Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems

Fadri Grünenfelder,[1,2,*] Alberto Boaron,[1] Giovanni V. Resta,[1,3] Matthieu Perrenoud,[1] Davide Rusca,[1,2] Claudio Barreiro,[1] Raphaël Houlmann,[1] Rebecka Sax,[1] Lorenzo Stasi,[1,3] Sylvain El-Khoury,[3] Esther Hänggi,[4] Nico Bosshard,[4] Félix Bussières,[3] and Hugo Zbinden[1]

[1] *Group of Applied Physics, Rue de l'Ecole-de-Médecine 20, CH-1211 Genève 4, Switzerland*
[2] *Vigo Quantum Communication Center, University of Vigo, Estrada de Marcosende 89, ES-36310 Vigo, Spain*
[3] *ID Quantique SA, Rue Eugène-Marziano 25, CH-1227 Acacias - Genève, Switzerland*
[4] *HLSU, Suurstoffi 1, CH-6343 Rotkreuz, Switzerland*

fiber length (km)	att. (dB)	μ_0	μ_1	p_{μ_0}	$p_{\mathrm{Z,A}}$	$p_{\mathrm{Z,B}}$	R_{sift}(Mbps)	ϕ_{Z} (%)	Q_{Z} (%)	SKR (Mbps)
10.0	1.58	0.49	0.22	0.74	0.65	0.99	159.4	0.8	0.4	64
102.4	16.34	0.46	0.20	0.79	0.66	0.99	7.8	1.0	0.3	3.0

TABLE I: Measured secret key rate (SKR) and corresponding experimental parameters. The variables μ_0 and μ_1 stand for the mean photon number of the signal and decoy states, p_{μ_0} and $p_{\mu_1} = 1 - p_{\mu_0}$ are the corresponding probabilities to choose these values, $p_{\mathrm{Z,A}}$ and $p_{\mathrm{Z,B}}$ are the probabilities of Alice and Bob to choose the Z basis, R_{sift} is the sifted key rate, ϕ_{Z} is the phase error rate and Q_{Z} is the QBER Z.

We implemented a simplified time-bin BB84 quantum key distribution protocol [1, 2] with the purpose of achieving the highest possible secret key rate at short distances. The sender Alice emits signals at a rate of 2.5 GHz. In the key-generating basis, we use a superconducting nanowire single photon detector (SNSPD) with a novel design optimized for fast count rates. The in-house designed and fabricated NbTiN detector consists of 14 nanowires which are arranged in an interleaved pattern. Together with the in-house made readout electronics, the detector shows a jitter below 60 ps and simultaneously an efficiency of 64% at a count rate of 320 Mcps, which represents the operating point of the detector for our shortest-distance key exchange. We performed real-time error correction with a low-density parity check algorithm implemented on a dedicated field-programmable gate array. This algorithm has a leakage of 17% at the highest quantum bit error rate found in our experiment, which was 0.4%. The privacy amplification was performed in real time on a consumer-grade GPU. We achieved a secret key rate of 64 Mbps over a distance of 10.0 km of ultra-low-loss (ULL) single-mode fiber (0.16 dB/km) and 3.0 Mbps over 102.4 km of ULL single-mode fiber (see Table I). Additionally, we monitored the secret key rate over a longer time over 10.0 km ULL SMF, showing that the secret key rate can be maintained at a similar value for more than 1000 consecutive privacy amplification blocks.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984* (1984) pp. 175–179.

[2] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 GHz time-bin quantum key distribution, Applied Physics Letters **112**, 171108 (2018).

* fagrue@com.uvigo.ch