ENHANCED FREE-SPACE CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

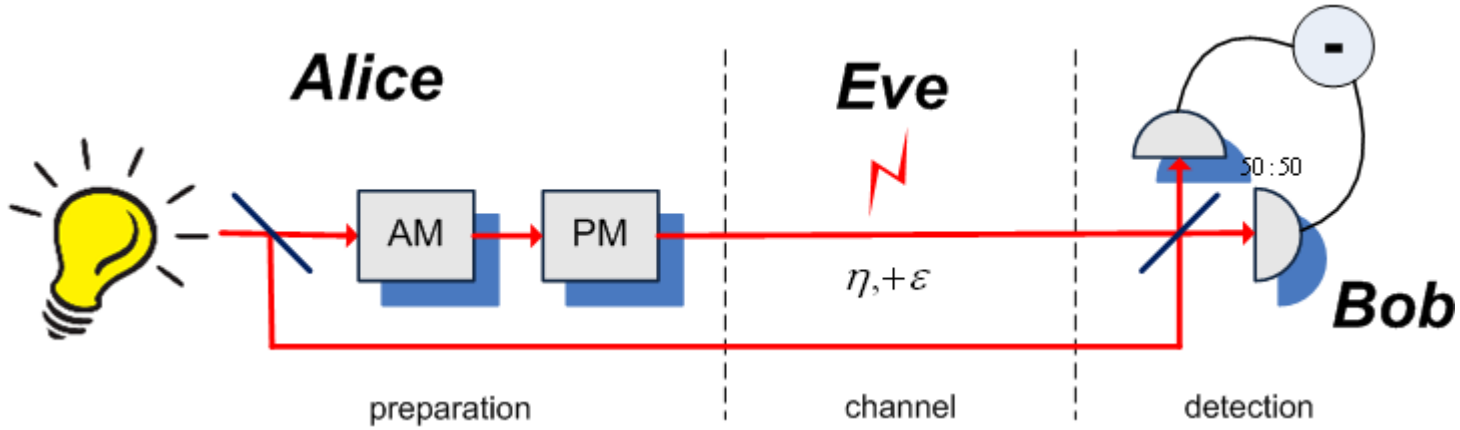
Vladyslav C. Usenko, Ivan Derkach, Laszlo Ruppert, and Radim Filip

Palacký University
Olomouc

Department of Optics, Palacký University, 17. listopadu 50, 772 07 Olomouc, Czech Republic

1. INTRODUCTION

Continuous-variable (CV) **quantum key distribution** (QKD) is aimed at going beyond single-photon statistics and using multiphoton quantum states for QKD. It is typically based on the Gaussian quadrature modulation of coherent or squeezed states of light [1].

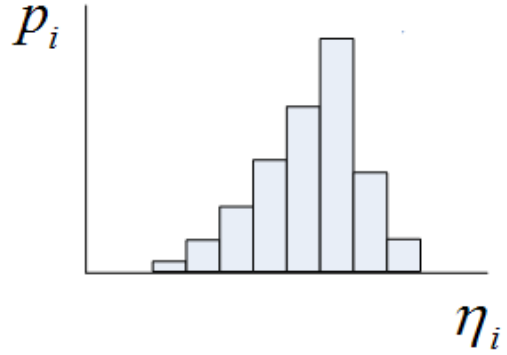


Generic CV QKD scheme based on amplitude and phase quadrature modulation and homodyne detection.

CV QKD is particularly promising for **free-space** implementation due to intrinsic filtering capabilities of a homodyne detector, thus potentially enabling efficient free-space QKD operation in daytime. However, **atmospheric turbulence** affects CV QKD and reduces its applicability. We suggest **channel binning** or use of **squeezed states** in order to overcome the limitations imposed by turbulence in free-space CV QKD.

2. CHANNEL FADING IN FREE-SPACE CV QKD

Atmospheric turbulence leads to **transmittance fluctuations** in free-space channels (also referred to as **fading**), mainly caused by **beam wander** (beam spot fluctuations around the receiver aperture) [2], which can be described by a transmittance probability distribution $p_i(\eta_i)$.



Security analysis of CV QKD is based on the optimality of Gaussian collective attacks. We consider the positivity of the lower bound on secure key rate in either direct (DR) or reverse reconciliation (RR) scenario:

$$K_{DR/RR} = \beta I_{AB} - \chi_{AE/BE},$$

where β is the post-processing efficiency, I_{AB} is the Shannon mutual information between Alice and Bob and $\chi_{AE/BE}$ is the Holevo bound between Eve and the reference side of the respective reconciliation scenario.

3. CHANNEL FADING IN FREE-SPACE CV QKD

We study security of CV QKD against collective attacks in the noisy channels, using equivalent entanglement-based representation with two-mode squeezed vacuum (TMSV) states and heterodyne (for coherent-state protocol) or homodyne (for squeezed-state protocol) detection on the Alice's side.

After a fluctuating channel, the covariance matrix of the two-mode Gaussian state shared between Alice and Bob reads [3]

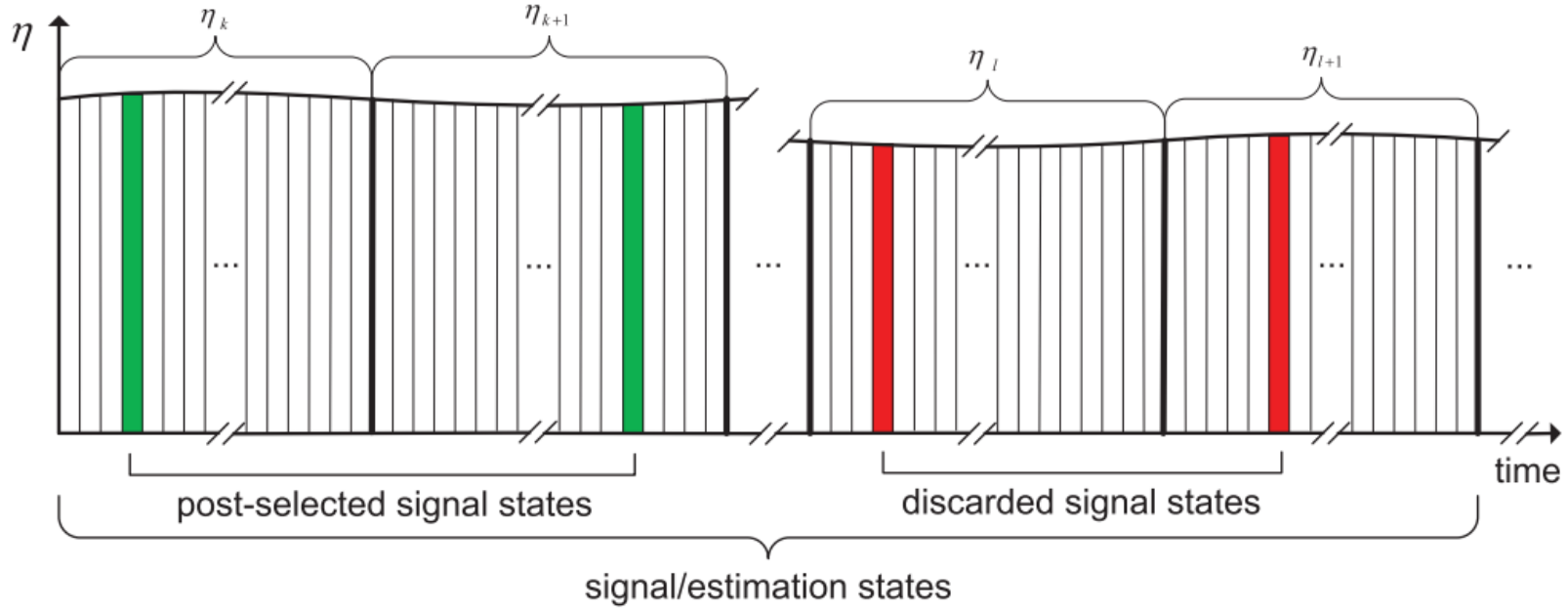
$$\gamma_{AB} = \begin{pmatrix} V\mathrm{I} & \left[\langle\sqrt{\eta}\rangle\sqrt{V^2-1}\right]\sigma_z \\ \left[\langle\sqrt{\eta}\rangle\sqrt{V^2-1}\right]\sigma_z & [V\langle\eta\rangle + 1 - \langle\eta\rangle + \varepsilon]\mathrm{I} \end{pmatrix},$$

where V is the variance of an equivalent TMSV state, I is the 2x2 unity matrix, σ_z is the 2x2 Pauli matrix, ε is the channel excess noise.

The fading channel is then equivalent to a fixed channel with transmittance $\langle\sqrt{\eta}\rangle^2$ and additional excess noise $\mathrm{Var}(\sqrt{\eta})$(V-1), where $\mathrm{Var}(\sqrt{\eta})=\langle\eta\rangle - \langle\sqrt{\eta}\rangle^2$. This noise limits the applicable modulation and may lead to loss of security of the protocol [4].

4. CHANNEL POST-SELECTION IN CV QKD

As a counter-measure against fading in CV QKD the post-selection of relatively stable sub-channels can be used so that only the data received in the certain estimated transmittance windows is stored and the rest is discarded:

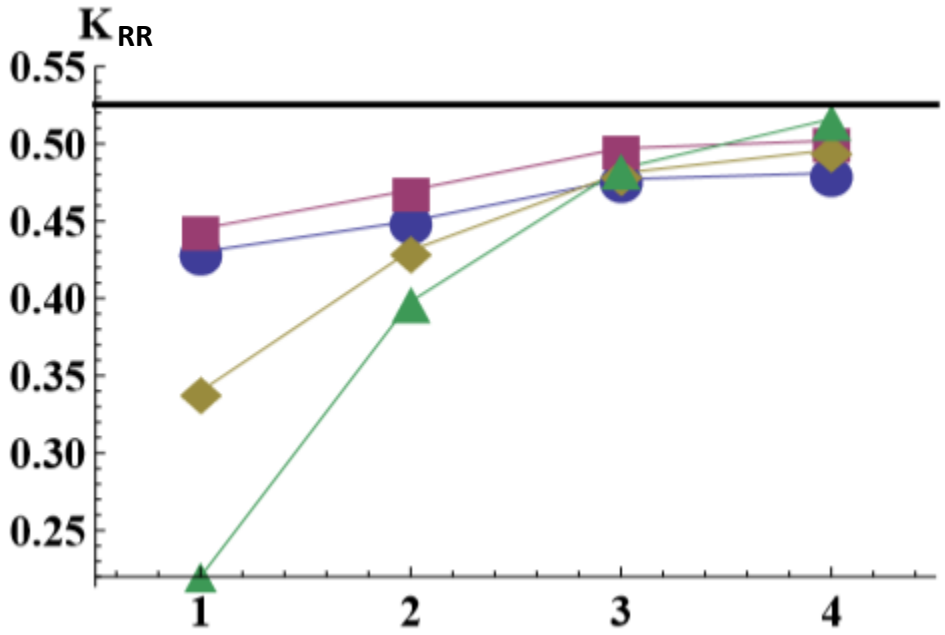


Sub-channel post-selection based on the channel binning and estimation.

It was shown that such method allows to substantially improve performance of free-space coherent-state CV QKD [4].

5. CHANNEL POST-SELECTION IN CV QKD

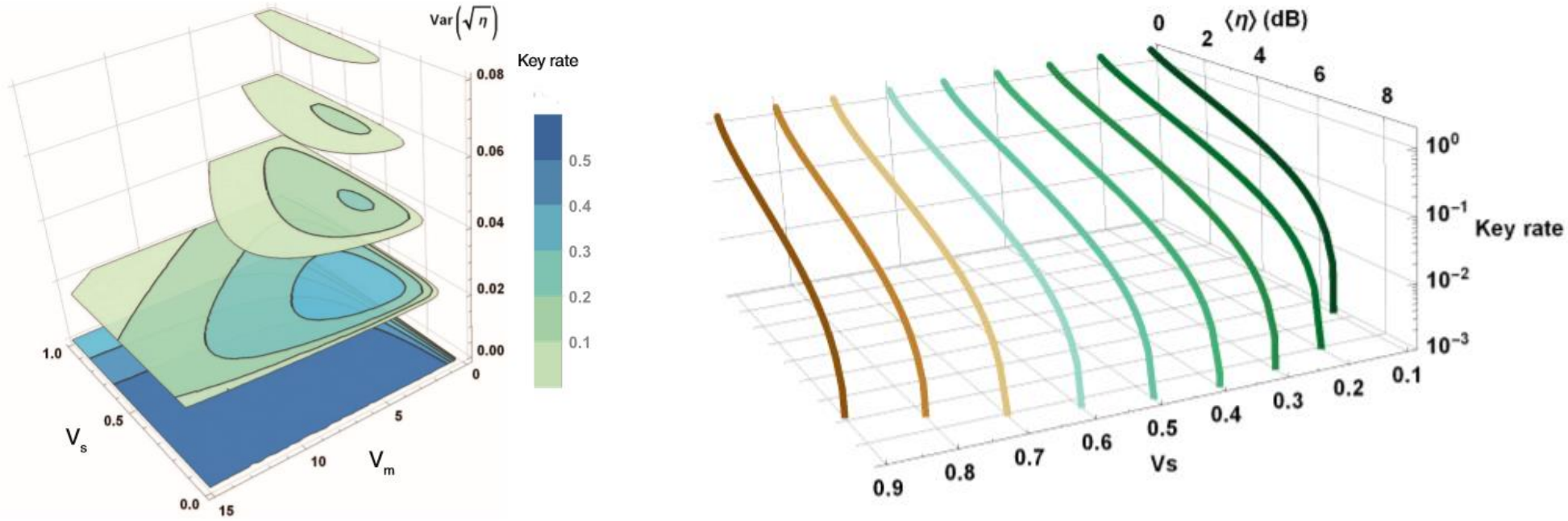
Channel post-selection can be optimized with clusterization of estimated sub-channels so that they are optimally combined and all the data is used for the key:



Key rate secure against collective attacks versus number of clusters in the typical coherent-state CV QKD settings for different transmittance distributions: Gaussian (circles), uniform (triangles), Weibull with strong fluctuations (diamonds) and Weibull with less fluctuations (squares).

6. SQUEEZED-STATE FREE-SPACE CV QKD

Free-space CV QKD can be enhanced using squeezed states:

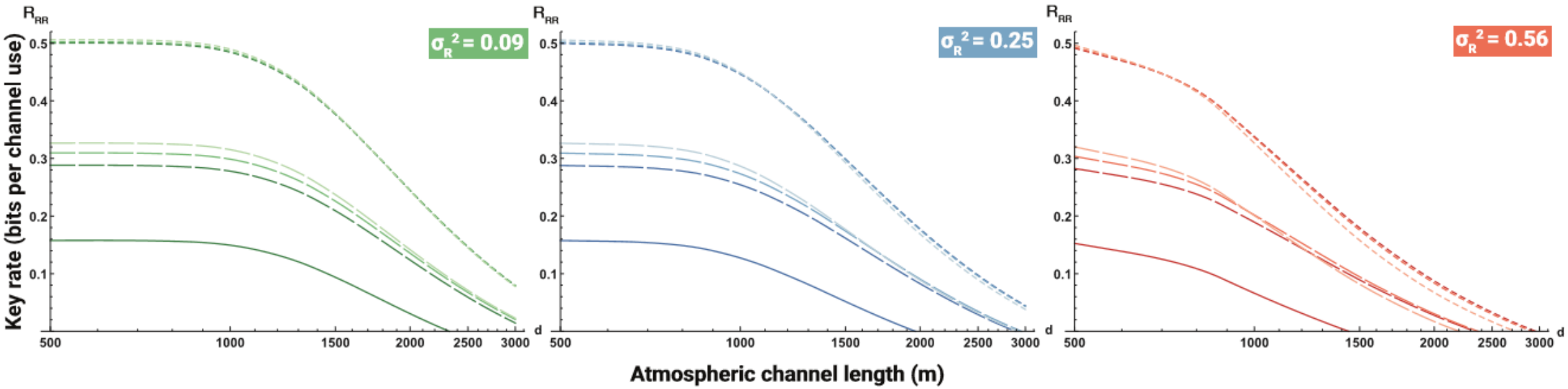


Key rate secure against collective attacks versus modulation variance and level of signal squeezing (left) and versus mean transmittance and level of squeezing (right).

Evidently, squeezing and modulation must be optimized to provide the best results in a given channel.

7. SQUEEZED-STATE FREE-SPACE CV QKD

Analysis shows the advantage of squeezing in the realistic free-space channels [5]:



Key rate versus distance in a realistic free-space channel upon different values of Rytov parameter σ_R and with optimized modulation and squeezing (up to -3 dB, long dash lines and up to -10 dB, short dash lines), compared to performance of coherent-state protocol (solid lines), taking into account finite-size effects with 10^6 data points.

SUMMARY

Transmittance fluctuations in free-space atmospheric channels can undermine the security of CV QKD protocols. For the coherent-state protocol, channel post-selection can be used and optimized by combining estimated sub-channels into clusters, contributing to the final key rate. Furthermore, squeezing of the signal states can improve robustness of CV QKD to fading and increase the secure distance in the atmospheric channels, but should be optimized along with the modulation variance.

REFERENCES

[1] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001); F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[2] D. Yu. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **108**, 220501 (2012).
[3] R. Dong et al., Phys. Rev. A **82**, 012312 (2010).
[4] V. C. Usenko et al., New J. Phys. **14**, 093048 (2012).
[5] M. Grabner, and V. Kvicera, Radioengineering **21**, 455 (2012).

Acknowledgements

Project LTC17086 of the INTER-EXCELLENCE program of the Czech Ministry of Education and project PrF-2018010 of Internal Grant Agency at Palacky University.