Simple and robust QKD system with Qubit4Sync temporal synchronization and the POGNAC polarization encoder

Costantino Agnesi
Luca Calderaro, Marco Avesani, Andrea Stanco, Giulio Foletto, Mujtaba Zahidy, Alessia Scriminich, Francesco Vedovato, Giuseppe Vallone and Paolo Villoresi
Dip. di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, Padova, Italy
costantino.agnesi@unipd.it

A major challenge for today's communication networks is to ensure safe exchange of sensitive data between distant parties. However, the rapid development of the Quantum Computer poses a substantial threat for current cyber-security systems, potentially rendering today's cryptographic schemes obsolete and completely insecure. Fortunately, Quantum Key Distribution (QKD) represents a solution to this catastrophic scenario. By leveraging on the principles of quantum mechanics and the characteristics of photons, QKD allows two distant parties, conventionally called Alice and Bob, to distil a perfectly secret key and bound the shared information with any adversarial eavesdropper [1]. Recent developments have focused mainly on rendering QKD implementations simpler and more robust, aiming for compatibility with standard communication networks and widespread usage. This has led, for example, to the introduction of improved optical setups and simpler QKD protocols. However, current QKD implementations usually include additional hardware that perform auxiliary tasks such as temporal synchronization and polarization basis tracking. Here we present a polarization-based QKD system operating at 1550 nm that performs synchronization and polarization compensation by exploiting only the hardware already needed for QKD. Temporal synchronization, which is crucial to discriminate between the quantum signal and noise as well as to correlate the qubit sequence transmitted by Alice with the detection events recorded by Bob, is performed using the Qubits4Sync method which does not require any auxiliary time reference and works by sending a public qubit sequence at pre-established times [2]. The novelty of Qubit4Sync is the implementation of a fast correlation algorithm requiring lower computational cost which allows real-time operation and copes with the high losses of a quantum channel. Polarization basis tracking, which compensate the mechanical and temperature fluctuations that transform the polarization state of the photons that travel through the quantum channel, also exploit predetermined qubit sequences to monitor and compensate for the polarization drift. Polarization encoding is performed by the POGNAC [3], a self-compensating Sagnac loop modulator that exhibits high temporal stability and, with a Polarization Extinction Ratio of over 33 dB, the lowest intrinsic quantum bit error rate reported so far. The QKD system was tested over a fiber-optic link, demonstrating tolerance up to about 40 dB of channel losses. Due to its reduced hardware requirements and the quality of the source, this work represents an important step towards technologically mature QKD systems. Further details of this work can be found in [4].

REFERENCES

[1] S. Pirandola et al., Adv. Opt. Photon. **12**, 1012 (2020)
[2] L. Calderaro *et al.*, Phys. Rev. Appl. **13**, 054041 (2020).
[3] C. Agnesi *et al.*, Opt. Lett. **44**, 2398 (2019).
[4] C. Agnesi et al., Optica **7**, 284 (2020).

FIGURES

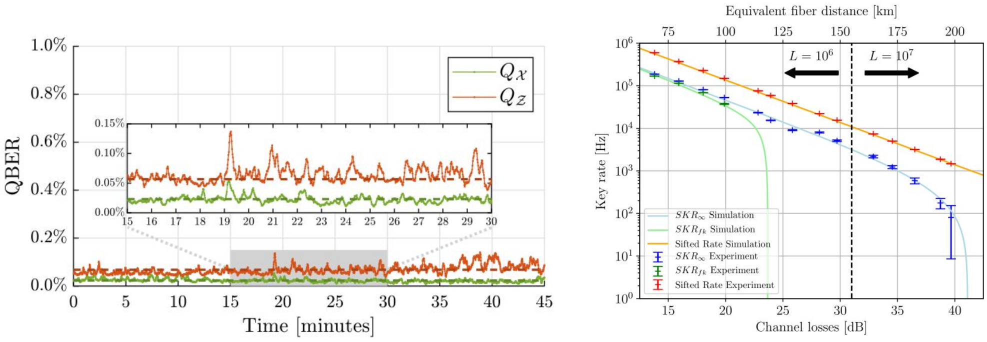

Figure 1: Record-low QBER of the POGNAC encoder and the Secret Key Rate achieved by our system.