New Journal of Physics

An Institute of Physics and Deutsche Physikalische Gesellschaft Journal

Quantum key distribution over 67 km with a plug&play system

D Stucki[1], **N Gisin**[1], **O Guinnard**[1,2], **G Ribordy**[1,2] **and H Zbinden**[1]

[1] GAP-Optique, University of Geneva, rue de l'Ecole-de-Médecine 20,
CH-1211 Geneva 4, Switzerland
[2] id Quantique SA, rue Cingria 10, CH-1205 Geneva, Switzerland
E-mail: hugo.zbinden@physics.unige.ch

New Journal of Physics **4** (2002) 41.1–41.8 (http://www.njp.org/)
Received 7 March 2002
Published 12 July 2002

Abstract. We present a fibre-optical quantum key distribution system. It works at 1550 nm and is based on the plug&play set-up. We tested the stability under field conditions using aerial and terrestrial cables and performed a key exchange over 67 km between Geneva and Lausanne.

1. Introduction

Quantum cryptography or, more exactly, quantum key distribution (QKD) is the most advanced subject in the field of quantum information technologies. Since the introduction of the BB84 protocol by Bennett and Brassard in 1984 [1] and their first implementation in 1992 [2], many experiments have been performed by numerous groups (see e.g. [3] for a review). However, to our knowledge, all experiments to date have been performed in laboratories or used laboratory equipment (e.g. liquid nitrogen cooled detectors) or needed frequent alignments (e.g. control of polarization or phase). In this paper, we present a turn-key, fibre-optic QKD-prototype that fits into two 19 inch boxes, one for Alice and one for Bob (see figure 1). We tested the stability of the auto-compensating plug&play (p&p) system [4] over installed terrestrial and aerial cables. Keys were exchanged over a distance of 67 km.

We start with a short introduction to the p&p auto-compensating set-up and describe the features of the prototype. We then recall the relevant parameters of a QKD system and briefly discuss some security issues. Finally the results of the field tests are presented.

2. Plug&play prototype

Let us recall the principle of the so-called p&p auto-compensating set-up [4]–[8], where the key is encoded in the phase between two pulses travelling from Bob to Alice and back (see figure 2).

1367-2630/02/000041+8$30.00

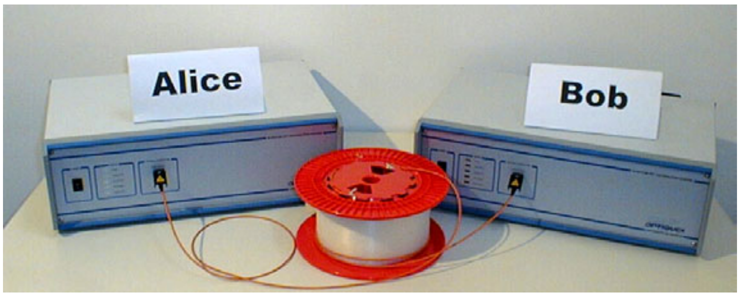

Figure 1. Picture of the p&p system.

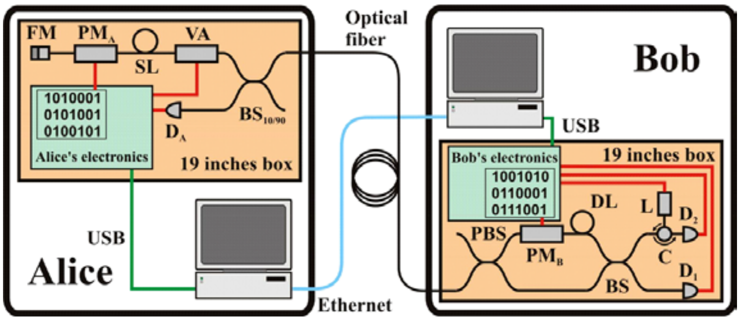

Figure 2. Schematic of the p&p prototype.

A strong laser pulse (@1550 nm) emitted at Bob is separated at a first $50/50$ beamsplitter (BS). The two pulses impinge on the input ports of a polarization beamsplitter (PBS), after having travelled through a short arm and a long arm, including a phase modulator (PM$_B$) and a 50 ns delay line (DL), respectively. All fibres and optical elements at Bob are polarization maintaining. The linear polarization is turned by $90°$ in the short arm, therefore the two pulses exit Bob's set-up by the same port of the PBS. The pulses travel down to Alice, are reflected on a Faraday mirror, attenuated and come back orthogonally polarized. In turn, both pulses now take the other path at Bob and arrive at the same time at the BS where they interfere. Then, they are detected either in D$_1$, or after passing through the circulator (C) in D$_2$. Since the two pulses take the same path, inside Bob in reversed order, this interferometer is auto-compensated. To implement the BB84 protocol, Alice applies a phase shift of 0 or π and $\frac{\pi}{2}$ or $\frac{3\pi}{2}$ on the second pulse with PM$_A$. Bob chooses the measurement basis by applying a 0 or $\frac{\pi}{2}$ shift on the first pulse on its way back.

The prototype is easy to use. The two boxes just have to be connected via an optical fibre. They are exclusively driven by two computers via the USB port. The two computers communicate via an ethernet/internet link. The system monitors on-line the temperature of the detectors, heat sinks and casings. The photon counters are Peltier-cooled, actively gated, InGaAs/InP APDs [9]. The dark count noise of the detectors is measured during the initialization (the dark count probability p_{dark} is $\approx 10^{-5}$ per gate). Although the set-up needs no optical alignment, the phases and the detection gates must be applied at the right time. Therefore, the system measures in a next step the length of the link (the operator has only to estimate the line's length to within 5 km). The variable attenuator (VA) at Alice is set to a low level and bright laser pulses are emitted by Bob. The time delay between the triggering of the laser and a train of gates of the detectors is scanned until the reflected pulses are detected. The delays for the two 2.5 ns detection gates are adjusted, as well as the timing for the 50 ns pulse applied on the phasemodulator PM$_B$. In the p&p scheme, where pulses travel back and forth, (Rayleigh) backscattered light can considerably increase the noise. Therefore, the laser is not continuously pulsed, but trains of pulses are sent, the length of these trains corresponding to the length of the storage-line introduced for this purpose behind the attenuator at Alice's station [5]. Consequently, the backward propagating pulses no longer cross bright pulses in the fibre. For a storage line measuring approximately 10 km, a pulse train contains 480 pulses at a frequency of 5 MHz. A 90% coupler (BS$_{10/90}$) directs most of the incoming light pulses to a APD-detector module (D$_A$). It generates the trigger signal used to synchronize Alice's 20 MHz clock with the one of Bob. This synchronized clock allows Alice to apply a 50 ns pulse at the phasemodulator PM$_A$ exactly when the second, weaker pulse passes. Only this second pulse contains phase information and must be attenuated below the one-photon-per-pulse level. Measuring the height of the incoming pulses with D$_A$ would allow one to adjust the attenuator in order to obtain the correct average number of photons per outgoing pulse. For this purpose, the attenuator and the detector must be calibrated beforehand. In practice, we measure the incoming power with a power metre. Random numbers are generated on both sides with a quantum random number generator [10]. At Bob, clicks from each of the photon counters are written together with the index of the pulse into a buffer and transferred to the computer.

As a measure of security, the number of coincident clicks at both detectors is registered, which is important to limit beamsplitting attacks (see below). Moreover, the incoming power at Alice is continuously measured with D$_A$, in order to detect so-called Trojan horse attacks.

3. Key parameters in QKD

3.1. Key and error rates

The first important parameter is the raw key rate R_{raw} between Alice, the transmitter, and Bob, the receiver:

$$R_{raw} = q\nu\mu t_{AB} t_B \eta_B \tag{1}$$

where q depends on the implementation ($\frac{1}{2}$ for the BB84 protocol, because half the time Alice and Bob bases are not compatible), ν is the repetition frequency, μ is the average number of photons per pulse, t_{AB} is the transmission on the line Alice–Bob, t_B is Bob's internal transmission ($t_B \approx 0.6$) and η_B is Bob's detection efficiency ($\eta_B \approx 0.1$).

After R_{raw} the second most important parameter is the quantum bit error rate (*QBER*) which consists of four major contributions:

$$QBER = \frac{\text{false counts}}{\text{total counts}} = QBER_{opt} + QBER_{dark} + QBER_{after} + QBER_{stray}. \tag{2}$$

$QBER_{opt}$ is simply the probability for a photon to hit the wrong detector. It can be measured with strong pulses, by always applying the same phases and measuring the ratio of the count rates at the two detectors. This is a measure of the quality of the optical alignment of the polarization maintaining components and the stability of the fibre link. In the ideal case, $QBER_{opt}$ is independent of the fibre length. $QBER_{dark}$ and $QBER_{after}$, the errors due to dark counts and after-pulses, depend on the characteristics of the photon counters [9]. $QBER_{dark}$ is the most important, it is the probability to have a dark count per gate p_{dark}, divided by the probability to have a click p_{det}:

$$QBER_{dark} \cong \frac{p_{dark}}{\mu t_{AB} t_B \eta_B}.$$

$QBER_{dark}$ increases with distance and consequently limits the range of QKD. $QBER_{after}$ is the probability to have an after-pulse $p_{after}(t)$ summed over all gates between two detections:

$$QBER_{after} \cong \sum_{n=0}^{n=\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{\nu}\right) \tag{3}$$

where τ is the dead time, during which the detectors' gate are inhibited after each detection. The probability p_{after} depends on the type of APD as well as on the temperature, and decreases rapidly with time [9]. Nevertheless, for high pulse rates ($\nu = 5$ MHz) $QBER_{after}$ can become significant. For instance, for $p_{det} = 0.15\%$ (corresponding to about 7 dB loss with $\mu = 0.1$) we measured a $QBER_{after}$ of about 4%. By introducing a dead time τ of 4 μs (during this time, following a detection, no gates are applied), $QBER_{after}$ can be reduced to 1.5%. The bit rate R_{raw} in contrast, is only slightly reduced by a factor η_τ:

$$\eta_\tau = \frac{1}{1 + \nu p_{det} \tau} \lessapprox 1. \tag{4}$$

In this example, η_τ becomes 0.97 and 0.92, for 4 and 12 μs, respectively. In our prototype the dead time can be varied between 0 and 12 μs. The optimum dead time varies as a function of distance, in our measurements, however, we applied a constant dead time of 4 μs. Finally, $QBER_{stray}$, the errors induced by stray light, essentially Rayleigh back-scattered light, is a problem proper to the p&p set-up. It can be almost completely removed with the help of Alice's storage line and by sending trains of pulses as mentioned above. However, we have to introduce another factor η_{duty} that reduces our bit rate. It gives the duty cycle of the emitted pulse trains and depends on the length of Alice's DL l_D and the length of the fibre link l_{AB}:

$$\eta_{duty} = \frac{l_D}{l_{AB} + l_D}. \tag{5}$$

Hence with our prototype we can expect a raw rate of R_{raw} of about

$$R_{raw} = q\nu\mu t_{AB} t_B \eta_B \eta_{duty} \eta_\tau \approx 140\ \text{kHz}\left(\mu t_{AB} \frac{l_D}{l_{AB} + l_D}\right). \tag{6}$$

3.2. *Error correction, privacy amplification and eavesdropping*

The net secret key rate is further reduced during the error correction and privacy amplification processes by a factor of η_{dist}. We did not implement error correction and privacy amplification for our field tests, but we would like to roughly estimate the net key rate that could be obtained with our system. In theory, η_{dist} is simply given as the difference between the mutual information of Alice and Bob, I_{AB}, and Alice and Eve, I_{AE} [3]:

$$\eta_{dist} = I_{AB}(D) - I_{AE}. \tag{7}$$

Due to the errors, I_{AB} is smaller than 1. It is a function of the disturbance D, which is equal to the total $QBER$:

$$I_{AB} = 1 + D\log_2 D + (1 - D)\log_2(1 - D). \tag{8}$$

In the following we estimate the information of Eve, I_{AE}. In the line of Felix *et al* [11] we make the following assumptions:

• The measured *QBER* should, within the statistical limits, be equal to what is estimated according equation (2). If this is not the case, a real user will not proceed and blindly apply privacy amplification, he will stop the key exchange and look for the problem. If the *QBER* is within these limits, we attribute to Eve the $QBER_{opt}$ ($\lesssim 0.5\%$) plus the error (2σ) of the error estimation ($\lesssim 0.5\%$ for reasonably long keys), say 1% in total. In the case of perfect equipment of the eavesdropper and true single-photon source this error corresponds to an information of $\frac{2}{\ln 2} 1\% \cong 3\%$ [13].

• In the case of faint laser pulses and especially in the presence of high fibre losses, Eve can take advantage of multi-photon pulses and gain information while creating few or no errors [11]. In this case, it is important to measure the length of the line and to register coincident clicks at Bob's two detectors in order to limit Eve's possibilities. We assume that Eve possesses perfect technology, but cannot efficiently measure the number of photons without disturbing them and cannot store them. Furthermore, she uses fibres with losses as low as 0.15 dB km^{-1}. Under these assumptions one can calculate Eve's information per bit due to multi-photon pulses $I_{2\nu}$ and obtains about 0.06, 0.14 and 0.40 for, 5, 10 and 20 dB losses, respectively (for $\mu = 0.2$, 0.25 dB km^{-1} fibre loss and 10^8 pulses sent). Consequently, we obtain

$$I_{AE} \cong 0.03 + I_{2\nu}. \tag{9}$$

With equations (7)–(9) we can calculate a theoretical value of η_{dist}. In practice, η_{dist} will be smaller due to the limitations of the used algorithm. Privacy amplification can be performed without additional bit loss in contrast to error correction. For our estimation, we use the results of Tancewsky *et al* [12] for I'_{AB} after error correction

$$I'_{AB} = 1 + D\log_2 D - \tfrac{7}{2}D \tag{10}$$

which is in fact considerably smaller than I_{AB}. The information of Eve I_{AE} is reduced by the same factor $\frac{I'_{AB}}{I_{AB}}$, too. Finally, we obtain the following estimate of R_{net}:

$$\begin{aligned} R_{net} = \eta_{dist} R_{raw} &\cong (I_{AB} - I_{AE})\frac{I'_{AB}}{I_{AB}} R_{raw} \\ &\approx [1 + D\log_2 D - \tfrac{7}{2}D - (0.03 + I_{2\nu})(1 - (1-D)\log_2(1-D) - \tfrac{7}{2}D)]R_{raw}. \end{aligned} \tag{11}$$

4. Field measurements

4.1. Visibilities

In principle, the prototype can be tested in the laboratory by performing key exchange with different fibre losses and comparing the measured *QBER* and bit rates with the estimated values according to the simple formulae developed above. There are two motivations for field tests on installed cables. The first reason is to check if the auto-compensating set-up is robust in many different situations. Several effects could reduce the visibility of the interference. First, we have previously shown that Faraday rotation due to the Earth's magnetic field cannot considerably decrease the visibility [14]. Second, the time delay between the two pulses, travelling back and forth between Alice and Bob, could change due to a temperature drift. Let us assume that the temperature of the fibre increases with a rate $\theta[\frac{K}{h}]$. The time delay Δt between the two pulses

Table 1. Visibility measurements on different fibres.

Fibre	Length (km)	Loss (dB)	Visibility (%)
Geneva–Nyon (under lake)	22.0	4.8	99.70 ± 0.03
Geneva–Nyon (terrestrial)	22.6	7.4	99.81 ± 0.03
Nyon–Lausanne (terrestrial)	37.8	10.6	99.63 ± 0.05
Geneva–Lausanne (under lake) A	67.1	14.4	99.62 ± 0.06
Geneva–Lausanne (under lake) B	67.1	14.3	99.66 ± 0.05
Ste croix (aerial) A	8.7	3.8	99.70 ± 0.01
Ste croix (aerial) B	23.7	7.2	99.71 ± 0.01

is 54 ns. If θ is constant for the whole trip of the pulses, the second pulse will see a fibre that is longer by Δl:

$$\frac{\Delta l}{l} = \alpha \Delta T \tag{12}$$

$$\Delta l = \alpha 2 l_{AB} \Delta T = \alpha 2 l_{AB} \theta \Delta t. \tag{13}$$

With $\alpha = 10^{-5}[\frac{1}{K}]$, $l_{AB} = 50$ km, $\theta = 10[\frac{K}{h}]$ we obtain $150\ \mathrm{pm} \ll \lambda$. Hence this effect should be negligible especially since installed fibres have slow temperature drifts. In contrast, slow temperature induced length drifts can be large enough that frequent readjustment of Bob's delay becomes necessary. In fact, we noticed that during the heating up of Alice's box within the first hour of operation, the changes in the DL require a recalibration every 10 min or so. However, a bad synchronization of the detection window does not affect $QBER_{opt}$. Finally, mechanical stress could change the fibre length and/or birefringence. If the birefringence changes rapidly, the pulses are no longer orthogonally polarized at the input of Bob, despite the Faraday mirror. In this case the two pulses might suffer different losses at Bob's polarizing BS and the interference will no longer be perfect. Rapid changes in stress are unlikely in installed cables, a couple of meters below the surface. For this reason we also tested the prototype over an aerial cable. We had at our disposal two fibres of 4.35 km length, of which 2.5 km in an aerial cable. In order to amplify a hypothetical effect we put Alice and Bob side by side and passed twice through the cable (config. A). In configuration B we inserted one spool of about 15 km at the other end of the cable. Hence, the pulses made the following trip: Bob, the aerial cable, 15 km spool, the aerial cable, Alice (with her 10 km storage line), and back.

To measure the visibilities we sent relatively strong pulses (a couple of photons per pulse), always with the same compatible phase values and look at the counts on the two detectors, R_{right} and R_{wrong} (subtracting the counts due to detector noise). We then obtain the fringe visibility according to the standard definition

$$V = \frac{R_{right} - R_{wrong}}{R_{right} + R_{wrong}} \tag{14}$$

and the corresponding $QBER_{opt}$:

$$QBER_{opt} = \frac{1 - V}{2}. \tag{15}$$

Table 1 summarizes the result of visibility measurements over different cables. The indicated visibilities are the mean values over all four possible compatible phase settings. There was no

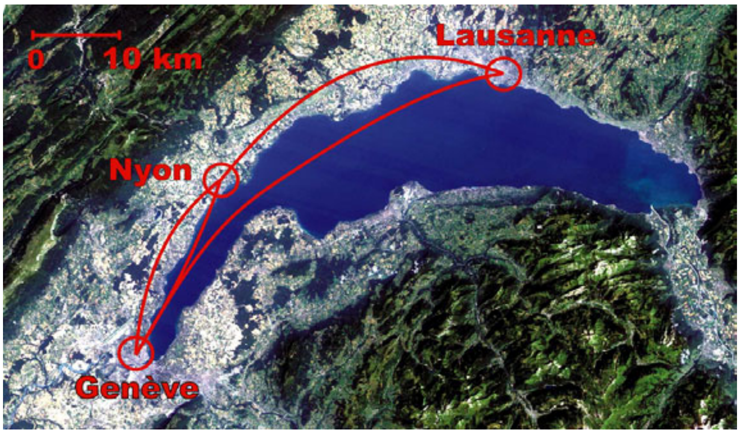

Figure 3. Satellite view of Lake Geneva with the cities of Geneva, Nyon and Lausanne.

Table 2. Overview of exchanged keys over different fibres ($\mu = 0.2$).

Fibre	Length (km)	Key (kbit)	R_{raw}(kHz)	*QBER* (%)	R_{net} (kHz)
Geneva–Nyon (under lake)	22.0	27.9	2.06	2.0 ± 0.1	1.51
Geneva–Nyon (terrestrial)	22.6	27.5	2.02	2.1 ± 0.1	1.39
Nyon–Lausanne (terrestrial)	37.8	25.1	0.50	3.9 ± 0.2	0.26
Geneva–Lausanne (under lake) A	67.1	12.9	0.15	6.1 ± 0.4	0.044
Geneva–Lausanne (under lake) B	67.1	12.9	0.16	5.6 ± 0.3	0.051
Ste Croix (aerial) A	8.7	63.8	6.29	3.0 ± 0.1	4.34
Ste Croix (aerial) B	23.7	117.6	2.32	3.0 ± 0.1	1.57

considerable decrease of the visibility in any fibre, hence the auto-compensating interferometers worked well under all conditions tested.

We tried to simulate an extremely unstable fibre link in the lab. For this purpose, we put a fibre-optical polarization scrambler (GAP-optique) at the output of Bob followed by 25 km of fibre. We measured the visibility as a function of the scrambler frequency. This frequency is defined as the number of complete circles that the vector of polarization would describe per second on the Poincaré sphere, if the birefringence changed uniformly. The visibility drops from 99.7 to 99.5% and 98% at frequencies of 40 and 100 Hz, respectively. This shows that the visibilities can decrease under rapid perturbations, however, it is unlikely to find such conditions using installed fibres.

4.2. Key exchange

We performed key exchange over different installed cables, the longest connecting the cities of Lausanne and Geneva (see figure 3). For testing we always used the same file of random numbers so that Bob could make the sifting and calculation of error rate without communication. We estimated the net key rate using equation (11). Table 2 gives an overview of the exchanged keys with $\mu = 0.2$.

We notice that secure key exchange is possible over more than 60 km with about 50 Hz of net key rate.

5. Conclusion

We presented a QKD prototype, which can be simply plugged into the wall, connected to a standard optical fibre and a computer via the USB port. It allows key exchange over more than 60 km, with a net key rate of about 50 bits s^{-1}. The system is commercially available [15].

Acknowledgments

We would like to thank Michel Peris and Christian Durussel from Swisscom for giving us access to their fibre links, as well as Laurent Guinnard and Mario Pasquali for their help with the software and firmware, Jean-Daniel Gautier and Claudio Barreiro for their help with the electronics. Finally, we thank Régis Caloz for the satellite picture. This work was supported by the Esprit project 28139 (EQCSPOT) through Swiss OFES and the NCCR 'Quantum Photonics'. We also acknowledge the support of Sun Microsystems.

References

[1] Bennett Ch H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)* pp 175–9

[2] Bennett Ch H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptograpy *Rev. Mod. Phys.* at press
(Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Preprint* quant-ph/0101098)

[4] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 Plug&play systems for quantum cryptography *Appl. Phys. Lett.* **70** 793–5

[5] Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H 2000 Fast and user-friendly quantum key distribution *J. Mod. Opt.* **47** 517–31

[6] Bethune D and Risk W 2000 An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light *IEEE J. Quantum Electron.* **36** 340–7

[7] Nielsen P M, Schori C, Sorensen J L, Savail L, Damgard I and Polzik E 2001 Experimental quantum key distribution with proven security against realistic attacks *J. Mod. Opt.* **48** 1921–42

[8] Bourennane M, Ljunggren D, Karlsson A, Jonsson P, Hening A and Ciscar J P 2000 Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols *J. Mod. Opt.* **47** 563–79

[9] Stucki D, Ribordy G, Stefanov A, Zbinden H, Rarity J G and Wall T 2001 Photon counting for quantum key distribution with Peltier cooled InGaAs APDs *J. Mod. Opt.* **48** 1967–82

[10] Stefanov A, Guinnard O, Guinnard L, Zbinden H and Gisin N 2000 Optical quantum random number generator *J. Mod. Opt.* **47** 595–8 (available from id Quantique, www.idquantique.com.)

[11] Félix S, Gisin N, Stefanov A and Zbinden H 2001 Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses *J. Mod. Opt.* **48** 2009–22

[12] Tancevski L, Slutsky B, Rao R and Fainman S 1997 *Proc. SPIE* **3228** 322

[13] Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 Optimal eavesdropping in quantum cryptography: I. *Phys. Rev.* A **56** 1163–72

[14] Zbinden H, Gisin N, Huttner B, Muller A and Tittel W 2000 Practical aspects of quantum cryptographic key distribution *J. Cryptol.* **13** 207–20

[15] id Quantique SA, www.idquantique.com