Investigating feasibility of broadband continuous variable quantum key distribution in telecom fibers with local local oscillator

Nitin Jain,[1] Christian S. Jacobsen,[1] Dino Solar Nikolic,[1] Arne Kordts,[1] Cosmo Lupo,[2] Ruben Grigoryan,[1] Thomas Pedersen,[3] Stefano Pirandola,[2,4] Tobias Gehring,[1] and Ulrik L. Andersen[1]

[1)] *Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark*

[2)] *York Centre for Quantum Technologies (YCQT), University of York, York YO10 5GH, United Kingdom*

[3)] *Cryptomathic A/S, Jaegergardsgade 118, 8000 Aarhus, Denmark*

[4)] *Computer Science, University of York, York YO10 5GH, United Kingdom*

The use of quantum continuous variables (CV) in quantum key distribution (QKD) presents important advantages with respect to qubit-based protocols, particularly from a practical point of view and cost[1,2]. These schemes allow standard telecommunication technology to be employed, thus making implementations simpler and cheaper. Also, CV-QKD schemes promise high key rates at metropolitan distances.

Traditionally, CV-QKD systems transmit a local oscillator (LO) through the quantum channel, which is assumed to be fully controlled by an adversary. Side-channel attacks, where the adversary can manipulate such a transmitted LO (used as such by the receiver to establish a phase reference) are known. In our setup, we therefore use local local oscillator (LLO) to close such side channels[3–5]. This makes the transmitter design more simple, however, introduces some implementation challenges on the receiver side.

In order to achieve high key rates, we employ broadband coding where quantum states are encoded in sidebands of several tens of MHz. In principle, the sidebands could be broadened to GHz regimes with suitable RF electronics. The quantum signal can also be manipulated in spectral domain in order to achieve full QKD functionality even when transmitter and LLO frequencies do not match.

There are many challenges following the building of a practical QKD system. We are addressing several important ones: frequency and phase recovery and symbol synchronization, polarization drifts in the quantum channel which require polarization control feedback at the receiver side, different modulation schemes such as single side band modulation using IQ modulators, and high rate postprocessing in high-end FPGA technology. Finally, it is vital that the implemented protocol is secure in a model with carefully chosen threat assumptions. Our system employs coherent states with Gaussian modulation for which there is a proof of security against collective Gaussian attacks[6,7] but there are still some challenges in adapting that security proof to real-world scenarios, which we are also addressing.

[1] Diamanti, E.; Leverrier, A. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. Entropy, 17, 6072-6092 (2015)

[2] Scarani V., Bechmann-Pasquinucci H., Cerf N., Dusek M., Lutkenhaus N., and Peev M. The security of practical quantum key distribution. Rev. Mod. Phys., 81, 1301-1350 (2009)

[3] Qi B., Lougovski P., Pooser R., Grice W., and Bobrek M. Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X, 5, 041009 (2015)

[4] Huang D., Huang P., Lin D., Wang C., and Zeng G. High-speed continuous-variable quantum key distribution without sending a local oscillator. Opt. Lett., 40(16), 3695-3698 (2015)

[5] Kleis S., Rueckmann M., and Schaeffer C. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. Opt. Lett. 42, 1588-1591 (2017)

[6] Leverrier A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States.Phys. Rev. Lett. 114, 070501 (2015)

[7] Leverrier A. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. Phys. Rev. Lett. 118, 200501 (2017)