Effect of experimental imperfections in continuous-variable quantum key distribution

Andrés Ruiz-Chamorro[1], Daniel Cano[1], Aida García-Callejo[1] and Verónica Fernández-Mármol[1]

[1] Institute of Physical and Information Technologies, Spanish National Research Council (CSIC), 28006 Madrid, Spain

ABSTRACT

Quantum key distribution (QKD) enables secure communication using quantum mechanics. Continuous-variable quantum key distribution (CV-QKD) makes use of bosonic modes of the electromagnetic field generated by a laser field (coherent states) to achieve secure key transmission. However, experimental CV-QKD systems face challenges due to electronic and optical imperfections in the experimental devices. This study develops a model and a simulated twin of an experimental CV-QKD system to analyze the impact of such imperfections on the security of the key transmission.

The CV-QKD system we consider follows the GG02 protocol. In this protocol, Alice, the transmitter, sends gaussian-modulated coherent states to Bob, the receiver, over a noisy channel. Bob performs heterodyne detection, measuring both the amplitude and phase of the received coherent states simultaneously. This measurement introduces quantum uncertainty, which is experimentally observed as noise. After transmission, Alice and Bob share a portion of the key to assess the security of the transmission and detect if a potential eavesdropper could obtain excessive information. If such a scenario is detected, the protocol is aborted. Otherwise, error correction and privacy amplification algorithms are employed to distill the key.

We simulate the first part of the protocol, detailing all experimental electro-optical components to analyze how they affect the quality of the transmission. The setup includes software-defined radios (SDR) for signal generation/reception, an IQ modulator, a 2x2 beam-splitter, and a balanced photodetector.

Experimental imperfections considered during the simulations are frequency and phase drifts in the laser sources, an imbalanced IQ modulator, differences in beam splitter reflectance and transmittance indices, and gain imbalances in the balanced detector. "Our simulation engine reproduces the setup by simulating the transmission of a key consisting of random symbols. By comparing the sent and received symbols, we are able to estimate the Secret Key Rate (SKR) of the transmission. The SKR is the most important security and performance metric in CV-QKD, as it ensures that the key cannot be obtained by an eavesdropper.

Our simulations show that laser frequency drifts significantly reduce the secret key rate, while even slight impairments in beam splitter ratios or photodiode gains have noticeable effects on key transmission. However, minor variations in the IQ modulator do not significantly impact the SKR. Our model and simulations aid in the initial calibration of CV-QKD systems, enabling faster optimization and preventing a decrease in SKR due to common imperfections. By addressing and optimizing these imperfections, we enhance the performance of CV-QKD systems, potentially enabling secure long-distance or high-speed transmission in future quantum networks.