Noisy Detector? Good!
Analysis of Trusted-Receiver Scenario in Continuous-Variable Quantum Key Distribution

Fabian Laudenbach1,* and Christoph Pacher1

1 Security & Communication Technologies, Center for Digital Safety & Security, AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria
*Contact: fabian.laudenbach@ait.ac.at

Abstract
In CV-QKD the trusted-receiver assumption allows for a significant improvement in terms of key rate and achievable transmission distance. Moreover, as we demonstrate, sometimes imperfect detection can even be beneficial for the key rate.

Introduction
In continuous-variable quantum key distribution (CV-QKD) [1,2] the achievable secure-key rate and channel length are most prominently confined by optical loss and quadrature noise which are attributed to possible attacks conducted by a malicious eavesdropper. This sensitivity to loss and noise can be partially mitigated under the trade-off of relaxed security assumptions, i.e. by classifying the detection apparatus as well-calibrated and beyond influence of a potential eavesdropper. The trusted-receiver assumption makes a rather great difference in terms of system performance, not least because in practical systems the electronic receiver noise makes up by far the greatest contribution to the total noise.

On top of a trusted receiver, our approach of modelling an entangling-cloner attack allows us to consider the impact of trusted state-preparation noise [3] without an increase of the mathematical complexity.

Numerical evaluation
Secure-key rate with respect to channel length under various security assumptions. As the graph illustrates, declaring the receiver and/or state preparation as trusted yields a significant performance enhancement in terms of key rate and transmission distance.

Two approaches to compute the Holevo information \(\chi_{EB} = S_E - S_{E|B}\):

- Eve purifies Alice’s and Bob’s state: \(\rho_{AB} = Tr_E(\rho_{ABE})\).
- Therefore Eve’s entropy equals Alice’s and Bob’s entropy.
- \(S_E = S_{E|B}\) is computed by the symplectic eigenvalues of a 12 x 12 covariance matrix (3 EPR states \(\rightarrow\) 6 optical modes \(\rightarrow\) 12 quadrature components).

- Eve possesses her own EPR state and interferes with the channel.
- \(S_E\) is computed by the symplectic eigenvalues of a 4 x 4 covariance matrix (1 EPR state \(\rightarrow\) 2 optical modes \(\rightarrow\) 4 quadrature components)

CVsim – a multisided simulation tool for CV-QKD

- MATLAB-based standalone application
- >30 input parameters to specify setup
- Dynamic optimisation of modulation variance
- 8 numeric results
- 128 different plots to be arbitrarily parametrised

Acknowledgements
This work has been funded by the European Union’s Horizon 2020 research and innovation programme over the Quantum-Flagship projects UNIQORN (no. 820474) and CiViQ (no. 820466).

References