Continuous high speed coherent one-way quantum key distribution

Damien Stucki[1], Claudio Barreiro[1], Sylvain Fasel[1], Jean-Daniel Gautier[1], Olivier Gay[2], Nicolas Gisin[1], Rob Thew[1], Yann Thoma[1], Patrick Trinkler[2], Fabien Vannel[1], Hugo Zbinden[1]*

[1] Group of Applied Physics, University of Geneva, 1211, Geneva 4, Switzerland
[2] id Quantique SA, Chemin de la Marbrerie 3, 1227, Geneva, Switzerland
hugo.zbinden@unige.ch

Abstract: Quantum key distribution (QKD) is the first commercial quantum technology operating at the level of single quanta and is a leading light for quantum-enabled photonic technologies. However, controlling these quantum optical systems in real world environments presents significant challenges. For the first time, we have brought together three key concepts for future QKD systems: a simple high-speed protocol; high performance detection; and integration both, at the component level and for standard fibre network connectivity. The QKD system is capable of continuous and autonomous operation, generating secret keys in real time. Laboratory and field tests were performed and comparisons made with robust InGaAs avalanche photodiodes and superconducting detectors. We report the first real world implementation of a fully functional QKD system over a 43dB-loss (150km) transmission line in the Swisscom fibre optic network where we obtained average real-time distribution rates over 3 hours of 2.5bps.

OCIS codes: (060.0060) Fiber optics and optical communications; (270.0270 Quantum optics; (270.5565) Quantum communications; (270.5568) Quantum cryptography; (270.5570) Quantum detectors; (270.5585) Quantum information and processing; (250.1345) Avalanche photodiodes (APDs)

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145-195 (2002).
2. Commercial QKD company web sites: www.idquantique.com, www.magiqtech.com, www.smartquantum.com.
3. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New J. Phys. **4,** 41.1-41.8 (2002).
4. Z. L. Yuan, and A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," Opt. Expr. **13,** 660-665 (2005).
5. R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, "Low jitter up-conversion detectors for telecom wavelength GHz QKD," New. J. Phys **8,** 32 (2006).
6. E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km differential phase shift quantum key distribution with low jitter up-conversion detectors," Opt. Expr. **14,** 13073-13082 (2006).
7. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Appl. Phys. Lett. **92,** 201104 (2008).
8. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nature Phot. **1,** 343-348 (2007).
9. K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89,** 037902 (2002).
10. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," Phys. Rev. Lett. **92,** 057901 (2004).
11. M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," Phys. Rev. Lett. **93,** 120501 (2004).
12. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87,** 194108 (2005).

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

13. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, "Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography," Quant. Inf. Comp. **7,** 639-664 (2007).
14. W. Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91,** 057901 (2003).
15. X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," Phys. Rev. Lett. **94,** 230503 (2005).
16. H. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94,** 230504 (2005).
17. Website for BBN Technologies: www.bbn.com.
18. Website for the EU project SECOQC: www.secoqc.net.
19. Although there are still no complete formal security proofs for finite keys, initial efforts in this direction suggest the need for large blocks of data to ensure security, V. Scarani, R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," Phys Rev. Lett. **100,** 200501 (2008).
20. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, Bangalore, 1984), pp. 175-179.
21. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68,** 3121 (1992).
22. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast Quantum Cryptography," quant-ph/0411022 (2004).
23. C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," New J. Phys. **10,** 013031 (2008).
24. U. Atsushi, A. Kazuya, I. Masaki, H. Kunihito, N. Sunao, S. Hiroyuki, O. Isao, K. Takayuki, S. Masaru, Y. Shigeru, Y. Kazuyuki, and D. Peter, "Fast physical random bit generation with chaotic semiconductor lasers," Nature Phot. **2,** 728-732 (2008).
25. R. T. Thew, D. Stucki, J.-D. Gautier, H. Zbinden, and A. Rochas, "Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths," Appl. Phys. Lett. **91,** 201114 (2007).
26. R. T. Thew, H. Zbinden, and N. Gisin, "Tunable upconversion photon detector," App. Phys. Lett. **93,** 071104 (2008).
27. A. Korneev, Y. Vachtomin, O. Minaeva, A. Divochiy, K. Smirnov, O. Okunev, G. Gol'tsman, C. Zinoni, N. Chauvin, L. Balet, F. Marsili, D. Bitauld, B. Alloing, L. H. Li, A. Fiore, L. Lunghi, A. Gerardino, M. Halder, C. Jorel, and H. Zbinden, "Single-Photon Detection System for Quantum Optics Applications," Selected Topics in Quantum Electronics, IEEE Journal of Quant. Electr. **13,** 944-951 (2007).
28. Website for the EU project Sinphonia: www.sinphonia.org.
29. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology - EUROCRYPT `93. Workshop on the Theory and Application of Cryptographic Techniques - Proceedings* (Springer-Verlag, Berlin, 1994), pp. 410-423.
30. M. N. Wegman, L. Carter, "New Hash Functions and Their Use in Authentication and Set Equality," J. Comput. Syst. Sci. **22,** 265-279 (1981).
31. L. Carter, M. N. Wegman, "Universal Classes of Hash Functions," J. Comput. Syst. Sci. **18,** 143-154 (1979).
32. J. Zhang, R. T. Thew, J.-D Gautier, N. Gisin, and H. Zbinden, "Comprehensive Characterization of InGaAs/InP Avalanche Photodiodes at 1550 nm with an Active Quenching ASIC," IEEE Journal of Quantum Electronics (to be published), arXiv/0812.2840.

1. Introduction

Quantum key distribution (QKD) provides a means of generating secret random bits, or keys, for cryptographic purposes, between two distant locations such that their secrecy is guaranteed by the laws of quantum physics [1]. Invented in 1984, QKD witnessed rapid development during the 1990s, culminating in the first commercial systems [2] and prototypes [3,4] a few years ago. While capable of continuous operation their rates were relatively low. More recent approaches have focussed on increasing clock rates to more than 1GHz [5-7] or even 10GHz [8], although these generally measure only raw data, over a fraction of a second in a so-called "burst mode", and *estimate* secret key rates via post-processing. At long distances, these often also rely on special fibres to compensate for chromatic dispersion [8]. It is with this in mind that recent efforts have focused on combining three crucial elements: new protocols that render faint laser systems less vulnerable to photon number splitting (PNS) attacks [9-16]; improved components for increasing maximum transmission range and bit rates using, for example, superconducting detectors [8], and more generally, system integration and standardisation for continuous operation in secure real world networks [17,18], targeting long term commercial viability. It is in this context that we see a paradigm shift for QKD from purely optical interference experiments to systems that integrate the quantum optics with fast

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

electronics, Field Programmable Gate Arrays (FPGAs), computer processors and software to implement quantum and classical algorithms in parallel over classical communication systems and networks. The results of our work have been the successful combination of these concepts.

The comparison between QKD systems need not be complicated. The role of QKD is to generate and distribute secure keys and, as such, the figure of merit for any QKD system is shifting towards the *real-time secret bit rate,* which can be described by $K = Rr$, where R is the sifted bit rate and r denotes the secret key fraction. K is necessarily an average over a long period of time, since efficient key distillation needs a minimum number of secret bits [19]. In principle, R is proportional to the pulse rate of the source ν_s and the average number of photons per pulse μ, which obviously motivates an increase in rates (or μ). However, r depends on the potential information of an eavesdropper and in the case of faint laser systems, which are vulnerable to PNS attacks, is limited by μ. The implementation of PNS resistant faint laser protocols, like "differential phase shift" (DPS) [9], SARG [10], or decoy states [14-16], allows one to securely increase μ and, therefore, the maximum distance and secret bit rate.

We have developed a QKD system based on a PNS-attack resistant protocol called *coherent one-way* [12] (COW) capable of taking advantage of both high pulse rates, and continuous and automated operation even over long distances. We report on laboratory tests up to 150km, in particular a 10-hour exchange averaging 2kbps over 100km using InGaAs avalanche photodiodes (APDs) is shown. We also performed a field trial, over the Swisscom fibre optic network between the Swiss cities of Geneva and Neuchâtel, with a fibre transmission distance of 150km in a high loss (43dB) line. Using superconducting single photon detectors (SSPDs), the COW QKD system continuously produced average distribution rates of 2.5bps in real time over periods of hours.

2. The Coherent One-Way QKD Protocol

In the COW QKD protocol, logical bits are encoded in time [12]. A sequence of weak coherent pulses is tailored from a CW-laser with an external intensity modulator (see Figure 1). The emitter, Alice, encodes bits using time slots (separated by T) containing either 0-pulses, no light, or μ-pulses, with a mean number of photons of $\mu<1$. The logical bit 0_L (1_L) corresponds to a sequence 0-μ (μ-0). For security reasons, we also send μ-μ decoy sequences.

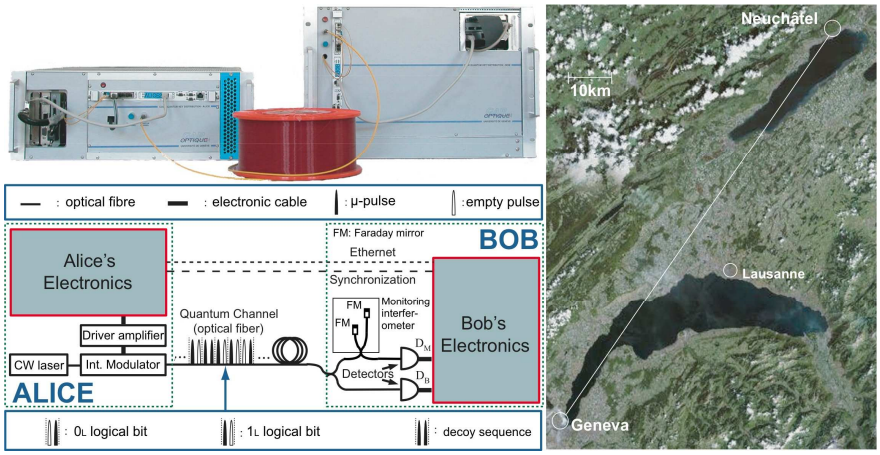

Fig. 1. Coherent one-way protocol. A schematic of the setup is shown (bottom left) with a photograph (above) of the final 19" rack-mountable system, containing the free-running InGaAs detectors (used in the lab trial). On the right we see a satellite image showing the two cities used for this QKD field trial. This experiment was performed with the external cryogen free superconducting detectors.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

The receiver, Bob, registers the time-of-arrival of the photons on detectors D_B for the bit or data channel and D_M for the monitoring channel. The D_B times provide the raw key from which Alice and Bob can sift out the net key. The security is guaranteed by checking the statistics for the detections on D_M, for destructive interference of decoy and logical sequences 1_L0_L. Photons are detected at random times after an unbalanced interferometer that has a path-length difference of T (pulse period). Unlike other protocols the interferometer is only used to estimate the information of the eavesdropper and cannot introduce errors on the key.

2.1. Security

Proving the security of the COW protocol remains a work in progress. The standard methods for proving the security of QKD protocols were, so far, developed for protocols in which the quantum symbols are sent one-by-one (e.g., qubits in the BB84 [20], B92 [21], SARG [10] protocols). The COW protocol, however, does not use this symbol-per-symbol type of coding and the standard security proofs do not apply in any straightforward way. To the contrary, the COW protocol is a so-called *distributed-phase-reference* protocol, like DPS, which relies on the coherence between successive non-empty pulses to ensure the security of the protocol. So far, the security of the COW protocol has been proven against the beam-splitting attack (BSA) [12,13,22,23], some intercept-resend attacks [12,22] and against a wide class collective attacks, under the assumption that Bob receives at most one photon per bit [23]. Here we use an estimate on Eve's information:

$$I_{AE}(\mu) = \mu(1-t) + (1-V)\frac{1+e^{-\mu t}}{2e^{-\mu t}}, \tag{1}$$

where the first term corresponds to BSAs and the second to intercept-resend attacks. t is the line transmission and V the interferometer's visibility. From this we can also determine an upper bound on the secret key rate:

$$K = R(\mu, \nu_s)\left[1 - h(Q(\mu)) - I_{AE}(\mu)\right]. \tag{2}$$

The second term corresponds to the previously mentioned secret key fraction *r*. $h(Q(\mu))$ is the Shannon entropy for a given quantum bit error rate (QBER), that is related to the minimum fraction of bits lost due to error correction (EC).

3. Description of the COW QKD system

The system has been developed to be rack mountable in two 19 inches boxes. Two fibres link them together; the first used for the quantum channel, the second for the classical communication, synchronisation and pre-sifting, which we explain shortly. Each box is connected to the Internet for the classical processing of the raw key. Alice and Bob have similar structures: optical and electronics modules with FPGAs and embedded computers.

The optical modules are very simple (see Figure 1). Alice's optics consists of a CW DFB telecom laser diode at 1550nm (Thorlabs, 1554.94-20) and a Lithium niobate intensity modulator (Avanex, 10Gbits/s) to tailor the sequence of pulses. After the intensity modulator a 50/50 coupler splits the beam in two where a PIN InGaAs detector (calibrated with a certified power meter) monitors the power so as to set the variable attenuator (OZ Optics, DD-600-xx) to the appropriate mean number $\mu = 0.5$ photons per pulse, independent of link loss. On Bob's side, a 90/10 coupler sends 90% of the photons directly to a single photon detector D_B. The remaining 10% of the photons go through an unbalanced Michelson interferometer and are detected by D_M. Note that the Faraday mirrors ensure that the interferometer is polarisation independent. Instead of using an actively stabilized interferometer, we implement a novel feedback scheme. It just consists of good thermal insulation of the interferometer and tuning of the laser wavelength for optimal interferences.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

Alice and Bob's units use embedded computers to monitor and control the full system. Each computer has several tasks: one process supervises all the subsystems and the communication between Alice and Bob; and a second controls various regulation tasks, e.g. for Alice, the current of the DFB laser to scan Bob's interferometer for optimal interference. Another process handles communication between the embedded computer and FPGA. The optical system is driven at a rate of 625MHz with a subsequent logical bit rate of 312.5Mb/s. The outgoing signal of the FPGA is shaped via a homemade emitter-coupled logic (ECL) electronic circuit and driver amplifier (Picosecond, 5865, 12.5Gb/s). The electronic signal drives the intensity modulator, which tailored 300ps long optical pulses with extinction ratio between 0-pulses and μ-pulses of 21.5dB (leading to 0.7% of QBER). Synchronisation and pre-sifting (from Bob to Alice) signals are combined using a WDM and sent through the second (classical) optical channel.

A Quantum Random Number Generator (QRNG) (id Quantique, Quantis OEM module) produces random bits at a rate of 4Mbps. However, logical bits, at a rate of 312.5Mb/s have to be generated. To overcome this we use the output of this QRNG to frequently seed a pseudo-random number generator (PRNG) implemented inside the FPGA. This PRNG is made of a 32-bit Linear Feedback Shift Register (LFSR)[1] and produces pseudo random sequences of $(2^{32} - 1)$ bits, a period of around 13s. In our system, the QRNG supplies a new seed to the PRNG every 64μs thus avoiding sequence repetitions. Decoy sequences are sent whenever the 1010 string is found at the output of the random generator (with probability 1/16). Work on the generation of quantum random bits at GHz rates is still in progress, however, a random number generator based on chaotic semiconductor lasers was demonstrated recently [24]. A distinct advantage of the COW protocol is that it only requires a RNG on Alice's side.

On Bob's side, InGaAs APDs are Peltier cooled to around -50°C and provide a simple and reliable detection system. Normally, these detectors are used in a so-called gated mode but in our case we take advantage of the recently developed free running mode [25]. We obtain dark count rates and quantum efficiencies of the order of 10^{-6} per ns and 10%, respectively. To limit the error detection rate, electronic coincidences windows of 400ps have been used. Furthermore, to limit the after-pulse probabilities to below 10^{-5} per ns, dead times of the order of 30μs have been applied that limits the maximal detection rate to ~30kHz, which is not a problem for longer distances, but a limiting factor at short distances. At short distances up-conversion based detection schemes [26], with detection rates up to 20MHz, could provide an interesting alternative. For the long distance experiments we used SSPDs, because of their low noise capabilities [27]. The sub-4K operating temperature is certainly a handicap for a commercial system, however, within the European project Sinphonia [28], we have developed a system that has fibre coupled SSPDs in a cryogen free cooler [8] that makes their application more straightforward in a laboratory environment. These detectors have typical quantum efficiencies of 2.5% with noise levels of 10 counts per second depending on the applied bias current. SSPDs have two advantages over InGaAs APD's: The better efficiency to noise ratio of the SSPDs allows to increase the range of QKD. The smaller dead time of the SSPDs (~25ns) allows to increase the bit rate at short distances. Currently though, their dependence on polarisation, which can reduce the photon detection efficiency by 50%, is problematic for fibre transmission.

[1] LSFR is not a cryptographically secure algorithm, other algorithms offer better, complexity based security (e.g. Mersenne twister). However, for "absolute" security, a QRNG (or at least a physical RNG) without expansion is needed.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

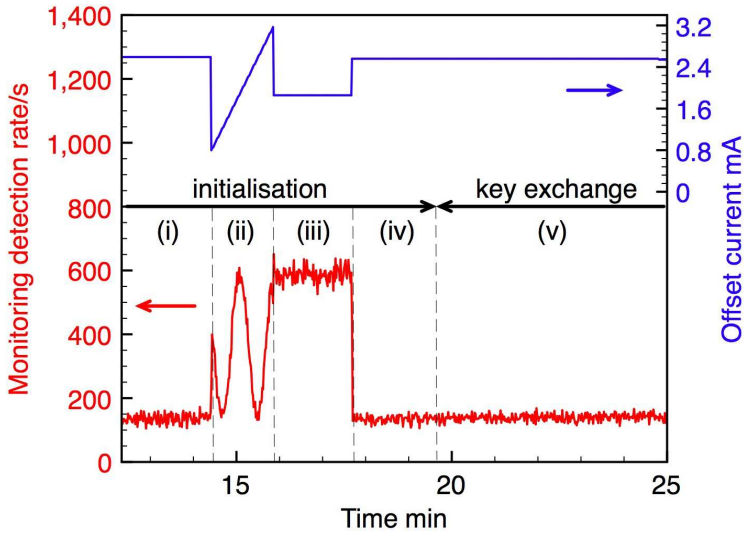

Fig. 2. Initialisation procedure and security monitoring. The noise is measured (i). Alice's laser wavelength (current) is scanned to determine the visibility of Bob's monitoring interferometer (ii). To obtain a more precise value for the visibility we accumulate detections for constructive (iii) and destructive interference (iv). Assuming trusted detectors, we subtract the noise (i) from (iii) and (iv), and obtain the net visibility. During the key exchange, the monitoring rate is minimized by continuously adjusting the laser wavelength (v). This figure shows an example of data recorded with InGaAs detectors and losses equivalent to 80km of fibre.

4. Autonomous QKD operation

Before the operation of any real QKD system, an installation procedure must be undertaken that includes checking component operation, such as the efficiency of detectors and the optimum parameters for the intensity modulator, as well as network characteristics like the total attenuation of the fibre transmission line. However, from this point, all the initialisation and synchronisation for the exchange is performed automatically by the COW system. In particular, the following steps are carried out:

a) Identification of bit numbers: During initialisation, Alice sends a series of different pulse patterns over the synchronisation channel, so that Bob can identify the pulse numbers, i.e. the length difference between the classical and quantum fibres.

b) A fine temporal tuning of the detection window. The delay between synchronisation and the detector output pulses is scanned to maximise the count rates, which also reduces noise and crosstalk between adjacent pulses.

c*) Wavelength adjustment and interference visibility (see Figure 2).* Random pulse sequences are sent over the quantum channel, the wavelength of the laser is scanned and the count-rate on the monitoring detector is recorded. The resulting interference fringe is used to calculate the visibility and set the wavelength for destructive interference.

It is important to note that the detectors are considered as trusted devices (in particular an eavesdropper can't change their noise level). As such, we can subtract the noise and consider the net visibility to estimate Eve's information. If the visibility is larger than 97%, we begin the key exchange. During the key exchange, the laser wavelength is continuously and automatically tuned in order to minimise the monitoring count rate and keep the visibility above 95%. If for some reason the visibility drops below this limit, a complete scan is automatically performed again and the key exchange restarts. For all exchanges, a visibility of 95% is assumed to determine Eve's information.

To perform the key exchange Alice randomly sends bits encoding 0_L, 1_L and decoy sequences. Bob registers all detection times for the data and the monitoring detector. He then announces for which bit there was a detection on D_B, as well as the times when he got clicks

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

on the monitoring detector D_M. In order to save memory space, Alice uses this *pre-sifting* information to immediately delete the bit values that are not needed. She then checks the security using the relevant monitoring detections, i.e. detections that correspond to interfering pulses. Alice then tells Bob, which detections, corresponding to decoy sequences, have to be removed from his data. Thus, Alice and Bob finally have a shared stream of bits, the sifted key.

The integrated distillation software then performs EC, using the Cascade algorithm [29], on the sifted key and applies the privacy amplification (PA) algorithm. As the bit exchange is continuous, the distillation software has to run in parallel, in real time, and treats blocks of data, 2^{13} or 2^{14} bits, depending on the distance, so as to ensure a good efficiency. Eve's information is removed through privacy amplification implemented using hashing functions based on Toeplitz matrices [30]. Finally, all information exchanges over the classical channel during the distillation procedure are securely authenticated using a Wegman-Carter type scheme, implementing universal hashing functions [31].

5. Lab measurements with InGaAs detectors

We have performed a series of measurements in the lab using InGaAs detectors. We introduced 25km of fibres and a variable attenuator between Alice and Bob and started all key exchanges with the complete initialisation and synchronisation procedure. In Figure 3 we can see the results of a key exchange with 21dB loss, corresponding to >100km of standard fibre with losses of 0.2dB/km. We find a mean secret bit rate of around 2kbps after the automatic distillation and authentification process. This figure illustrates the system's capability for continuous operation and its ability to automatically recover when the QBER increases excessively.

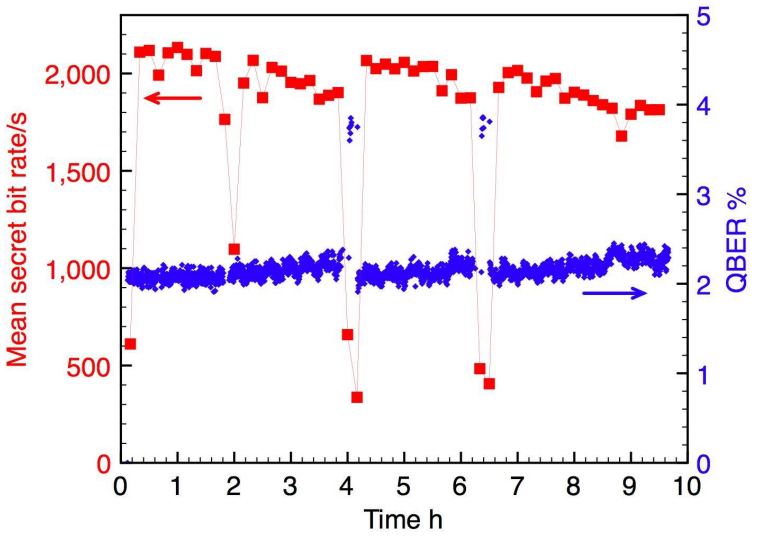

Fig. 3. Secret bit rate and QBER vs Time. A 10-hour key exchange with 25km of fibre plus 15dB attenuation, equivalent to around 100km of standard fibre with InGaAs detectors. We show the rate averaged over 10 minute intervals. The drops in rate denote periods of auto re-alignment (~20 minutes) when key generation is interrupted.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

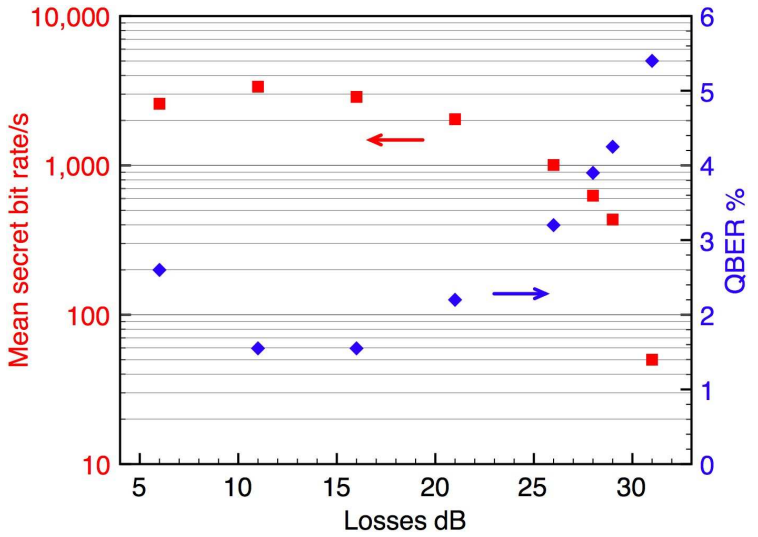

Fig. 4. Secret bit rate and QBER vs Distance. Rates and errors as a function of the loss, or distance with InGaAs detectors. 31dB corresponds to ~150km of standard fibre.

In Figure 4 we present the results obtained with 25km of fibre (around 6dB loss) with additional loss from an attenuator. Each point of the graph gives the mean secret bit rate and the QBER obtained over one hour. *Note that the rate is the direct output from the distillation software, it is not an evaluation based on the raw detection rate, the QBER and the visibility of the interferometer.* For short distances and low losses, the rate is limited by detector saturation, leading to the almost constant rate up to 21dB. Nonetheless, we are able to distribute > 50bps over a 31dB-loss line (150km of standard fibre with losses of 0.2dB/km). At 6dB, we see a sharp increase in the QBER that is due to charge persistence in the detectors [32]. This effect is due to the high photon flux where there is an increased probability that a photon arriving before the detector is "on" provokes a detection avalanche. This leads to additional errors and the increase in QBER.

6. Field measurements with SSPDs

To perform the field measurements we connected the SSPDs to Bob in Geneva, taking advantage of their larger efficiency to noise ratio compare to the InGaAs detectors. Alice was transported to a lab of our colleagues at the University of Neuchâtel, some 110km beeline from Geneva. The fibre, however, had a length of about 150km and rather high losses of 43dB, due to multiple line connections. At this distance the effects of chromatic dispersion that broaden the optical pulse widths of ~150ps, as well as timing jitter, reduces the signal in the coincidence by a factor of one third. Furthermore, parasitic light entering the fibre increases the "noise count". A 1nm band-pass filter is added to reduce this to around $17s^{-1}$ but also introduces extra internal losses (2.6dB total from input to data detector) for Bob.

In Figure 5(a) we show the data for an exchange over 3.5 hours, featuring a mean secret bit rate of roughly 2.5bps with a reasonable QBER of 5%. At this long distance, the count rates on the monitoring line become very small (< 1 per 10s) and the statistics aren't sufficient to correctly establish the value of the visibility and continuously adjust the laser wavelength. Therefore, while this is probably the longest key exchange ever, its security is questionable. To guarantee the security at such long distances active and independent stabilization of the laser wavelength and/or the interferometer is necessary.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009

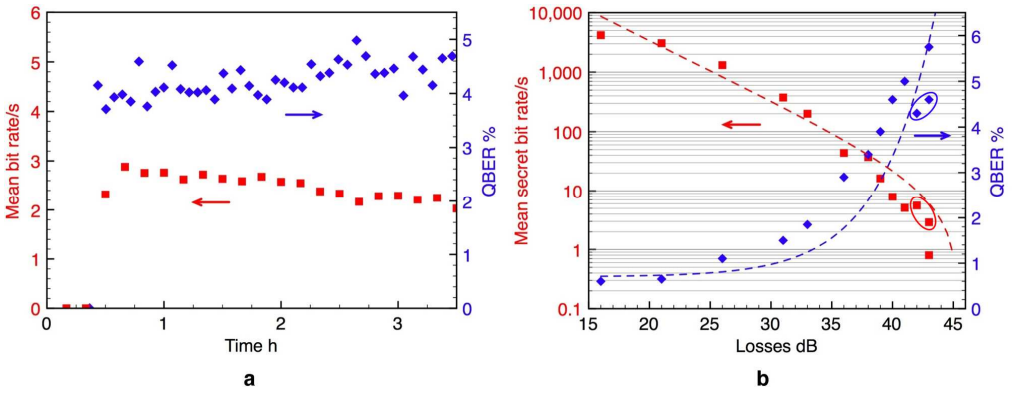

Fig. 5. Long distance QKD with SSPD. (a) Continuous operation over 3.5 hours for a 43dB-loss line. (b) Rates and errors as a function of loss in the installed, Geneva-Neuchâtel, fibre.

We finally used the same installed 150km fibre and mimicked key exchanges over intermediate distances by increasing the average photon number of the outgoing pulses at Alice. The results are summarised in Figure 5(b), where one can see the secret key rate as a function of fibre loss. At shorter distances < 20dB the rate is again saturated, although here, it is due to the EC and the classical communication time between Alice and Bob who are still separated by 150km of fibre in this case. The plotted curves show the estimates for the bit rate and the QBER for typical values of quantum efficiency and noise of the detectors. The experimental data points differ from this curve due to polarisation, parasitic noise and detector bias current fluctuations. For some measurements, we also fine-tuned the detector bias current to optimize the results. For example, the circled rates of 2.5bps at 42-43dB (equivalent to 200km of standard fibre) were obtained by this way.

7. Conclusion

We have presented results for a QKD system operating continuously and autonomously in a real world implementation of QKD over distances corresponding to 43dB in the Swisscom fibre optic network between the Swiss cities of Geneva and Neuchâtel. The QKD system reinforces the need for a high level of integration for the optics, electronics and software to allow for continuous and autonomous operation and the resulting unparalleled performance. We have used the coherent one-way (COW) protocol, which is a protocol that was invented with this specific goal in mind and have shown laboratory and field trial results for the system. The fully integrated version uses InGaAs avalanche photodiodes (APDs) and was laboratory tested up to 31dB (~150km), with a 10-hour exchange averaging secret bit rates over 2kbps for 21dB. In the field trials, with SSPDs, we find average bit rates of 2.5bps for 43dB. These landmark results presented here are a major step forward towards real inter-city QKD for future quantum networks.

Acknowledgements

The authors thank: C. Branciard & V. Scarani for useful discussions concerning QKD security; D. Salart & N. Walenta for their assistance with the field installation and the SSPDs; Y. Hasani, T. Lörunser, from ARC GmbH, with the RNG; CES SA with the FPGA cards; M. Rufer & D. Hofstetter for the use of their lab at the University of Neuchâtel; and Swisscom for access to their fibre link. Financial support is acknowledged from the EU projects, SECOQC and SINPHONIA as well as the Swiss NCCR “Quantum Photonics”.

#111121 - $15.00 USD Received 8 May 2009; revised 8 Jul 2009; accepted 13 Jul 2009; published 20 Jul 2009