Quantum key distribution system with 2.5 GHz clock rate

Alberto Boaron,[1,*] Boris Korzh,[1] Gianluca Boso,[1] Raphael Houlmann,[1,2]
Charles Ci Wen Lim,[3] Ming-Jun Li,[4] Daniel Nolan,[4] and Hugo Zbinden[1]

[1]*Group of Applied Physics, University of Geneva,*
Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland
[2]*ID Quantique SA, 3 Ch. de la Marbrerie, CH-1227 Carouge, Switzerland*
[3]*Quantum Information Science Group,*
Computational Sciences and Engineering Division,
Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, US
[4]*Corning Incorporated, New York, United States*

Over the last decades, Quantum Key Distribution (QKD) has made tremendous progress towards achieving high secret key rates (SKR) of the order or MHz over short distances [1]. The challenges in order to reach SKR of the order of tens of MHz are the following. At the emitter side (Alice), the source should generate qubits at rates of a more than 1 GHz. At the receiver side (Bob), the detection apparatus should be capable of detection rates approaching 100 MHz, and finally the post-processing must be fast enough to allow for real-time key generation.

In this paper, we present our new system designed to achieve high SKR and exchange keys over long distances. The emitter (depicted in Fig. 1) continuously generates true random qubits at a clock rate of 2.5 GHz.

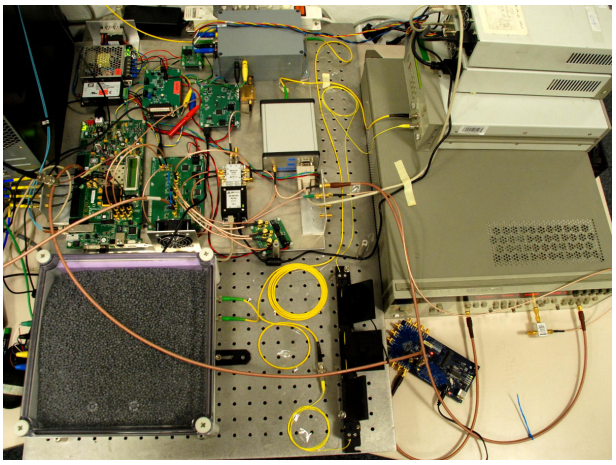

FIG. 1: Global view of Alice's setup.

This is, to our knowledge, the highest clock rate ever achieved in a system capable of generating secret keys. Indeed, other systems running at comparable or higher rates, were working in burst mode and/or with pseudo-random sequences [2].

We use a three-state protocol [3] implemented in time-bin encoding and the decoy-state method with three intensity levels. A

*Electronic address: alberto.boaron@unige.ch

rigorous finite-key security analysis based on Ref. [4] is performed. The system is controlled by a field programmable gate array (FPGA) at Alice's and at Bob's.

At Alice a gain-switched laser produces pulses (about 40 ps at 1550 nm) at a rate of 2.5 GHz, which are doubled using an imbalanced interferometer. I.e. each qubit consists of two time-bin separated by only 200 ps.

As a quantum channel, we use ultra low loss fibres (Corning SMF-28 ULL fibre featuring an attenuation as low as 0.16 dB/km [7]). The chromatic dispersion is compensated with dispersion compensating fibres, which is mandatory for fibre lengths longer than 50km in order to limit dispersion-induced quantum bit errors.

Bob is designed to deal with high detection rates. He can collect and process the detections coming from up to 8 detectors at a total count rate of more than 300 Mhz. For long distance experiments we use InGaAs/InP negative feedback avalanche diodes single photon detectors (NFAD SPDs) [5]. For short distance experiments, 8 superconducting nanowire single photon detectors (SNSPDs), are connected in parallel. We use MoSi SNSPDs designed in-house featuring detection efficiencies of more than 80% and timing jitters of less than 30 ps.

The following active stabilization schemes

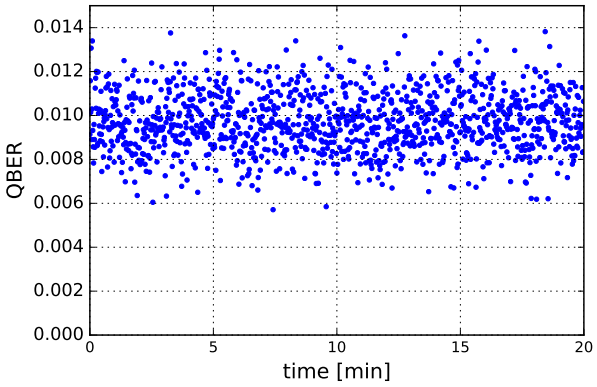

FIG. 2: Stability of the QBER over 20 minutes.

are implemented. 1. Feedback on the phase of Alice's interferometer. 2. Feedback on the bias voltage of the intensity modulator. 3. Synchronization of the signals coming from the detectors with the temporal bins of the FPGA to compensate for the fluctuations in the length of the quantum channel.

The post-processing is performed in real time by the FPGAs. Classical communication between Alice and Bob is performed through a dedicated fibre channel using small form-factor pluggable transceivers. The error correction step can be performed either by the FPGAs themselves (for high rates, using low-density parity-check) or by an external software (for long distances, using a CASCADE algorithm [6]).

Preliminary results

As a first step we have characterized and tested the system using NFAD SPDs operat-

ing in the free-running and cooled with a free-piston Stirling cooler. As shown in Fig. 2, the quantum bit error rate (QBER) with a few meters of fibre is 1.0%. When the feedbacks are activated, the system is stable over several hours.

We expect a slight improvement of the QBER when using SNSPDs instead of NFAD SPDs thank to their reduced timing jitter.

At the conference we will present and discuss in detail the results of both long distance and short distance/high rate experiments.

---

[1] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Efficient decoy-state quantum key distribution with quantified security*, Opt. Express **21**, 24550 (2013), URL `http://www.opticsexpress.org/abstract.cfm?URI=oe-21-21-24550`.

[2] I. Choi, R. J. Young, and P. D. Townsend, *Quantum key distribution on a 10gb/s wdm-pon*, Opt. Express **18**, 9600 (2010), URL `http://www.opticsexpress.org/abstract.cfm?URI=oe-18-9-9600`.

[3] C.-H. F. Fung and H.-K. Lo, *Security proof of a three-state quantum-key-distribution protocol without rotational symmetry*, Phys. Rev. A **74**, 042342 (2006), URL `https://link.aps.org/doi/10.1103/PhysRevA.74.042342`.

[4] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, *Concise security bounds for practical decoy-state quantum key distribution*, Phys. Rev. A **89**, 022307 (2014).

[5] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, *Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency*, Appl. Phys. Lett. **104**, 081108 (2014).

[6] J. Martínez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, *Demystifying the Information Reconciliation Protocol Cascade*, Quantum Inf. Comput. **15**, 0453 (2015), URL `http://www.rintonpress.com/xxqic15/qic-15-56/0453-0477.pdf`.

[7] https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28%20ULL.pdf