CVsim: a novel CVQKD simulation tool

Fabian Laudenbach*[1], Christoph Pacher[1], Chi-Hang Fred Fung[2], Momtchil Peev[2], Andreas Poppe[2], and Hannes Hübel[1]

[1]Optical Quantum Technology, Digital Safety & Security Department,
AIT Austrian Insitute of Technology GmbH, Donau-City-Str. 1, 1220 Vienna, Austria
[2]Quantum Communication and Computing Laboratory, German Research Center,
Huawei Technologies Düsseldorf GmbH, Riesstr. 25-C3, 80992 Munich, Germany

We present a novel piece of software which simulates continuous-variable quantum key distribution (CVQKD) using Gaussian-modulated coherent states. The user enters the details of an experimental setup, specifying the transmitter laser, the channel loss, noise figures, post-processing parameters and several other characteristics, and the program will deliver the according numerical and graphical performance results. **CVsim** allows the user to analyse and compare different experimental setups as well as the effects of specific hardware components in great detail and in a matter of seconds.

Continuous-variable quantum key distribution using coherent states [1–4] is regarded as a promising realisation of quantum cryptography due to high compatibility with existing telecom components and high detection efficiency (PIN diodes vs. single-photon detectors). However, the actual performance of a CVQKD system depends on a large variety of parameters related to the transmitter system (e.g. modulation variance, symbol rate, wavelength, phase noise) the quantum channel (e.g. channel length, transmittance, coupling losses, Raman noise), the receiver setup (e.g. detection efficiency, detection noise, quantisation error) and postprocessing (e.g. reconciliation efficiency, code rate, frame-error rate). Our software **CVsim** allows the the user to enter arbitrary specifications of his system into a graphical user interface (Figure 1) and delivers a detailed analysis of the experimental setup. The calculated numeric results include

- Secret bits per symbol r and secret key rate K
- Mutual information I_{AB} shared by Alice and Bob
- Holevo information χ_{EB} between Eve and Bob
- Code rate R
- Signal-to-noise ratio SNR
- Modulation noise, phase noise, Raman noise, detection noise, quantisation noise and the total excess noise ξ
- Total transmittance T and loss L
- Energy per bit over spectral noise density E_b/N_0
- Key-rate-maximising modulation variance $V_{\mathrm{A,max}}$
- Voltage range δU of the amplified signal.

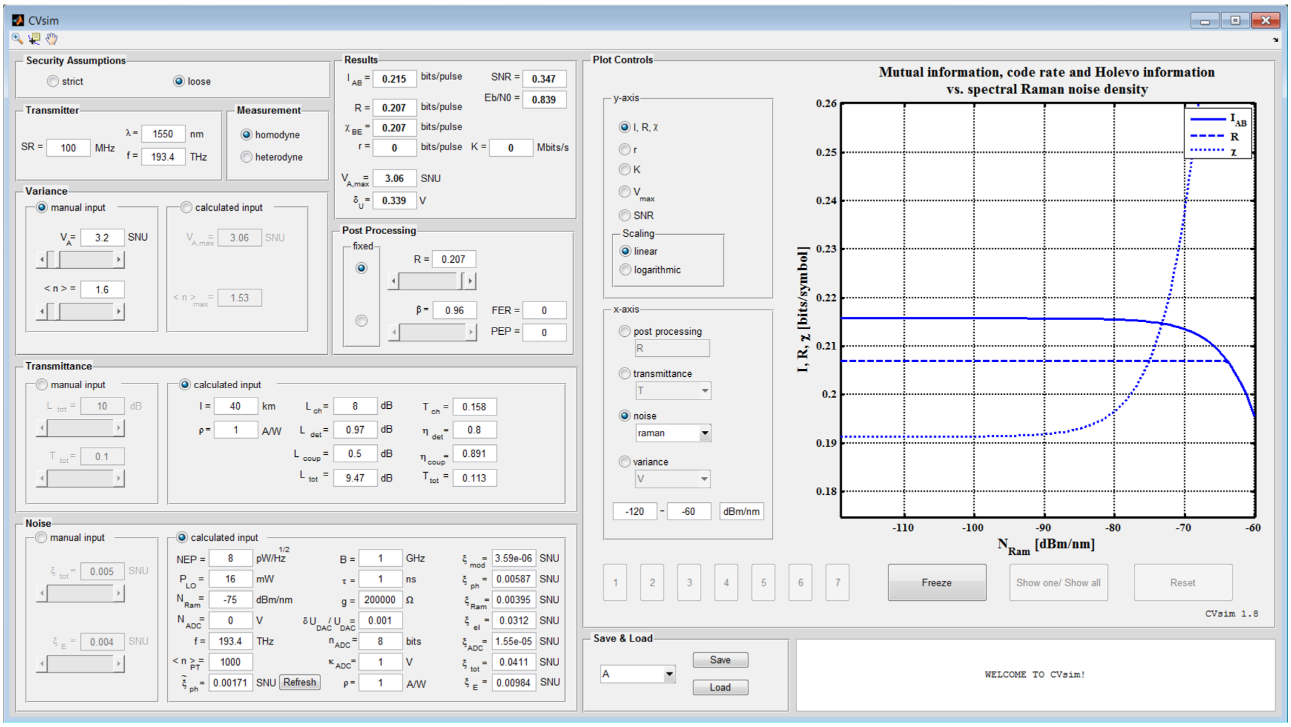
Moreover, **CVsim** comes with a large variety of plots to analyse and compare different configurations. The user can freely choose which parameter should be displayed with respect to which (independent selection of y- and x-axis), therefore being able to select from a total number of 142 different plots in which any of the 42 input parameters can be arbitrarily parametrised (see Figures 2 and 3 for examples).

The equations on which this software is based on are derived from Gaussian quantum information, phase-space quantum optics, information theory and signal processing theory. In order to correctly take account of experimental imperfections and their impact on the protocol's performance, we developed models for various noise sources, including [5]

- Modulation noise, caused by voltage fluctuations of the digital-to-analog converter
- Phase noise, caused by phase fluctuations of the transmitter laser
- Raman noise, caused by Raman scattering, generated by a classical DWDM channel in the fibre
- Electronic noise, caused by the balanced homodyne receiver
- ADC noise, caused by quantisation of an analog-to-digital converter.

Taking advantage of the intuitive use of the GUI and of the large amount of input parameters, numeric results and optional plots, we were able to gain intriguing and unprecedented insights on the mutual relation of various components and their influence on the quality of the actual experiment. We will present the results most relevant for typical realisations and demonstrate which parameters are particularly crucial to enhance the experimental performance in terms of key rate and channel length. Given its extensive features and the large variety of result output, we believe that our software is a resourceful tool which contributes to the better understanding of any realistic CVQKD setup.

*fabian.laudenbach.fl@ait.ac.at



CVsim

Security Assumptions: ○ strict ● loose

Transmitter: SR = 100 MHz; λ = 1550 nm; f = 193.4 THz

Measurement: ● homodyne ○ heterodyne

Variance: ● manual input: V_A = 3.2 SNU; < n > = 1.6. ○ calculated input: $V_{A,max}$ = 3.06 SNU; $< n >_{max}$ = 1.53

Results: I_{AB} = 0.215 bits/pulse; SNR = 0.347; Eb/N0 = 0.839; R = 0.207 bits/pulse; χ_{BE} = 0.207 bits/pulse; r = 0 bits/pulse; K = 0 Mbits/s; $V_{A,max}$ = 3.06 SNU; δ_U = 0.339 V

Post Processing: fixed ● R = 0.207; ○ β = 0.96; FER = 0; PEP = 0

Transmittance: ○ manual input: L_{tot} = 10 dB; T_{tot} = 0.1. ● calculated input: l = 40 km; ρ = 1 A/W; L_{ch} = 8 dB; L_{det} = 0.97 dB; L_{coup} = 0.5 dB; L_{tot} = 9.47 dB; T_{ch} = 0.158; η_{det} = 0.8; η_{coup} = 0.891; T_{tot} = 0.113

Noise: ○ manual input: ξ_{tot} = 0.005 SNU; ξ_E = 0.004 SNU. ● calculated input: NEP = 8 pW/Hz$^{1/2}$; P_{LO} = 16 mW; N_{Ram} = -75 dBm/nm; N_{ADC} = 0 V; f = 193.4 THz; $< n >_{PT}$ = 1000; $\tilde{\xi}_{ph}$ = 0.00171 SNU; B = 1 GHz; τ = 1 ns; g = 200000 Ω; $\delta U_{DAC} / U_{DAC}$ = 0.001; n_{ADC} = 8 bits; κ_{ADC} = 1 V; ρ = 1 A/W; ξ_{mod} = 3.59e-06 SNU; ξ_{ph} = 0.00587 SNU; ξ_{Ram} = 0.00395 SNU; ξ_{el} = 0.0312 SNU; ξ_{ADC} = 1.55e-05 SNU; ξ_{tot} = 0.0411 SNU; ξ_E = 0.00984 SNU

Plot Controls: y-axis: ● I, R, χ ○ r ○ K ○ V_{max} ○ SNR; Scaling: ● linear ○ logarithmic. x-axis: ○ post processing: R ○ transmittance: T ● noise: raman ○ variance: V; -120 - -60 dBm/nm

Save & Load: A

WELCOME TO CVsim!

Figure 1: The graphical user interface of **CVsim**.

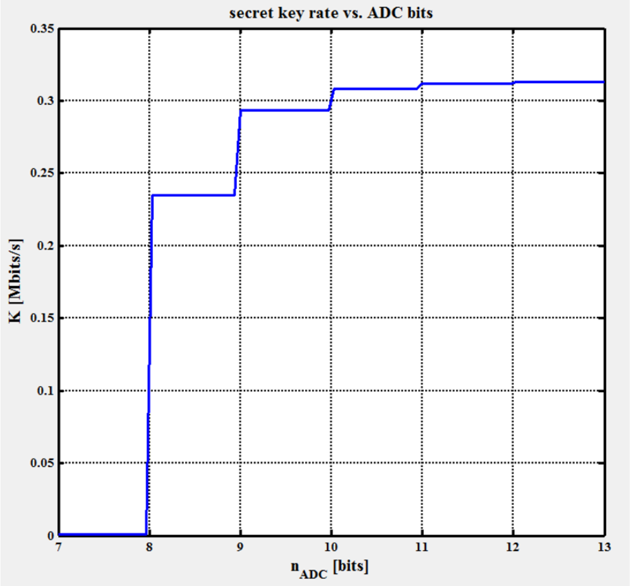


Figure 2: Dependence of the key rate K on the bit resolution of the analog-to-digital converter.

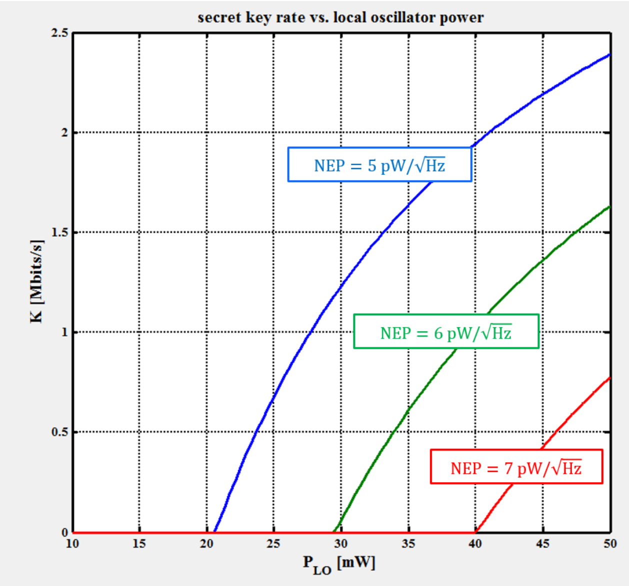


Figure 3: Dependence of the key rate K on the local-oscillator power P_{LO}, parametrised after the noise-equivalent power (NEP) of the balanced homodyne receiver.

References

[1] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5):057902, 2002.

[2] Frédéric Grosshans, Nicolas J Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Ph Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0306141*, 2003.

[3] Christian Weedbrook, Stefano Pirandola, and Timothy C Ralph. Continuous-variable quantum key distribution using thermal states. *Physical Review A*, 86(2):022318, 2012.

[4] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[5] Fabian Laudenbach, Christoph Pacher, and Hannes Hübel. Theoretical model for CVQKD simulation software. *Manuscript in preparation*, 2016.