Optimal Transmitter for Last Mile QKD

Y Kurochkin[1], V Rodimin[1], A Pereszlenyi[1], J Tembridis[1], C Vorhemus[1], V Revici[1], I Samsonenko[1], and J A Grieve[1]

[1] *Quantum communications, TII, Abu Dhabi, United Arab Emirates*
Contact Email: yury.kurochkin@tii.ae

A principal limitation of practical QKD deployment is equipment cost. Existing city and intercity scale quantum networks are built from high-end components that are justifiable for state and large-corporate end-users, but that strongly restricts the number of subscribers who can afford an access point to such a network. In this work we focus on enabling affordable connections from the end-user to the nearest node of the quantum network, where the priority is the simplest possible user equipment, with key rate and maximum distance treated as secondary objectives. From an architectural point we chosen a star-type network architecture in which a single receiver at the network node is time-shared between many users via an optical switch. Single-photon detectors (for DV-QKD) and low-noise local oscillators (for CV-QKD) do not fit this "affordability philosophy," the user-side equipment is transmitter.

Analyzing the principal cost drivers of QKD transmitters, we identify high-speed electro-optical modulation as the dominant one, since it requires wideband RF amplifiers and digital to analog converters, while inter-symbol correlations adds severe requirements on every active component. A natural way out is the passive state-preparation approach [1], which merges the QRNG and state-preparation stages into a single passive optical instrument with no active modulation. We use the standard BB84 protocol without decoy states: for the targeted 15–30 km range, weak coherent pulses are sufficient, and the photon-number-splitting attack is mitigated by stronger attenuation of the laser pulses [2].

The time-bin qubit, in which information is encoded in the phase difference between two pulses, is widely used in QKD and also known as the basic primitive of phase-diffusion QRNGs [3]. Unifying these two functions, we generate pairs of gain-switched laser pulses with independent random phases at a pair rate of 100 MHz, keeping all electronics below the high-speed regime. Each pair is split between a heavily attenuated signal arm ($\mu \leq 0.1$ photons per qubit, sent to the receiver) and a strong local copy. The local copy is analyzed by a passive tomography stage that converts the time-bin qubit into a polarization state, allowing all four BB84 states to be distinguished simultaneously; the angle between the two bases is fixed by a single, once-fabricated waveplate. Each tomography output is monitored by a photodiode followed by an amplifier and a comparator; a click on a given channel indicates constructive interference for one of the BB84 states, prepared either in one basis ($\delta\phi = 0,\ \pi$) or the other ($\delta\phi = \pi/2,\ 3\pi/2$).

Following an initial proof-of-principle at 1.5 MHz on SNSPD detectors [4], we have implemented an FPGA-based system operating at a 100 MHz state-preparation rate with free-running APDs. We achieve an asymptotic secret-key rate of 300 bps at 7 dB of quantum-channel attenuation, equivalent to ∼20 km of fiber at 1310 nm. This rate is sufficient to refresh 256 bit the key once per minute for 64 users connected via an optical switch. Our next goal is the co-integration of the quantum and classical signals on the same fiber infrastructure.

References

[1] M Curty, X Ma, H-K Lo and N Lütkenhaus, Phys. Rev. A 82, 052325 (2010)

[2] N Lütkenhaus, Phys. Rev. A 61, 052304 (2000)

[3] R Shakhovoy, D Sych, V Sharoglazova, A Udaltsov, A Fedorov and Y Kurochkin, Opt. Express 28, 6209 (2020)

[4] Y Kurochkin, M Papadovasilakis, A Trushechkin, R Piera and J A Grieve, arXiv:2405.08481 (2024)