Secure quantum key distribution over 421 km of optical fiber

Alberto Boaron,1,∗ Gianluca Bosso,1 Davide Rusca,1 Cédric Vallier,1 Claire Autebert,1 Misael Caloz,1 Matthieu Perrenoud,1 Gaëtan Gras,1,2 Félix Bussières,1 Ming-Jun Li,3 Daniel Nolan,3 Anthony Martin,1 and Hugo Zbinden1

1Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland
2ID Quantique SA, 3 Ch. de la Marbrerie, CH-1227 Carouge, Switzerland
3Corning Incorporated, Corning, NY 14831, United States

We present a quantum key distribution system with a 2.5 GHz repetition rate using a three-state time-bin protocol combined with a one-decoy approach. Taking advantage of superconducting single-photon detectors optimized for quantum key distribution and ultra low-loss fiber, we can distribute secret keys at a maximum distance of 421 km and obtain secret key rates of 6.5 bps over 405 km.

The first experimental demonstration of quantum key distribution (QKD) was over a short distance of 32 cm on an optical table [1]. Since then, there has been a continuous progress on the theoretical and technological side such that nowadays commercial fiber-based systems are available [2] and the maximum distance has been pushed up to 400 km with academic systems [3]. Recently, the feasibility of satellite-based QKD has been demonstrated [4], opening the door for world-wide key distribution (QKD) was over a short distance of 32 cm on an optical table [1]. Since then, there has been a continuous progress on the theoretical and technological side such that nowadays commercial fiber-based systems are available [2] and the maximum distance has been pushed up to 400 km with academic systems [3]. Recently, the feasibility of satellite-based QKD has been demonstrated [4], opening the door for world-wide key distribution. Indeed, taking into account finite key analysis, a maximum acceptable key accumulation rate is shown to be optimal for block sizes smaller than 108 bits [8]. All pulses have random relative phase in order to render coherent attacks inefficient.

Figure 1 schematically shows our experimental realization. Alice’s and Bob’s setups are situated in two separated laboratories 20 m apart. Each of them is controlled by a field programmable gate array (FPGA).

Alice uses a phase-randomized diode laser pulsed at 2.5 GHz. Phase randomness is achieved by switching the current completely off between the pulses [12]. The pulses then pass through an unbalanced Michelson interferometer (200 ps delay). One of its arms is equipped with a piezoelectric fiber stretcher to adjust the phase. The different qubit states are now encoded by a lithium niobate intensity modulator controlled by the FPGA. The qubit states and the pulse energies (signal or decoy state) are chosen at random. For this purpose, we rely on a quantum random number generator [ID Quantique, Quantis] which supplies 4 Mbps of random bits which are expanded to 40 Gbps using the NIST SP800-90 recommended AES-CTR cryptographically secure pseudo-random number generator.

Bob’s choice of measurement basis is made passively by a beamsplitter. In the Z basis, the photons are directly sent to a single-photon detector that measures their arrival time. This basis is used to generate the raw key. In the X basis, used to estimate the eavesdropping information, an unbalanced interferometer identical to that of Alice allows to measure the coherence between two consecutive pulses. Only one detector is employed at the output of the interferometer.

The quantum channel (QC) is composed of spools of SMF-28® ultra low-loss (ULL) single-mode fiber (SMF) [Corning] which has an attenuation of about 0.16 dB/km (0.17 dB/km including the connections loss) and a positive chromatic dispersion of around 17 ps/nm−1 km−1. The ULL fiber consists of a pure silica core and a fluorine doped cladding. To reduce the impact of the chromatic dispersion, we pre-compensate it with disper-
sion compensation fiber (DCF) fabricated by Corning Inc. placed on Alice’s side. The DCF dispersion is around \(-140 \text{ ps nm}^{-1} \text{ km}^{-1}\) and its attenuation is about \(0.5 \text{ dB/km}\).

The synchronization and communication between Alice’s and Bob’s devices is performed through a communication link, denoted as service channel (SC), based on small form-factor pluggable (SFP) transceivers connected through a short 50 m duplex fiber. For practicality, we use this fiber for all QC lengths. However, a SC of the same length as the QC (implemented with optical amplifiers) would offer better stability. Anyway, we compensate actively the fluctuations of the path length difference between the QC and the SC. For this purpose, the detectors signals are sampled at 10 GHz (i.e. only half of the bins are used for the sifting). The temporal tracking is performed by minimizing the ratio between the detections in the inactive and active bins. At the distances under study, we observed drifts having a sinusoidal behavior over one day, with amplitudes up to about 10 ns (which correspond to a 0.5 K difference in the average fiber temperature at 400 km). The intrinsic phase stability of our interferometers exceeds 10 minutes. Still, an automatic feedback loop also stabilizes the relative phase between Alice’s and Bob’s interferometers using the quantum bit error rate (QBER) in the \(X\) basis as an error signal. The temporal tracking and the phase stabilization work in real time for distances up to 400 km. However, at the maximal distance (421 km), given the low detection rate, the statistical fluctuations of the error signal become too important to stabilize in real time. Therefore, we interrupt data acquisition after each block of error correction (EC) (about half an hour of acquisition) in order to perform an adjustment with a higher power of Alice’s signal.

The detection is done with two custom-made molybdenum silicide superconducting nanowire single-photon detectors (SNSPDs) cooled at 0.8 K [7]. For SNSPDs, reducing the noise of the detectors implies filtering out black-body radiation present in the optical fiber leading to the detector. The black-body radiation around the laser wavelength (1550.92 nm) is eliminated using a standard 200 GHz fibered dense wavelength division multiplexer bandpass filter cooled to 40 K. Infrared light above 1550 nm is filtered by coiling the optical fiber just before the detector [13]. In this way, we achieve a dark count rate (DCR) of 0.1 Hz, which is close to the intrinsic DCR of the detectors. The maximum efficiencies of our detectors are between 40 to 60\%, depending on the detector and on the filtering configuration. Because of the meander structure of the SNSPDs, the detection efficiency depends on the input polarization (the ratio between the minimum and maximum efficiencies is about 1/2). This leads to slow variations of the detection rate, since we adjust the polarization of the light at the beginning of the runs, but do not perform any further adjustment during the acquisition. The system timing jitter of the detectors is lower than 40 ps.

The model of our protocol consists in a modification from the already proven to be secure three-state protocol [14–16]. The difference stands in the fact that we have only one detector in the \(X\) basis. Therefore, we do not have access to all measurements outcomes of the standard protocol. However, this does not affect the security of the protocol as demonstrated in Rusca et al. [9]. Note that the proof covers the security against collective attacks. However, given the phase-randomization of the states sent by Alice, the results can be extended to coherent attacks using techniques such as Azuma’s inequality [17–19] or De Finetti’s theorem [20, 21].

The secure key bits per privacy amplification block is given by [8]:

\[
\log_2 \frac{1}{\epsilon_{sec}} - \log_2 \frac{2}{\epsilon_{cor}},
\]

where \(s_{Z,0}\) and \(s_{Z,1}\) are the lower bound on the number of vacuum and single-photon detections in the \(Z\) basis, \(\phi_Z\) is the upper bound on the phase error rate, \(\lambda_{EC}\) is the total number of bits revealed during the EC, and \(\epsilon_{sec} = 10^{-9}\) and \(\epsilon_{cor} = 10^{-9}\) are the secrecy and correctness parameters, respectively.
We performed key exchanges with fiber lengths between 252 and 421 km. For every distance we optimized the following experimental parameters to maximize the SKR. On Alice’s side, we varied the probability of choosing the Z and X basis, the mean photon number of the two decoy states $\mu_1$ and $\mu_2$ and their respective probabilities. On Bob’s side, we used different detectors following a trade-off between high efficiency and low DCR. The latter criterion becomes increasingly important with increasing distances. For simplicity, Bob’s probability of choosing the Z and X basis was kept constant to 1/2, which is a good value at long distances to minimize the penalty due to the finite-key analysis in both bases.

Table I summarizes the experimental settings and performance for different fiber lengths. *Data considering only the duration of the data transmission.

| length (km) | attenuation (dB) | $\mu_1$ | $\mu_2$ | block size | block time (h) | QBER Z (%) | $\phi_z$ (%) | RKR (bps) | SKR (bps) |
|------------|-----------------|--------|--------|-----------|---------------|------------|-------------|-----------|-----------|
| 251.7      | 42.7            | 0.49   | 0.18   | $8.2 \times 10^5$ | 0.20         | 0.5        | 2.2         | $12 \cdot 10^4$ | $4.9 \cdot 10^4$ |
| 302.1      | 51.3            | 0.48   | 0.18   | $8.2 \times 10^6$ | 1.17         | 0.4        | 3.7         | $1.9 \cdot 10^3$ | $0.79 \cdot 10^3$ |
| 354.5      | 60.6            | 0.35   | 0.15   | $6.2 \times 10^6$ | 14.8         | 0.7        | 1.8         | 117       | 62        |
| 404.9      | 69.3            | 0.35   | 0.15   | $4.1 \times 10^5$ | 6.67         | 1.0        | 4.3         | 17        | 6.5       |
| 421.1      | 71.9            | 0.30   | 0.13   | $2.0 \times 10^5$ | 24.2 (12.7*) | 2.1        | 12.8        | 2.3 (4.5*) | 0.25 (0.49*) |

![FIG. 2. Circles: experimental final SKR versus distance. Triangles: simulation of an idealized BB84 protocol with the same block sizes as the corresponding experimental points. Squares: results of other long-distance QKD experiments using ULL fibers: (1) BB84, B. Frölich et al. [22]; (2) Coherent one-way, B. Korzh et al. [23]; (3) Measurement-device-independent QKD, H.-L. Yin et al. [3]. The upper axis is obtained by considering an attenuation of 0.17 dB/km.](image1)

![FIG. 3. System stability over more than 24 h for a distance of 302 km of ULL SMF. (a) RKR, SKR, and (b) corresponding QBER in the Z basis and $\phi_z$ as a function of time.](image2)
exchange the 25 EC blocks (12.7 h), we obtain a SKR of 0.49 bps.

To demonstrate the long-term operation capability of our system, we run it over a continuous period of more than 24 h at a transmission distance of 302 km. The phase stabilization and temporal alignment were performed automatically by the control software. The relevant experimental results are shown in figure 3 as a function of time. Fluctuations of the raw key rate (RKR) are mainly due to polarization fluctuations of the signal arriving at Bob’s side.

Figure 2 also shows a comparison of our experimental results with other QKD realizations. 421 km is the maximal transmission distance reported for a QKD system in fiber. Compared to the previous record [3], at 405 km, the rate is improved by four orders of magnitude. Moreover, our acquisition times, shorter than a day, are still of practical utility.

In order to appreciate the performance of our system with respect to a perfect one, we simulated (for the same distances and block sizes as our experimental points) the SKRs of an idealized BB84 system with no DCR, 0% of QBER and 100% detection efficiency (represented as triangles on figure 2). Most of the difference is due to the lower detection efficiency in our experiment. Indeed, if we took it into account, the simulated and experimental points would almost overlap. Therefore, we can conclude that our simplifications of the protocol (three-state) and the implementation (with only one detector in the X basis) do not significantly affect the performance. Except for the detection efficiency, our system is close to an ideal system.

How far could one still increase the transmission distance of QKD? With an ideal, noiseless implementation, the limiting factor is in the end the minimum block size needed to still extract a secret key with good confidence. Given that the number of detected photons decreases exponentially with distance, the resulting, necessary exponential increase of the acquisition time cannot be satisfactorily mitigated by an increased pulse repetition rate. We simulate a system with the following properties: BB84 protocol, 10 GHz repetition rate, 100% detection efficiency, 0 Hz DCR and $e_{\text{sec}} = 10^{-9}$. For this system, a constraint of 1 day of acquisition leads to a maximal distance of around 600 km, with a SKR of $2.5 \times 10^{-2}$ bps (i.e. 2.2 kHz per day (block)) at 600 km. Going significantly beyond this limit would require switching to protocols featuring a more favorable dependency of the RKR as a function of the fiber length $l$, such as the recently proposed twin-field QKD ($\sim \exp(-l^{1/2})$) [24], or a quantum repeater [25]. However, these alternatives are of much greater technological complexity.

**ACKNOWLEDGEMENTS**

We would like to acknowledge Jesús Martínez-Mateo for providing the error correction code and Charles Ci Wen Lim for useful discussions. We thank the Swiss NCCR QSIT. D.R. and G.G. thank the EUs H2020 programme under the Marie Skłodowska-Curie project QCAL (GA 675669) for financial support. This work was partly supported by the COST (European Cooperation in Science and Technology) Action MP1403 Nanoscale Quantum Optics and by the Eurostars-2 joint programme (grant agreement: E11493 - QuPIC) with co-funding from the European Union Horizon 2020 research and innovation programme.

* alberto.boaron@unige.ch

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of cryptology 5, 3 (1992).
[2] www.idquantique.com.
[3] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 117, 190501 (2016).
[4] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature 549, 43 (2017).
[5] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindeffer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, Phys. Rev. Lett. 120, 030501 (2018).
[6] A. Boaron, B. Korzh, R. Houlmann, G. Bosco, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Applied Physics Letters 112, 171108 (2018).
[7] M. Caloz, M. Perrenoud, C. Auterbert, B. Korzh, M. Weiss, C. Schenberger, R. J. Warburton, H. Zbinden, and F. Bussières, Applied Physics Letters 112, 061103 (2018).
[8] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Applied Physics Letters 112, 230503 (2018).
[9] D. Rusca, A. Boaron, A. Martin, M. Curty, and H. Zbinden, In preparation (2018).
[10] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[11] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[12] T. Kobayashi, A. Tomita, and A. Okamoto, Physical Review A 90, 032320 (2014).
[13] K. Smirnov, Y. Vachtomin, A. Divochiy, A. Antipov, and G. Goltzman, Applied Physics Express 8, 022501 (2015).
[14] C.-H. F. Fung and H.-K. Lo, Phys. Rev. A 74, 042342 (2006).
[15] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A 90, 052314 (2014).
[16] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New Journal of Physics 17, 093011 (2015).
[17] K. Azuma, Tohoku Math. J. (2) 19, 357 (1967).
[18] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. 94, 040503 (2005).
[19] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, Phys. Rev. A 80, 032302 (2009).
[20] C. M. Caves, C. A. Fuchs, and R. Schack, Journal of Mathematical Physics 43, 4537 (2002), https://doi.org/10.1063/1.1494475.
[21] R. Knig and R. Renner, Journal of Mathematical Physics 46, 122108 (2005), https://doi.org/10.1063/1.2146188.
[22] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Optica 4, 163 (2017).
[23] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nature Photonics 9, 163 (2015).
[24] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature 557, 400 (2018).
[25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. 83, 33 (2011).