Progress on Quantum Key Distribution Using Ultralow Loss Fiber

Alberto Boaron,[1] Davide Rusca,[1] Gianluca Boso,[1] Raphael Houlmann,[1] Fadri Grünenfelder,[1] Cédric Vulliez,[1] Misael Caloz,[1] Matthieu Perrenoud,[1] Gaetan Gras,[1] Claire Autebert,[1] Félix Bussières,[1] Ming-Jun Li,[2] Daniel Nolan,[2] Anthony Martin,[1] and Hugo Zbinden[1]

[1] *Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland*
[2] *Corning Incorporated, Corning, NY 14831, United States*

We use a 2.5 GHz clocked quantum key distribution system to perform long-distance and high-speed quantum key distribution. Taking benefit from superconducting detectors optimized for each operation regime and low-loss fiber, we achieve state-of-the-art performance.

Secure communication is a cornerstone of our society and finding a way to protect our personal data while making it globally accessible is a profound challenge. Quantum key distribution (QKD) enables the secure establishment of cryptographic keys between two remote users, Alice and Bob. Importantly, the security of QKD depends only on the principles of quantum physics.

QKD has become commercially available for point-to-point operation with MHz rates and over distances larger than 100 km. Achieving higher rates and long distances remains a challenge and to obtain such high performances both the hardware and the post-processing parts of a QKD system should be optimized.

Our experiment takes advantage of state-of-the-art performance on all fronts to push the limits to new heights. We rely on a new 2.5 GHz clocked setup, low-loss fibers, in-house-made highly efficient superconducting detectors, and last but not least a very efficient one-decoy state scheme.

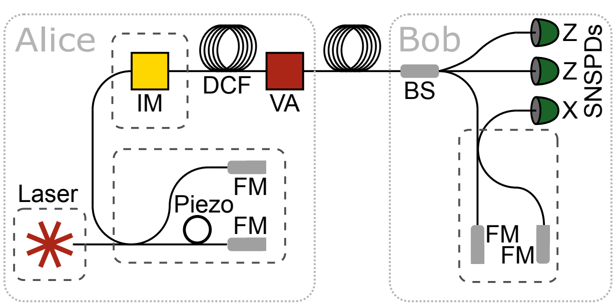

Figure 1. Schematics of the experimental setup. Laser: 1550 nm gain-switched laser; Piezo: piezoelectric fiber stretcher; FM: Faraday mirror; IM: intensity modulator; DCF: dispersion compensating fiber; VA: variable attenuator; BS: 3-port beamsplitter; SNSPD: superconducting nanowire single-photon detectors. Dashed lines represent temperature stabilized boxes.

Protocol: We use the simplified BB84 protocol presented in [1] with the one-decoy state method [2]. The experimental setup is depicted in figure 1. See [3, 4] and references therein for a detailed description of the system.

Source of quantum states: Time-bin encoded states are generated by a state-of-the-art source at a rate of 2.5 GHz. This is to our knowledge, the fastest repetition rate for a QKD platform. While modulation rates up to 40 GHz are standard in classical communication, QKD requires high extinction modulation and achieving rates of few GHz is already a challenge. The preparation error is responsible for less than 0.5 % of quantum bit error rate.

Quantum channel and dispersion management: In order to maximize the transmission distance, we use ultralow loss fiber (ULL) with an attenuation of 0.17 dB/km including the connections loss. To reduce the impact of the chromatic dispersion, we precompensate it with dispersion compensation fiber (DCF) placed on Alice's side. The DCF dispersion is around $-140\,\mathrm{ps\,nm^{-1}\,km^{-1}}$.

Experiment control and post-processing: The setup is controlled by two field programmable gate arrays (FPGA) which perform in real time the following steps: state preparation, sifting, error correction, error verification and privacy amplification. Real-time privacy amplification is usually a bottleneck for high-speed QKD. However, using a tight bound for the finite-key analysis, we are able

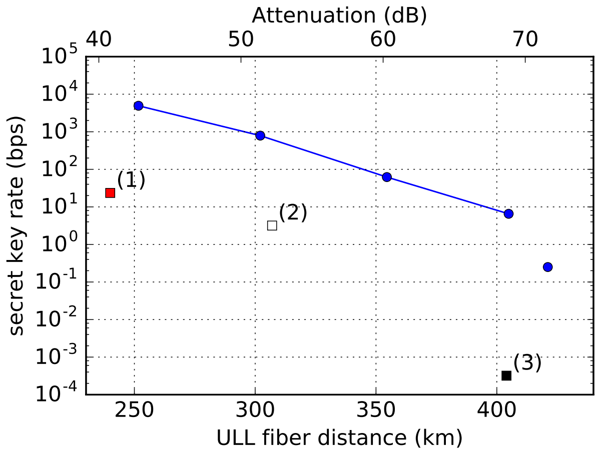

Figure 2. Circles: experimental final SKR versus distance. Squares: results of other long-distance QKD experiments using ULL fibers: (1) BB84, B. Frölich *et al.* [5]; (2) Coherent one-way, B. Korzh *et al.* [6]; (3) Measurement-device-independent QKD, H.-L. Yin *et al.* [7]. The upper axis is obtained by considering an attenuation of 0.17 dB/km.

to reduce the privacy amplification block size, therefore improving the maximum throughput. Synchronization and communication between Alice's and Bob's devices is performed through a communication link based on 10 GHz small form-factor pluggable transceivers.

Single-photon detectors: We employ in-house-made superconducting nanowire single-photon detectors (SNSPDs) wich feature dark count rates as low as 0.1 Hz, detection efficiencies up to 50 % and timing jitters smaller than 30 ps.

Long-distance operation: Experimental results are depicted in figure 2. We exchanged 0.25 bps at a transmission distance of 421 km, which is the maximal transmission distance reported for a QKD system in fiber. We achieve an improvement of the SKR by 4 orders of magnitude with respect to the only comparable experiment over 400 km [7] (which was using a measurement-device-independent QKD configuration).

High-speed operation: We also investigate the short distance regime which implies high detection rates. This regime requires detectors with very short recovery time. The SNSPDs we use feature more than 50 % detection efficiency at 50 Mcps detection rate and timing jitters lower than 60 ps. To reduce the detector saturation at short distance, we employ up to three detectors in the bit basis (Z). This is work under progress. We envisage secret key rates exceeding 50 Mbps at 2 dB attenuation. Moreover, the maximum throughput of the privacy amplification would be 75 Mbps of secret key rate with a privacy amplification block size of 10^5 bits and compression factor of 0.3.

[1] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, Phys. Rev. A **98**, 052336 (2018).

[2] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Applied Physics Letters **112**, 171104 (2018).

[3] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Applied Physics Letters **112**, 171108 (2018).

[4] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).

[5] 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).

[6] 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).

[7] 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).