses time and polarization multiplexing for optimal transmission and detection of the signal and phase reference, and employs sophisticated error-correction codes for reconciliation. The security of the system is guaranteed against general coherent eavesdropping attacks. The performance of the prototype was tested over preinstalled optical fibres as part of a quantum cryptography network combining different QKD technologies. The stable and automatic operation of the prototype over 57 h yielded an average secret key distribution rate of 8 kbit s^{-1} over a 3 dB loss optical fibre, including the key extraction process and all quantum and classical communication. This system is therefore ideal for securing communications in metropolitan size networks with high-speed requirements.

[3] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Experimental quantum key distribution (QKD) has been the subject of intense research efforts during the last decade; these efforts have led to an impressive progress, which has allowed QKD to become the field in quantum information processing that is the closest to applications. The majority of the QKD systems that have been realized implement discrete-variable or distributed-phase-reference protocols [1], which use properties of single photons to encode key information. Continuous-variable (CV) QKD protocols, in which light carries continuous information such as the value of the quadrature of a coherent state, have been proposed as another option, which opens the door to very high secret key generation rates [2]–[9]. In the protocol that we have implemented [7], the key information is encoded by Alice in two orthogonal quadratures X and P (or equivalently the amplitude and phase) of a train of coherent states that are modulated according to a centred bi-Gaussian distribution. These states are sent along with a phase reference through the quantum channel to Bob, who randomly measures one of the two quadratures using a homodyne detection setup. Alice and Bob then extract a secret common binary key from their data, by performing classical procedures for channel characterization, error correction and privacy amplification. The security of this protocol stems from Heisenberg inequalities satisfied by the quantum CVs accessible to Alice, Bob and the eavesdropper Eve. Security proofs of this protocol against general individual and collective eavesdropping attacks have been provided [7], [10]–[12], and have been recently completed by unconditional security proofs against the most general type of attacks [13].

From a practical point of view, the coherent-state CVQKD protocol requires a simple system architecture and eliminates the need for specific resources such as single-photon sources and detectors. It was first implemented in a proof-of-principle table-top experiment at near-infrared wavelength (780 nm), based on a pulsed, shot-noise-limited homodyne detector [7].

Subsequently, the system went through successive phases of development that included the implementation of advanced error-correction algorithms and the operation at infrared wavelength (1550 nm) in order to enhance the performance of the system using standard, fast and efficient products of the telecommunication industry [14, 15]. The experimental implementation of a partial intercept-and-resend eavesdropping attack on such a system confirmed the entanglement-breaking bound for the coherent-state CVQKD protocol through a direct measurement of the system's excess noise [16]. However, despite this progress, the developed systems remained laboratory experimental setups, unsuitable for implementation of QKD in standard fibre optic networks. Here, we present a portable CVQKD prototype that provides stable and automatic distribution of secret keys over several days at high rates. To reach this goal, several experimental advancements were required, such as the time and polarization multiplexing of the signal and phase reference in the quantum channel, as well as the implementation of automation and hardware control procedures, combined with advanced reconciliation and key verification techniques. The prototype was tested in a field implementation of a quantum cryptography network developed within the European Integrated Project SECOQC [17], which brought together prototypes based on various QKD technologies [18]–[21]. The average secret key distribution rate provided by the CVQKD prototype over 3 days and through a 3 dB channel (corresponding to a 15 km standard optical fibre) was 8 kbit s^{-1}, including all quantum and classical communication. This system is therefore most suitable for use in metropolitan-size secure networks that require high communication rates.

2. CVQKD prototype layout

The optical layout of the CVQKD prototype we have designed is shown in figure 1. The setups of Alice and Bob are entirely composed of fibre optic components operating at telecom wavelength, pigtailed with polarization-maintaining (PM) single-mode fibres. They have been designed to implement the protocol briefly discussed in the introduction and presented in detail in [7].

2.1. Optical setup

As shown in figure 1, Alice generates coherent light pulses using a 1550 nm telecom laser diode pulsed with a frequency of 500 kHz. The length of the generated pulses is 100 ns. The pulses are then separated into a weak signal and a strong local oscillator (LO) using a highly asymmetric coupler. The signal is randomly modulated following a centred Gaussian distribution in both quadratures, using amplitude and phase modulators. In order to ensure the randomness of the modulation, a Quantis true random number generator has been implemented in the system. The mean intensity of the pulses is then adjusted roughly by a variable attenuator and finely by a second amplitude modulator, so that the variance of the Gaussian distribution reaches a target value of $V_A N_0$, where N_0 is the shot-noise variance.

Time and polarization multiplexing are used so that the signal and LO are transmitted to Bob in the same optical fibre without interfering. For the time multiplexing, two delay lines are inserted into the system, one in Alice's signal path and one in Bob's LO path, as shown in figure 1. Each line is composed of a 40 m non-PM single-mode fibre followed by a Faraday mirror. The Faraday mirror is a non-reciprocal optical device composed of a standard mirror

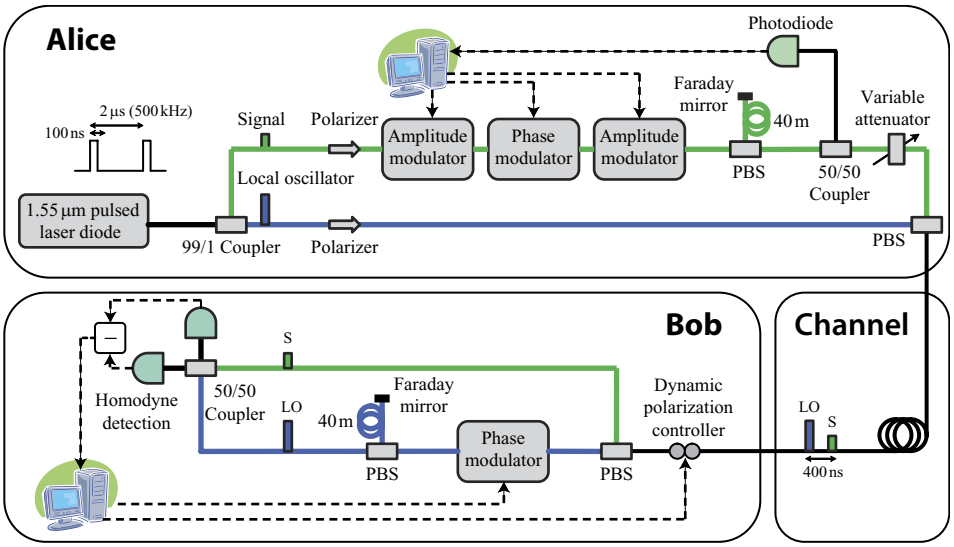

Figure 1. Optical layout of the CVQKD prototype.

and a 45° Faraday rotator; it therefore reflects the pulse by imposing a 90° rotation on its polarization. This system practically eliminates all birefringence-induced polarization drifts that the pulses experience during propagation in the delay line. Furthermore, to achieve polarization multiplexing, the pulses are coupled in the transmission fibre using a polarization beam splitter (PBS) [22, 23]. Therefore, the signal and LO pulses propagate through the quantum channel with orthogonal polarizations, and they are also delayed in time. With this configuration and provided that the quantum channel features a sufficiently low crosstalk between orthogonal polarizations, which is indeed less than −30 dB in our case, the two pulses can be demultiplexed at Bob's site very efficiently and with minimal losses, as shown in figure 1. The exact length of the delay lines is then adjusted in order to equilibrate the interferometer: the total optical path of the signal has to match the optical path of the LO, with a precision of 5 mm.

Finally, in Bob's system, the signal and LO interfere in a pulsed, shot-noise limited homodyne detector. This detection system outputs an electric signal, whose intensity is proportional to the quadrature X_ϕ of the signal, where ϕ is the phase difference between the signal and the LO. Following the implemented protocol, Bob measures randomly either X_0 or $X_{\pi/2}$ to select one of the two quadratures. For this purpose, he imposes randomly a $\pi/2$ phase shift to the local oscillator using a phase modulator placed in the LO path.

2.2. Feedback control and automation procedures

To ensure the automated operation of the described setup, we implemented several feedback control procedures to eliminate the effect of polarization and temperature drifts. More specifically, a dynamic polarization controller, placed at the output of the quantum channel as shown in figure 1, is used to correct the polarization drifts that occur in the transmission fibre because of temperature changes or mechanical strains. During system initialization, the controller explores randomly the Poincaré sphere to find an optimal polarization state at the output of the channel, and subsequently adjusts in real time this state to compensate for all such drifts.

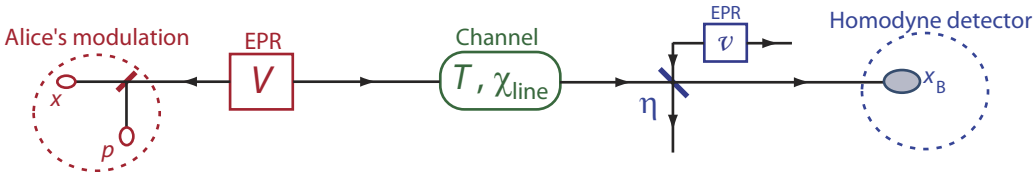

Figure 2. Schematic representation of the entanglement-based description of the CVQKD protocol.

Another implemented procedure is linked to the fact that the active material used in the amplitude and phase modulators, such as lithium niobate ($LiNbO_3$), is very sensitive to temperature changes. As a consequence, the voltages that need to be applied to reach target modulation values constantly drift with temperature. To overcome this problem, an automation software measures and corrects in real time these drifts, by analysing the outputs of the three photodiodes present in the system. In particular, the photodiode placed in Alice's signal path is used for the feedback control of the amplitude modulators, while the interference signal in the homodyne detector yields information on the relative phase between the signal and LO pulses, which is then used to control the phase modulators.

The time required for a complete feedback control of the system is 1 min, which is small compared to typical temperature drifts and allows the devices to remain in an optimal state over the entire system operation time.

3. Security of the CVQKD prototype

The security against individual Gaussian eavesdropping attacks of the coherent-state CVQKD protocol that we have implemented with reverse reconciliation was first proven in [7], and the proof was later extended to general individual attacks [10]. This was followed by security proofs against general collective attacks [11, 12]. Recently, the unconditional security of this protocol against coherent attacks, the most general attacks allowed by quantum mechanics, has also been proven [13]. Several of these proofs make the assumption that all the losses and detection-added noise present in Bob's apparatus are available to the eavesdropper. In a more realistic setting, however, Eve does not have access to Bob's system [7, 15]. For the practical prototype we have implemented, we have therefore taken into account this 'realistic' assumption.

In the following, we review the results for security against general collective attacks when Eve does not have access to Bob's setup and when Alice and Bob use Bob's data to extract the final secret key (reverse reconciliation) [7]. Since coherent attacks were shown not to be more powerful than collective attacks for the implemented protocol [13], the following expressions remain valid for this case as well, guaranteeing the unconditional security of the corresponding CVQKD system.

The security proofs against collective attacks rely on an entanglement-based description of the protocol, shown in figure 2, which is formally equivalent to the prepare-and-measure scheme presented in the previous section. In this scheme, Alice's bi-Gaussian modulation is modelled by an EPR state of variance V, on one half of which Alice performs a measurement of both quadratures. Bob's detector noise and losses are modelled by a beamsplitter, one input of which is the output state of the quantum channel and the other one half of an EPR state of appropriate

variance. Based on this description, the final secret information available to Alice and Bob is given by the expression [15]:

$$\Delta I = \beta\, I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{1}$$

where β is the reconciliation efficiency, discussed in section 5.3, and

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2 \frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}$$

$$\chi_{\mathrm{BE}} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right)$$

with

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \quad \chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/T,$$

$$\chi_{\mathrm{line}} = 1/T - 1 + \varepsilon, \quad \chi_{\mathrm{hom}} = (1+v_{\mathrm{el}})/\eta - 1,$$

$$\lambda^2_{1,2} = \tfrac{1}{2}(A \pm \sqrt{A^2 - 4B}), \quad \lambda^2_{3,4} = \tfrac{1}{2}(C \pm \sqrt{C^2 - 4D}),$$

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{\mathrm{line}})^2, \; B = T^2(V\chi_{\mathrm{line}} + 1)^2,$$

$$C = \frac{V\sqrt{B} + T(V+\chi_{\mathrm{line}}) + A\chi_{\mathrm{hom}}}{T(V+\chi_{\mathrm{tot}})}, \quad D = \sqrt{B}\frac{V+\sqrt{B}\chi_{\mathrm{hom}}}{T(V+\chi_{\mathrm{tot}})}.$$

In the above expressions, $V_{\mathrm{A}} = V - 1$ is Alice's modulation variance at the input of the channel, expressed in shot-noise units, T is the transmission efficiency of the quantum channel, ε is the excess noise at the channel's input, η is the global transmission efficiency of Bob's apparatus, v_{el} is the noise (mostly electronic) at Bob's setup input, and $\lambda_{1,2,3,4} \geqslant 1$. Given the parameters V_{A}, T, ε, η and v_{el}, Alice and Bob can therefore calculate the information they share after the quantum communication, I_{AB}, as well the maximal bound on the information available to the eavesdropper, χ_{BE}. They can then derive from equation (1) the maximal amount of secret information they can extract from their continuous data to form the secret key.

The security provided by the CVQKD prototype that we have implemented corresponds to the above analysis and, in the following sections, the theoretical values for the secret key generation rate are derived using equation (1).

4. From continuous data to a secret key

4.1. General scheme

In the previous sections, we have discussed in detail the quantum transmission phase of the coherent-state CVQKD protocol. In CV QKD, however, a significant amount of data post-processing is also required, which presents important differences compared to discrete-variable or distributed-phase-reference QKD schemes. In those protocols, when an ideal system with no detector dark noise is considered, and when no eavesdropper is present, the error rate is zero, hence the sifted data of Alice and Bob are identical. On the other hand, in CVQKD, even with a noiseless detector and no eavesdropping, Bob's measurements are always affected by Heisenberg uncertainty relations, which result in a fundamental quantum noise, the so-called shot noise, added to every quadrature measurement. Therefore, after quantum transmission, Alice and Bob do not share identical quadrature values, but only correlated data.

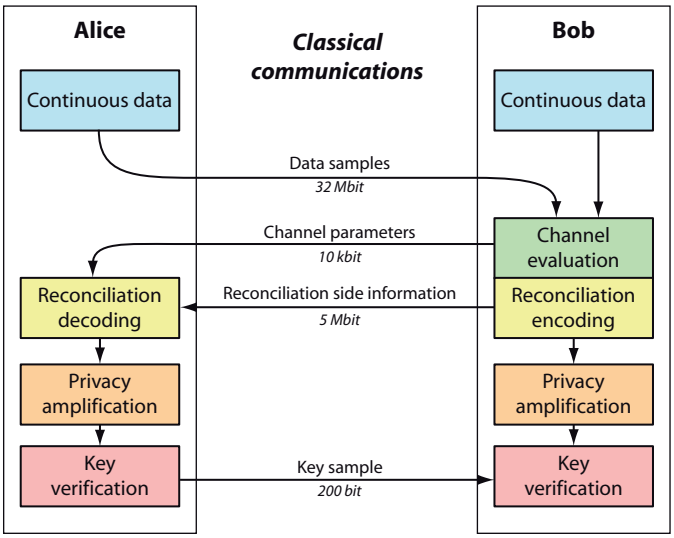

Figure 3. Block description of the data post-processing steps. The size of the data sent between Alice and Bob on the classical channel corresponds to the number of transmitted bits necessary to extract one secret key. In the current implementation, 2 million pulses are used for each key generation. The amplitude and phase (coded on 16 bits) of 1 million of them are sent for the channel evaluation, and the remaining 1 million are the material used for the key generation. With the parameters given in section 5.1, the final key size is typically of the order of 150 000 bits, for a total processing time of 20 s.

The various steps performed by Alice and Bob to convert their partially secret correlated continuous data into perfectly secure identical discrete data, i.e. a secret key, are summarized in figure 3. First, Alice and Bob need to evaluate the parameters of the transmission. Alice sends for this purpose random samples of her data to Bob, who compares them with his data. In this way, the parameters V_A, T and ε that appear in the calculations are evaluated. The parameters v_{el} and η are determined before the transmission by a calibration of Bob's apparatus. Using equation (1), Alice and Bob can then estimate the secret information ΔI present in the shared data.

Subsequently, Alice and Bob apply an error-correction (or reconciliation) algorithm to their data. In particular, in the prototype that we have implemented, they first discretize their respective continuous data by dividing the Gaussian distribution of each quadrature in 16 slots, and attributing to each continuous value a 4-bit label corresponding to its position in the distribution. After this process, in order for Alice to correct the errors that appear in her data with respect to Bob's data (reverse reconciliation), the two parties perform a multilevel reconciliation process based on low-density parity-check (LDPC) codes, which has been described in detail in [15]. This process has a finite efficiency, which plays a crucial role in the performance of the CVQKD system, as we will see in section 5.3. The reconciliation process also inevitably reveals to the eavesdropper a certain amount of side information, which has to be taken into account during the next phases of the data processing.

After reconciliation, Alice and Bob share identical discrete data, which are only partially secret. To extract the secret information present in this data, Alice and Bob use privacy amplification algorithms based on hash functions that combine the information known to Eve

with the information she ignores, yielding at the end of the process a shorter bit sequence entirely unknown to her. This output sequence is the perfectly secure key shared by Alice and Bob. Note that, for computational speed reasons, we use a combination of two hash functions chosen respectively from a non-universal family that allows rapid computation, and from a universal family that is slower to process. As described in [15], using a correct combination of these two families allows in practice the same security parameters as using a single universal family.

The last step of the data post-processing procedure shown in figure 3, such as key verification, is described below.

4.2. Integration into a real-size network and real-time operation requirements

The CVQKD prototype has been specifically developed to satisfy the requirements of the European Integrated project SECOQC [17]. This project aimed at developing a metropolitan-size QKD network implemented on preinstalled optical fibres, and led to a real-size demonstration of such a network in October 2008, on the Siemens fibre network of Vienna. The fundamental communication layer of this network, called 'quantum backbone', is composed of seven QKD links, based on five different technologies [15], [18]–[21]. The systems of this layer distribute keys between two points of the network; these keys can therefore only be used for a point-to-point secret message transmission. On top of this backbone, several networking layers are implemented, in order to transform the grid of point-to-point connections into a network that allows a user to transmit a secret message between two distant points, not necessarily directly connected by a QKD link, with unconditional security. On the uppermost layer of the network, practical applications such as secure phone communications or private bank transactions, can be implemented.

In order to meet the requirements imposed by such an architecture, and to ensure long-term system operation without human intervention, several features and verifications were implemented in the prototype software. In particular, as explained in detail in [15], there is a non-negligible probability that the LDPC codes leave a certain number of errors in the final sequence. Most of the time, these can be deterministically corrected using a Bose–Ray-Chaudhuri and Hocquenghem (BCH) code [24, 25]. However, if too many errors remain, the BCH code is unable to correct them, and thus Alice and Bob's data are different. Now, in the case of a network such as the SECOQC one, providing the upper network layers with slightly different keys results in loss of synchronization and ultimately in a transmission halt. It is therefore necessary to perform key verification, after the privacy amplification process. The most important property of the hash functions used in privacy amplification is that a single difference in two input bit sequences results in completely different output keys, but two identical input sequences always yield the same output. Hence, to verify the sequences, we compare a random sample of length n of the final keys of Alice and Bob. The probability of failure of this verification process, that is the probability of using an identical sample while the keys are different, is of the order of 2^{-n}. In our case, $n = 200$ is chosen, which yields a probability of error of 10^{-60}.

5. Results and discussion

The experiments that we present in this section took place during the field implementation of the SECOQC quantum cryptography network in Vienna, in October 2008. A first prototype based

on the setup presented in [15] was installed in Vienna in April 2008, and was then replaced by the advanced prototype presented in this work.

5.1. System calibration

Before performing the QKD experiments, it is essential to perform system calibration. More specifically, there are three basic parameters, expressed in shot-noise units, that determine the secret information rate: the modulation variance V_A (at the input of the channel), the variance V_B of the data measured by Bob, and the correlation $\rho^2 = \langle X_A X_B \rangle^2 / V_A V_B$ between the data of Alice and Bob. The value of the correlation ρ^2 is independent of any calibration. In order to determine V_A and V_B from the accessible experimental variances $V_A N_0$ and $V_B N_0$, it is necessary to calibrate the value of the shot noise, N_0. This is achieved by measuring the variance of Bob's data when only the local oscillator is present, i.e. $N = N_0 + v_{el}$, and by subtracting the electronic noise variance v_{el} measured when neither the signal nor the LO are present. In addition to N_0 and v_{el}, it is also necessary to determine the transmission efficiency of Bob's apparatus, η. Following the described process, the calibration of Bob's apparatus yields a transmission efficiency $\eta = 0.6$ and an electronic noise $v_{el} N_0 = 0.01 N_0$. Furthermore, when imposing a modulation variance $V_A N_0 = 10 N_0$, the measured excess noise is typically $0 \leqslant \varepsilon N_0 < 0.01 N_0$, depending on the surrounding noise and vibration conditions.

After the calibration procedure, the setups of Alice and Bob are placed at each side of a preinstalled optical fibre featuring a transmission efficiency $T = 0.51$. This efficiency corresponds to a standard 15 km optical fibre. In practice, the optical fibre used by the CV QKD prototype in the SECOQC quantum network was particularly lossy and its length was 9 km.

Note that the mean number of photons $\langle \hat{n}_A \rangle$ in the pulses can be determined from the modulation variance, by using $\hat{n}_A = \hat{a}^\dagger \hat{a}$, and

$$2\,(V_A + 1) = \frac{\langle \hat{X}^2 + \hat{P}^2 \rangle}{N_0} = 2\langle \hat{a}\hat{a}^\dagger + \hat{a}^\dagger \hat{a} \rangle = 4\langle \hat{n}_A \rangle + 2, \tag{2}$$

which implies $\langle \hat{n}_A \rangle = V_A/2$. Taking into account the previous parameters, we determine $\langle \hat{n}_A \rangle = 5$ photons pulse^{-1} at Alice's output, and $\langle \hat{n}_B \rangle = 1.5$ photons pulse^{-1} at the detector.

Based on the above measured parameters, the expected secret key generation rate with a reconciliation efficiency $\beta = 1$, calculated using equation (1) and with an optical emission rate of 500 kHz, is $\Delta I \approx 100$ kbit s^{-1}.

5.2. Prototype stability

During the six months that the prototypes were in operation several stability tests were made possible. The optoelectronic part of the prototypes did not require any human intervention; in particular, the optical pulse generation system and the detection system were in continuous operation during the entire period at a rate of 500 kHz without downtime. Furthermore, the birefringence, and consequently the polarization, in the installed fibre typically varied ten times slower than a laboratory fibre spool of equivalent length, facilitating the compensation of drifts of this nature.

On the contrary, phase drifts that occur because of temperature changes or vibrations in the environment can lead to important instability of the system. Indeed, as shown in figure 1, the

entire device is a Mach–Zehnder interferometer, in which the two paths are separated just after the laser diode and interfere in the homodyne detector. In the setups of both Alice and Bob, the LO and signal paths are separated by 80 m, which leads to relative phase drifts over time.

These phase drifts do not have a noticeable effect on the excess noise as long as their typical variation time is long relatively to the length of the data block used to evaluate the phase. This block is composed of 50 000 data points, emitted in 100 ms, while the phase drift linked to temperature changes in the devices is typically of 2π every 30 s. The effect of temperature on the excess noise is therefore small. Moreover, this drift is almost linear over 1 s, which makes possible an almost perfect control of the phase per pulse, by imposing an opposite linear phase ramp on Bob's phase modulator. The effect of vibrations of the racks containing the devices due to the surrounding environment, however, is more difficult to control. These vibrations have a typical frequency of 50–1000 Hz, which is fast compared to the phase evaluation frequency. Since these rapid phase variations cannot be modelled or controlled, it is necessary to isolate the optical devices mechanically. Anti-vibration mountings were placed between the racks and the metal plate supporting the optics to improve the mechanical isolation; nevertheless, the measured excess noise can reach $0.1N_0$ in the worst conditions.

Finally, concerning the software part of the prototype, and in particular the classical algorithms and network interface, significant combined efforts of the network developing team of the SECOQC project and the QKD teams participating in the network, led to good stability as well as compatibility of all the systems with the central network managing program.

5.3. Prototype performance during the SECOQC QKD network implementation

As we mentioned in section 5.1, the theoretically expected secret key generation rate of the CVQKD prototype, given the measured system parameters, is 100 kbit s^{-1}. However, the actual rate produced by the system during the QKD experiments that we performed was one order of magnitude lower than this value. There are several reasons why this decrease occurs, and it is actually very important to take into account such considerations when designing a practical QKD system for use in real networks. Figure 4 summarizes the various key drops that occur in the system, which are detailed below.

In most discrete-variable QKD systems, the secret key generation rate is limited by the detector technology, especially regarding dark noise and maximum detection rate. In CVQKD, the optical and optoelectronic components are not the limiting factor; in fact, all the optical components (including the photodiodes) would be able to operate at an optical rate increased by a factor of 100, which would be the case, for example, if 5 ns pulses emitted at a rate of 50 MHz were used. The limitations of the CVQKD system in terms of secret key generation rate are mainly due to insufficient computational speed and to the effects of environmental perturbations.

More specifically, the first reason for the key rate drop (part (a) of figure 4) is the excess noise induced by the vibrational environment of the prototype. As we observe in figure 5, which shows the results for the secret key generation rate and the excess noise as a function of time during the CVQKD prototype field test, the excess noise varies considerably with time, typically between 0 and 10% of the shot noise. This variation has a direct effect on the secret information rate, as illustrated in figure 6.

The second reason for the key rate decrease (part (b) of figure 4) is the finite efficiency of the reconciliation phase of the protocol. As we mentioned in section 4.1, the information

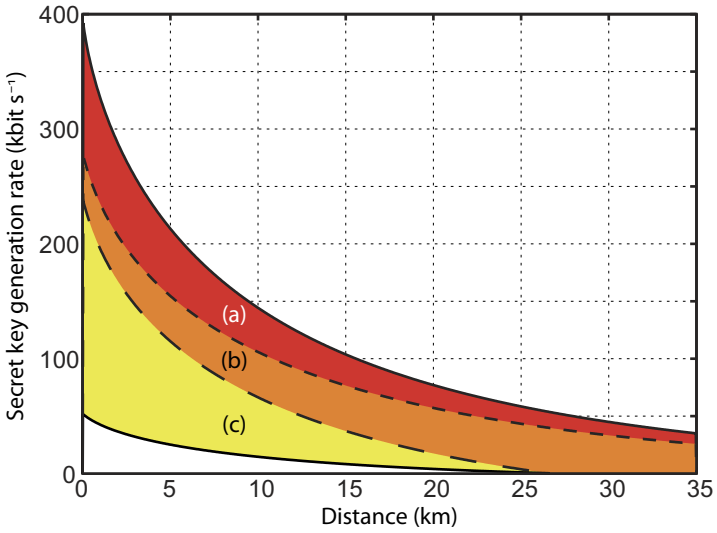

Figure 4. Summary of the practical reasons for the decrease of the secret key generation rate. The upper solid curve represents the maximum theoretical rate attainable by the system. (a) Drop in rate due to a realistic excess noise of 4%. (b) Drop due to a limited reconciliation efficiency of 90%. (c) Drop due to the current impossibility to postprocess all the data at the optical emission rate. The lower solid curve is the practical achievable secret key distribution rate. The curves are drawn using the standard optical fibre loss coefficient of 0.2 dB km^{-1}.

I_{AB} available in the data cannot in practice be entirely extracted, and this effect is taken into account by introducing the parameter β that appears in equation (1). In the prototype that we have implemented, $\beta = 0.9$. It is important to note that the finite reconciliation efficiency is also directly linked to the limited transmission distance of the prototype: finding ways of increasing the efficiency of the reconciliation process can result in a significant increase in its range [26].

Another major decrease in the secret key generation rate (part (c) of figure 4) stems from the limitations in computational speed of the processor used for data post-processing. Indeed, the reconciliation and privacy amplification algorithms are complex and very demanding in terms of computational power. The speed optimization of these algorithms depends on many parameters; in particular, there is a trade-off concerning the length of the set of data used to evaluate the parameters: a long set of data decreases the statistical uncertainty on the parameter evaluation, but increases the time required to process the data. For the field test, we chose a length of 2 million pulses per key. The optical emission of this set of pulses takes 5 s with the current optical pulse rate, while the reconciliation of the data (4 million bits) typically lasts 24 s and the privacy amplification algorithm another 5 s. As a direct consequence, when the system works continuously, one processor core is not sufficient to achieve real-time classical post-processing, which directly results in a loss of a factor of 6 between the optically available secret key rate and the final extracted rate. By using a quadruple-core processor, we have been able to implement three post-processing operations in parallel, which resulted in an increase of the secret key rate by a 2.1 factor, however even with this improvement the processing rate is still 3 times slower than the optical rate.

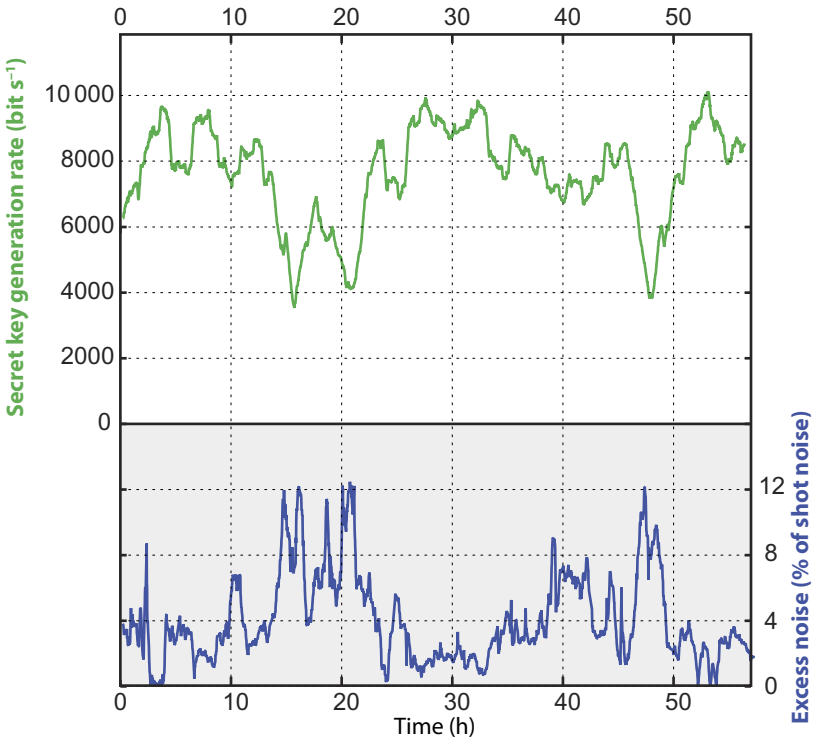

Figure 5. Secret key generation rate and excess noise of the system as a function of time. Both curves represent floating averages: over 100 successive keys for the excess noise, and over 1 h for the secret key rates. This averaging explains the differences between the theoretical key rate shown in figure 6 and the actual key rate shown here.

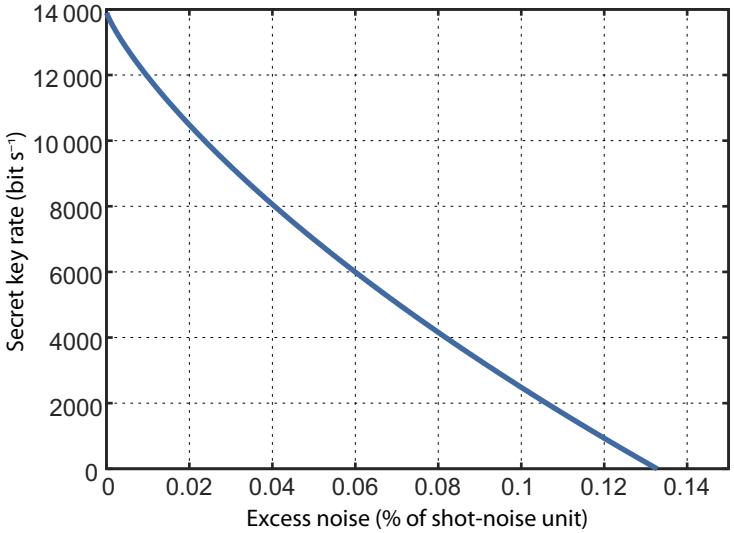

Figure 6. Secret key generation rate as a function of excess noise, with all the other parameters fixed as in section 5.1.

Finally, the classical communication that is necessary to transmit the various samples needed for channel evaluation and the side information required for reconciliation has a significant effect, which is dependent on the protocol and the implementation of these procedures. As shown in figure 3, the size of the transmitted messages is quite important in our case, and adds 5 s to the key extraction time. On the other hand, most two-way reconciliation algorithms (such as CASCADE) require numerous transmissions of small messages; the message transmission in itself is therefore negligible but the accumulated latency of all the transmissions can lead to important delays. In addition to these delays, a certain amount of key material is used for authentication purposes. In our case, the authentication requires typically 128 bits for every key generated ($\approx$150 000 bits), which is negligible.

In the field test, given all the factors described above, the CVQKD prototype generated secret keys during 57 h with an average rate of 8 kbit s^{-1}, as shown in figure 5. From figure 4, we can see that the maximal attainable communication distance with the current parameters is 27 km, and that the rate increases significantly when the transmission loss decreases. The prototype is therefore particularly adapted to metropolitan communications (up to 20 km) with high-speed requirements.

5.4. Discussion and future developments

The presented results clearly show that developing a table-top laboratory QKD system is a very different procedure than developing a prototype for integration into a realistic environment. Since one of the basic rules of QKD is to systematically attribute the practical imperfections to an eavesdropper's action, stability is of utmost importance, and the operational electromagnetic, vibrational or luminous environment can have a dramatic effect on system performance. Furthermore, the effects related to software cannot be neglected, since QKD systems are designed to work in combination with encrypters and network components, and interactions with such systems often lead to latencies or instabilities.

In the case of the CVQKD prototype, the two main factors that lead to a suboptimal system performance, such as vibrations and computer processor limitations, can certainly be eliminated. In order to avoid all mechanical-induced effects on the phase of the interferometer, the apparatuses should be specifically designed to prevent fibres from vibrating. Concerning the post-processing speed, the system performance is clearly directly affected by the steady increase in computer performance, but optimization work is still possible to achieve faster and more efficient reconciliation. In particular, the massive computing parallelization made possible by new-generation graphical processors is particularly adapted to LDPC-based algorithms. The implementation of such algorithms on graphical processors therefore offers a promising research direction. In parallel with these developments, new algorithms, which aim at reaching longer communication distances and higher secret key generation rates based on more efficient reconciliation, are currently being designed [26].

6. Conclusion

The CVQKD prototype that we have realized has been integrated into a quantum cryptography telecommunication network, and yielded an average secret key generation rate of 8 kbit s^{-1} over a 3 dB loss fibre, during 57 h. Time and polarization multiplexing have been used to transmit the signal and local oscillator in the same quantum channel, and complex feedback

control procedures have been implemented to ensure a stable and automatic operation without human intervention. The system has been proven secure against general coherent eavesdropping attacks. The secret key generation rate is currently mainly limited by the computing possibilities of the system's processor. In parallel with further stabilization of the interferometer's phase, work is currently in progress to increase the speed of classical post-processing. This will allow an increase in the pulse generation rate, and therefore a significant improvement in the final secret key generation rate. With these improvements, the CVQKD prototype can ultimately provide metropolitan-size networks with secret keys generated at rates greater than 100 kbit s^{-1}, an objective that appears to be within reach in the near future.

Acknowledgments

Financial support for this work was provided by the Integrated European Project SECOQC (grant no. IST-2002-506813) and the French National Research Agency Project SEQURE. ED acknowledges support from the European Union through a Marie-Curie fellowship and a Marie-Curie reintegration grant.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155 [quant-ph]
[2] Ralph T C 1999 *Phys. Rev.* A **61** 010303
[3] Hillery M 2000 *Phys. Rev.* A **61** 022309
[4] Cerf N J, Lévy M and Van Assche G 2001 *Phys. Rev.* A **63** 052311
[5] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[6] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[7] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier G 2003 *Nature* **421** 238
[8] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[9] Heid M and Lütkenhaus N 2007 *Phys. Rev.* A **76** 022313
[10] Grosshans F and Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905
[11] Navasqués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
[12] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[13] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[14] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev.* A **72** 050303
[15] Lodewyck J *et al* 2007 *Phys. Rev.* A **76** 042305
[16] Lodewyck J, Debuisschert T, García-Patrón R, Tualle-Brouri R, Cerf N J and Grangier P 2007 *Phys. Rev. Lett.* **98** 030503
[17] http://www.secoqc.net
[18] Yuan Z L, Dixton A R, Dynes J F, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **92** 201104
[19] Poppe A *et al* 2004 *Opt. Express* **12** 3865
[20] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[21] http://www.idquantique.com
[22] Marand C and Townsend P D 1995 *Opt. Lett.* **20** 1965
[23] Qi B, Huang L-L, Qian L and Lo H-K 2007 *Phys. Rev.* A **76** 052323
[24] Bose R C and Ray-Chaudhuri D K 1960 *Inf. Control* **3** 68–79
[25] Hocquenghem A 1959 *Chiffres* **2** 147–56
[26] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev.* A **77** 042325