CVsim: a novel CV-QKD simulation tool

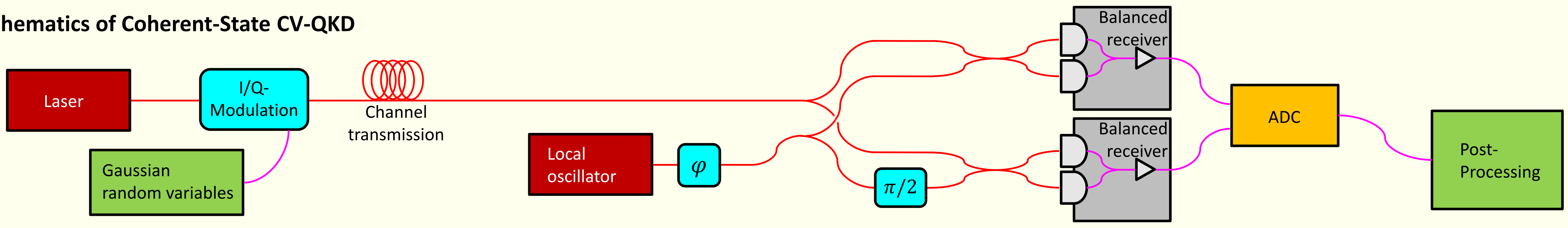
Fabian Laudenbach[1,3,*], Christoph Pacher[1], Chi-Hang Fred Fung[2], Momtchil Peev[2], Andreas Poppe[2], Hannes Hübel[1]

[1] Optical Quantum Technologies, Digital Safety and Security Department, **AIT Austrian Institute of Technology GmbH**, Donau-City-Straße 1, 1220 Vienna, Austria
[2] Quantum Communication and Computing Laboratory, German Research Center, **Huawei Technologies Düsseldorf GmbH**, Riesstr. 25-C3, 80992 Munich, Germany
[3] Quantum Optics, Quantum Nanophysics & Quantum Information, Faculty of Physics, **University of Vienna**, Boltzmanngasse 5, 1090 Vienna, Austria
*Contact: fabian.laudenbach.fl@ait.ac.at

Abstract

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 CV-QKD 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 post-processing (e.g. reconciliation efficiency, code rate, frame-error rate). Our software **CVsim** allows the user to enter arbitrary specifications of his system into a graphical user interface and delivers a detailed analysis of the experimental setup.

Schematics of Coherent-State CV-QKD



Numerical Results

- Mutual information
- SNR
- Code rate
- Holevo Information
- Secret fraction
- Key rate
- Key-rate-maximising variance
- Voltage range of amplified signal

Security Assumptions

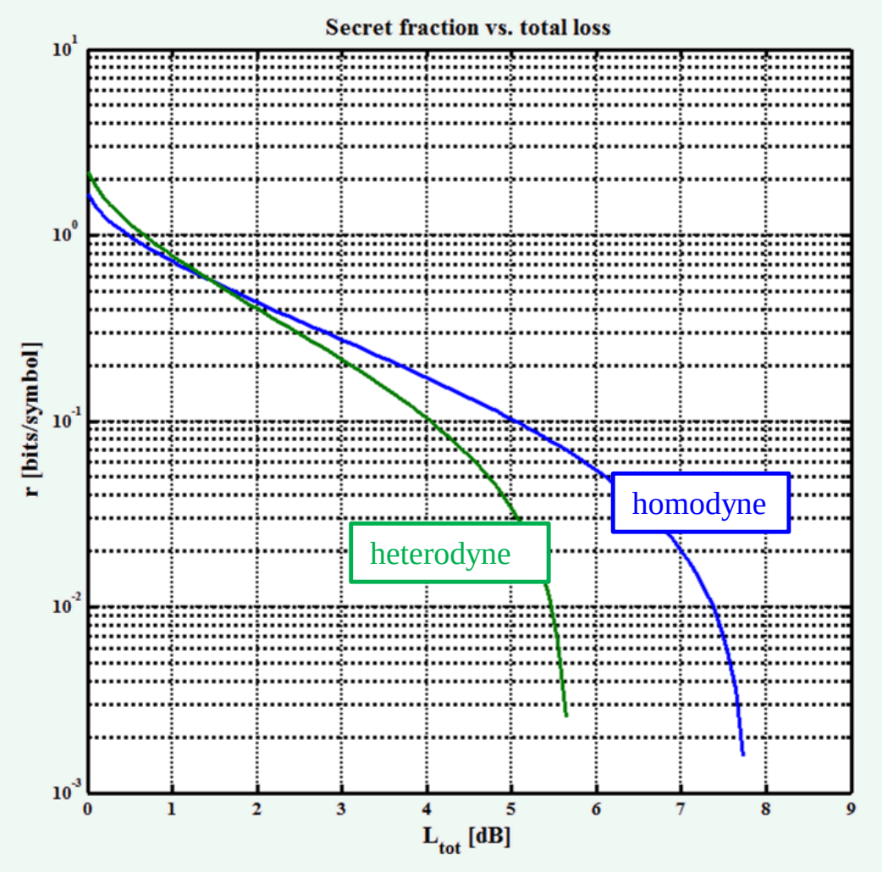
- Optional trusted-device assumption

Transmitter

- Symbol rate
- Optical wavelength/ frequency

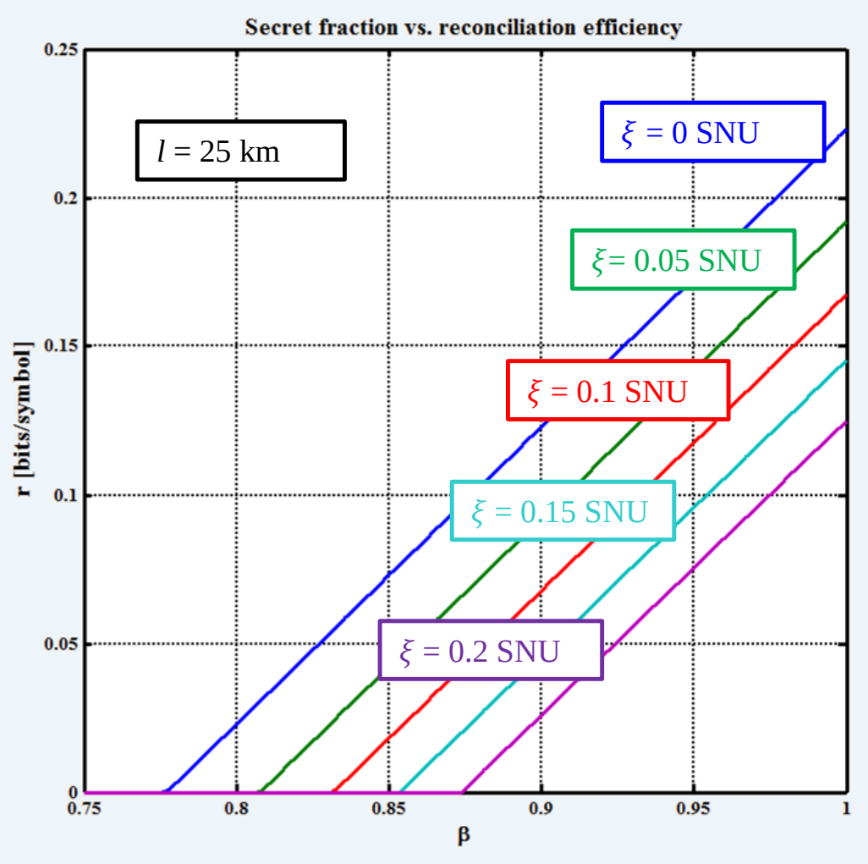
Measurement

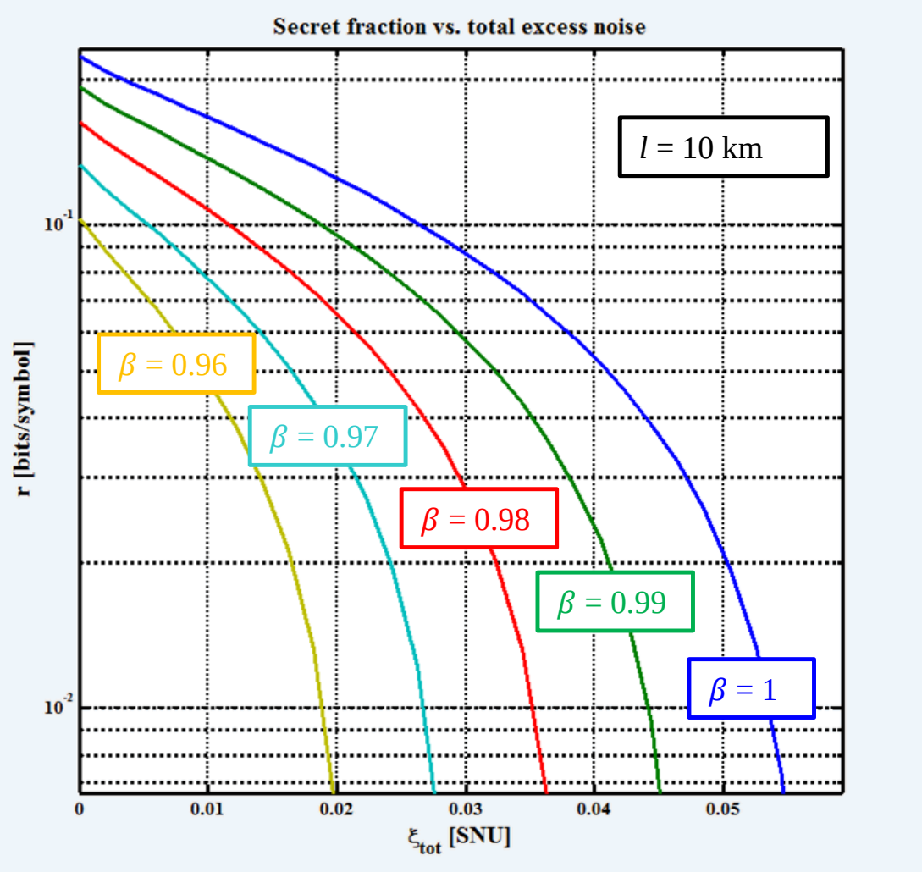
- Homodyne/ heterodyne detection



Post-Processing

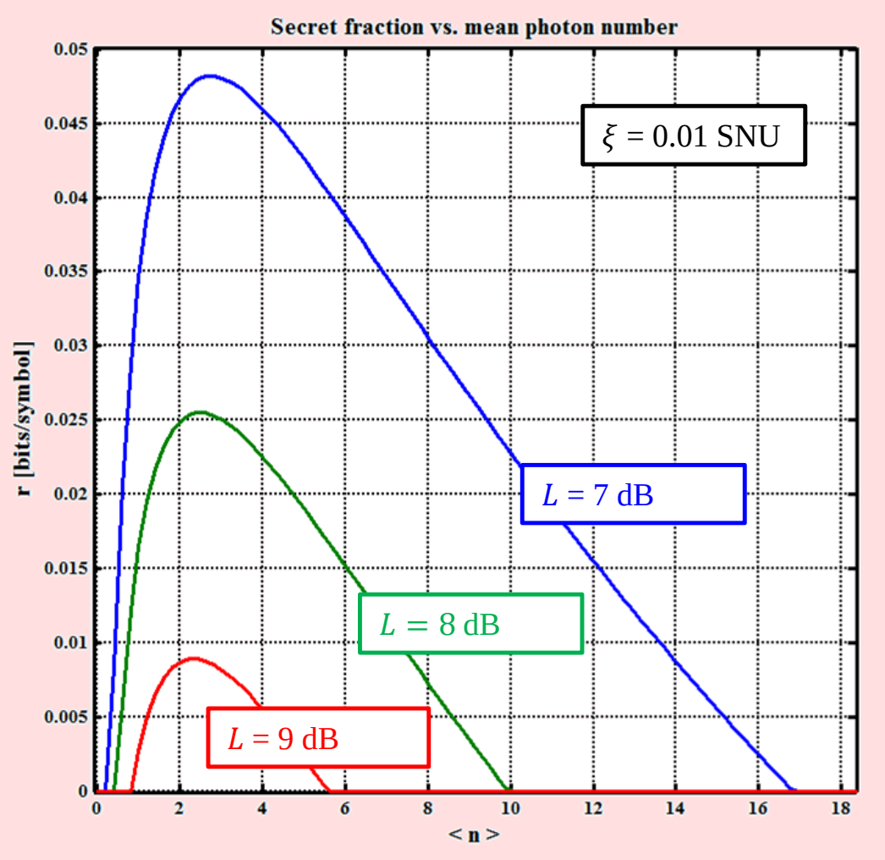
- Code rate
- Reconciliation efficiency
- Frame-error rate
- Fraction disclosed for parameter-estimation





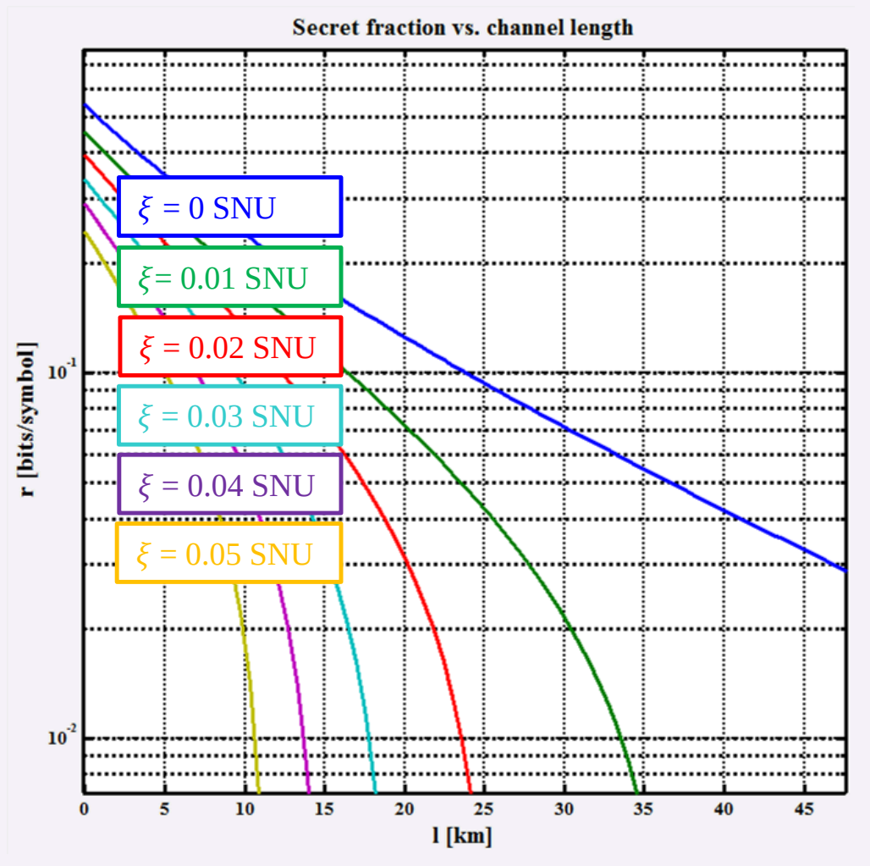
Variance

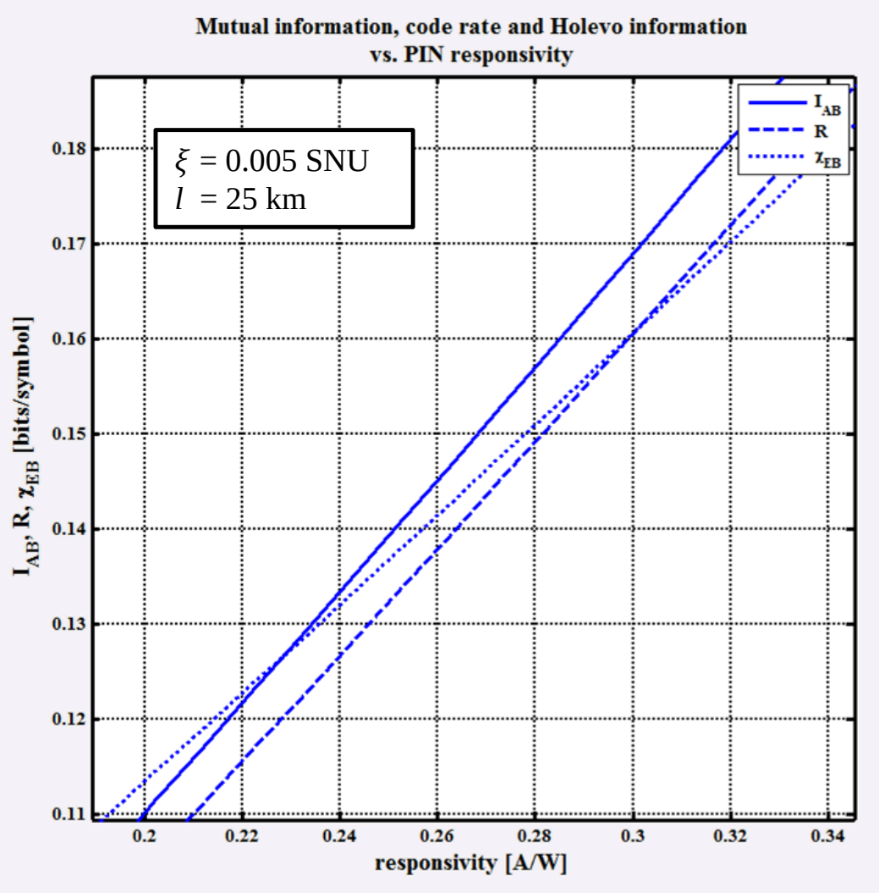
- Modulation variance
- Mean photon number
- Key-rate-maximising variance

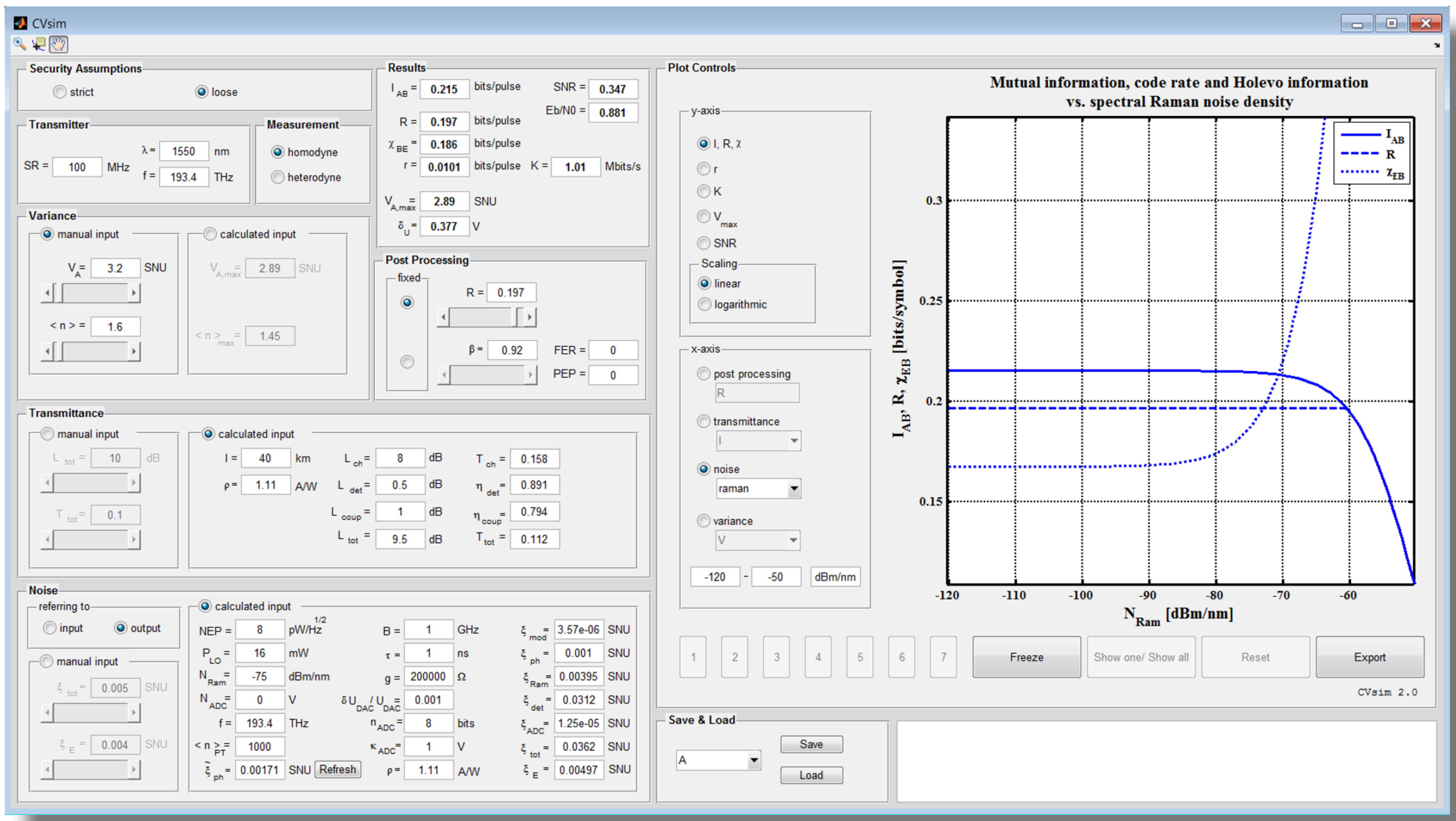


Transmittance

- Channel loss
- Coupling loss
- Detection efficiency/ PIN responsivity







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: $V_{A,max}$ = 2.89 SNU; $< n >_{max}$ = 1.45

Results: I_{AB} = 0.215 bits/pulse; SNR = 0.347; Eb/N0 = 0.881; R = 0.197 bits/pulse; χ_{BE} = 0.186 bits/pulse; r = 0.0101 bits/pulse; K = 1.01 Mbits/s; $V_{A,max}$ = 2.89 SNU; δ_U = 0.377 V

Post Processing: fixed ● R = 0.197; ○ β = 0.92; FER = 0; PEP = 0

Transmittance: ○ manual input: L_{tot} = 10 dB; T_{tot} = 0.1 — ● calculated input: l = 40 km; ρ = 1.11 A/W; L_{ch} = 8 dB; L_{det} = 0.5 dB; L_{coup} = 1 dB; L_{tot} = 9.5 dB; T_{ch} = 0.158; η_{det} = 0.891; η_{coup} = 0.794; T_{tot} = 0.112

Noise: referring to ○ input ● output; ○ 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 [Refresh]; 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 = 1.11 A/W; ξ_{mod} = 3.57e-06 SNU; ξ_{ph} = 0.001 SNU; ξ_{Ram} = 0.00395 SNU; ξ_{det} = 0.0312 SNU; ξ_{ADC} = 1.25e-05 SNU; ξ_{tot} = 0.0362 SNU; ξ_E = 0.00497 SNU

Plot Controls: y-axis: ● I, R, χ ○ r ○ K ○ V_{max} ○ SNR; Scaling: ● linear ○ logarithmic; x-axis: ○ post processing R ○ transmittance l ● noise raman ○ variance V; -120 - -50 dBm/nm

Save & Load: A [Save] [Load]

Mutual information, code rate and Holevo information vs. spectral Raman noise density
I_AB, R, χ_EB [bits/symbol]
N_Ram [dBm/nm]
I_AB
R
χ_EB
1
2
3
4
5
6
7
Freeze
Show one/ Show all
Reset
Export
CVsim 2.0

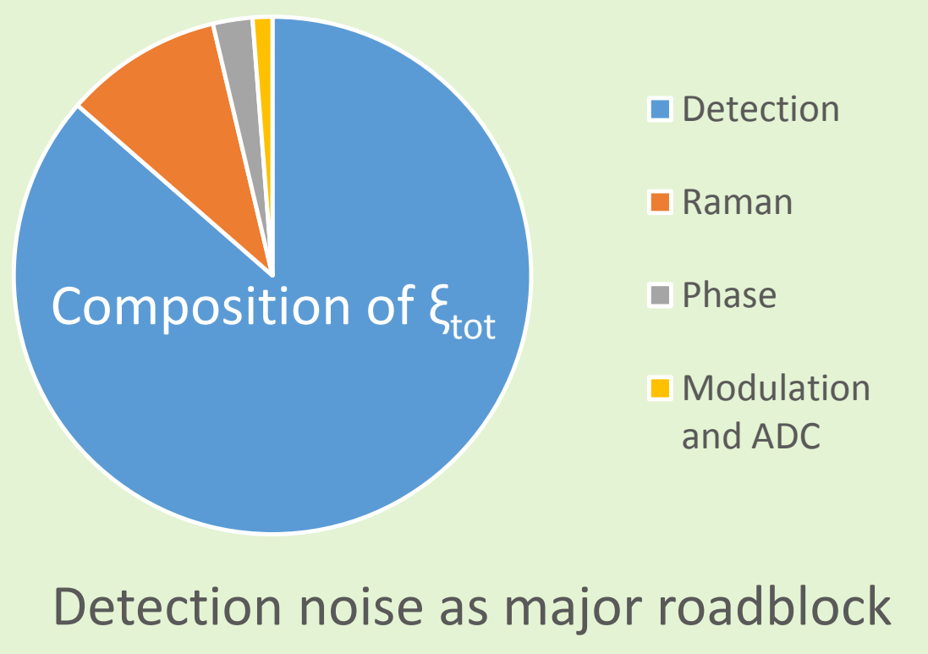
Plots

- *y*-axis
  - Mutual information
  - SNR
  - Code rate
  - Holevo information
  - Secret fraction
  - Key rate
  - Key-rate-maximising variance
- *x*-axis: 21 parameters related to:
  - Post-processing
  - Transmittance
  - Noise
  - Variance
- Independent choice of *x*- and *y*-axis
- 142 different plots
- Arbitrary parametrisation of 42 input parameters
- Linear and logarithmic scale

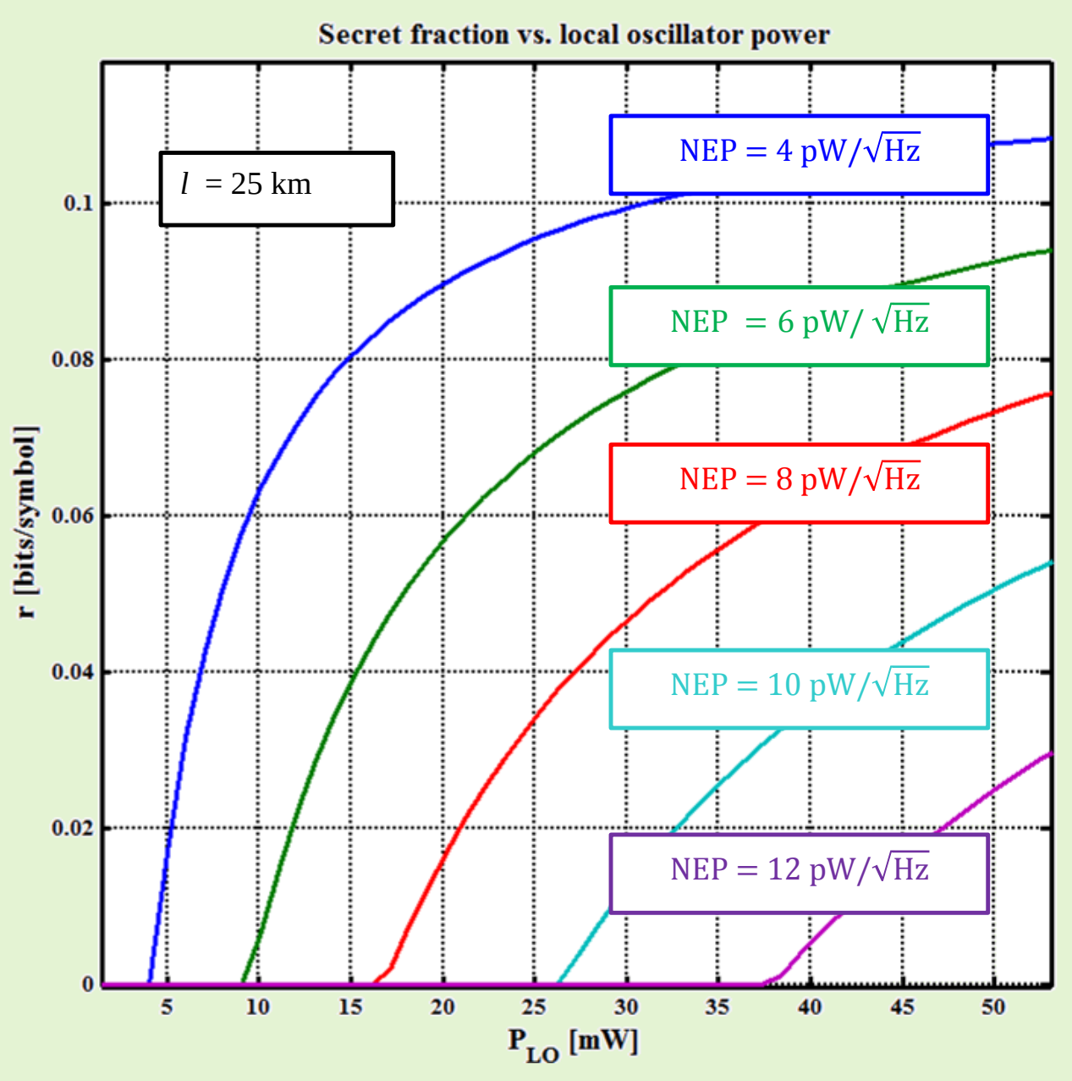
Excess Noise

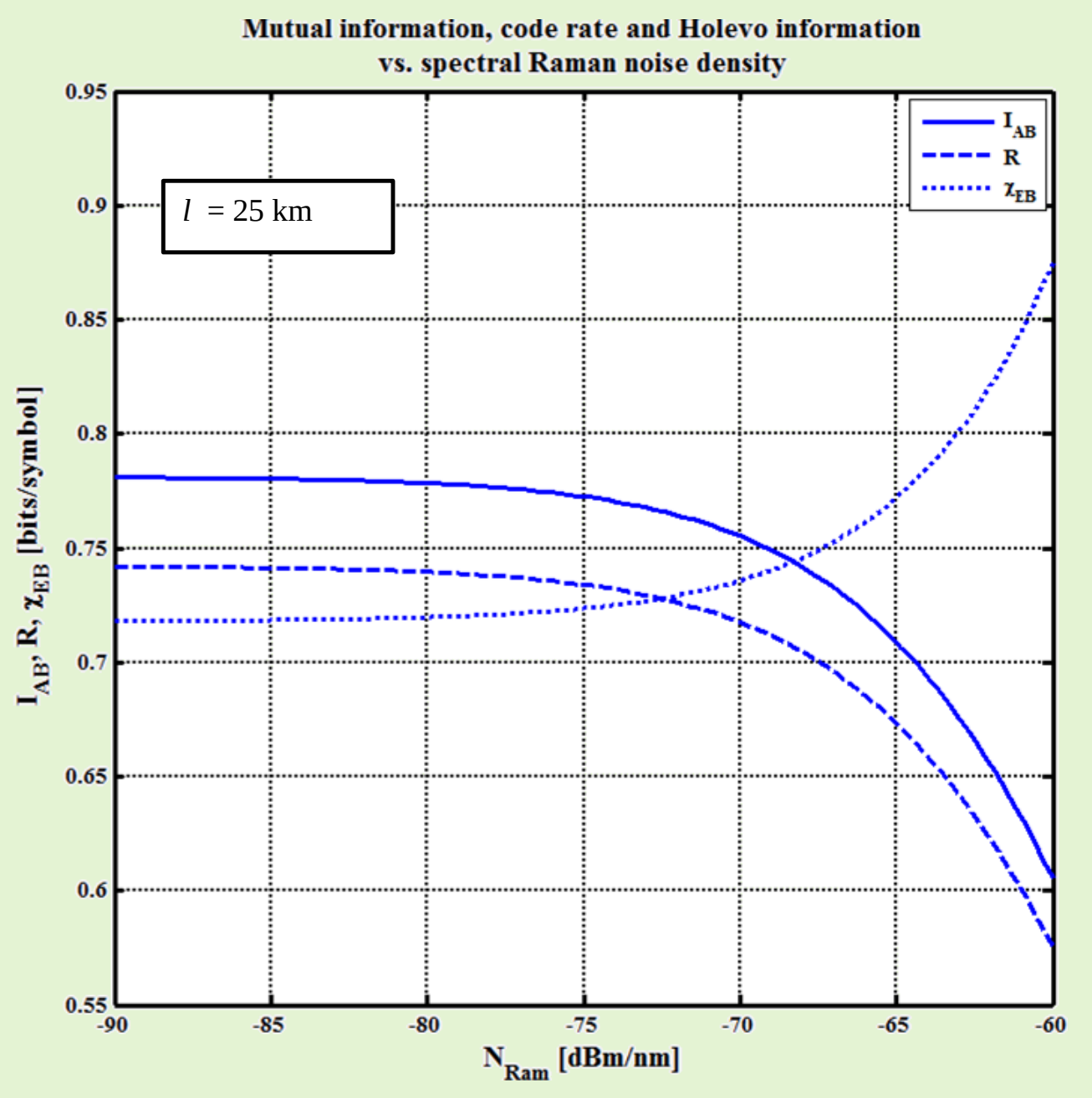
Self-developed models for

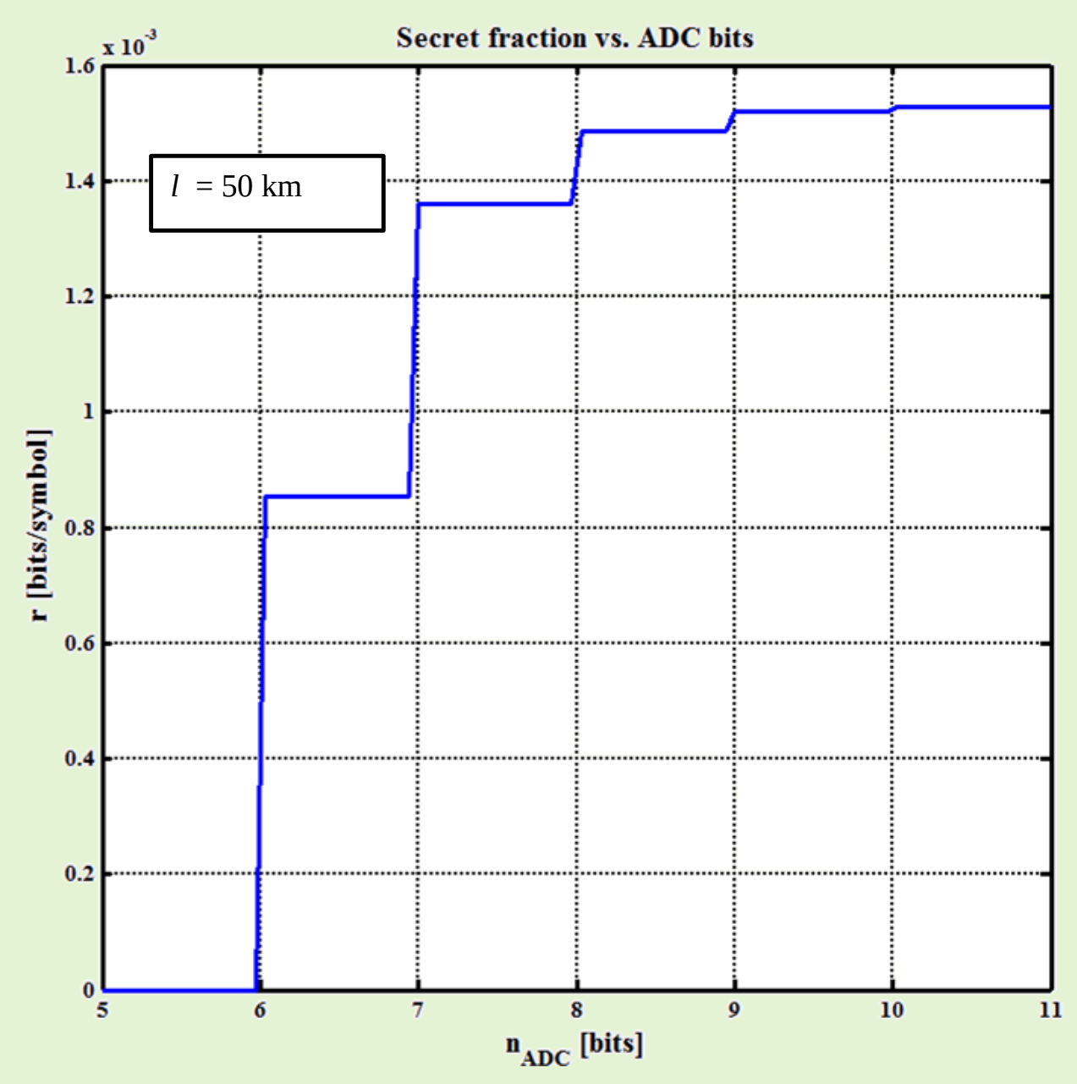
- Modulation noise
- Phase noise
- Raman noise
- Detection noise
- Quantisation noise



Detection noise as major roadblock







References

1. F. Grosshans and P. Grangier. *Continuous variable quantum cryptography using coherent states.* Physical Review Letters, 88(5):057902, 2002.
2. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, P. Grangier. *Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables*. arXiv preprint quant-ph/0306141, 2003.
3. C. Weedbrook, S. Pirandola, T.C. Ralph. *Continuous-variable quantum key distribution using thermal states*. Physical Review A, 86(2):022318, 2012.
4. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev. *The security of practical quantum key distribution.* Reviews of Modern Physics, 81(3):1301, 2009.

QCrypt 2016 • Washington DC, September 12th-16th, 2016