ANALYSIS AND COMPENSATION OF SIDE CHANNELS IN CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

Vladyslav C. Usenko

Palacký University
Olomouc

Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic

BQIT:19, Bristol

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].

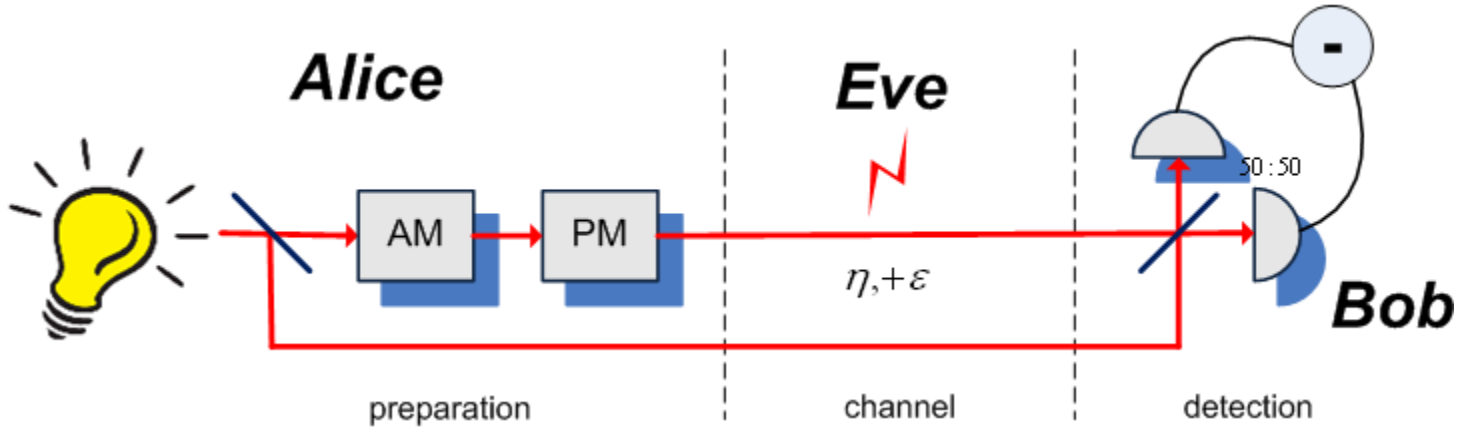

Fig. 1. CV QKD scheme based on amplitude and phase quadrature modulation and homodyne detection.

CV QKD protocols are well studied in attenuating and noisy **untrusted** channels, taking into account finite size effects and assuming collective/general attacks [2]. Moreover, part of noise and losses can be **trusted**, i.e. uncontrolled by an eavesdropper [3]. However, practical realizations of CV QKD are concerned with **side channels**, being under **partial control** of an eavesdropper. We consider side-channel loss and noise in various parts of CV QKD protocols and suggest methods aimed at compensation of side channels [4,5].

2. SIDE-CHANNEL SENDER-SIDE LEAKAGE

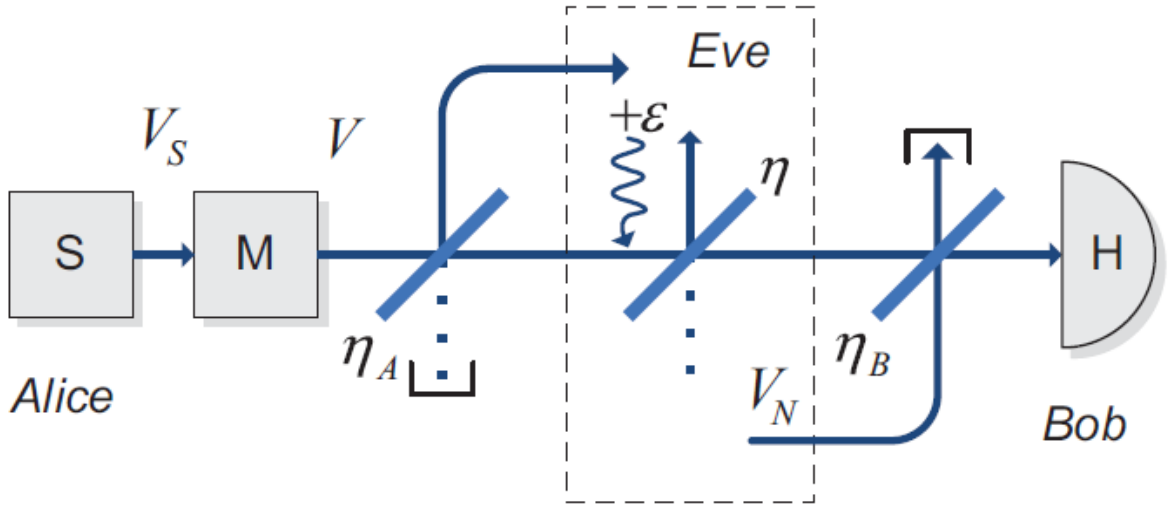

Fig. 2. Side-channel leakage on the sender side η_A and side-channel noise infusion on the receiver side η_B modeled as linear coupling to vacuum/thermal noise and contributing to/controlled by an eavesdropper Eve.

We analyze security as the positivity of the lower bound on secure key rate $K_{DR/RR} = \beta I_{AB} - \chi_{AE/BE}$, β is the post-processing efficiency, I_{AB} is the 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.

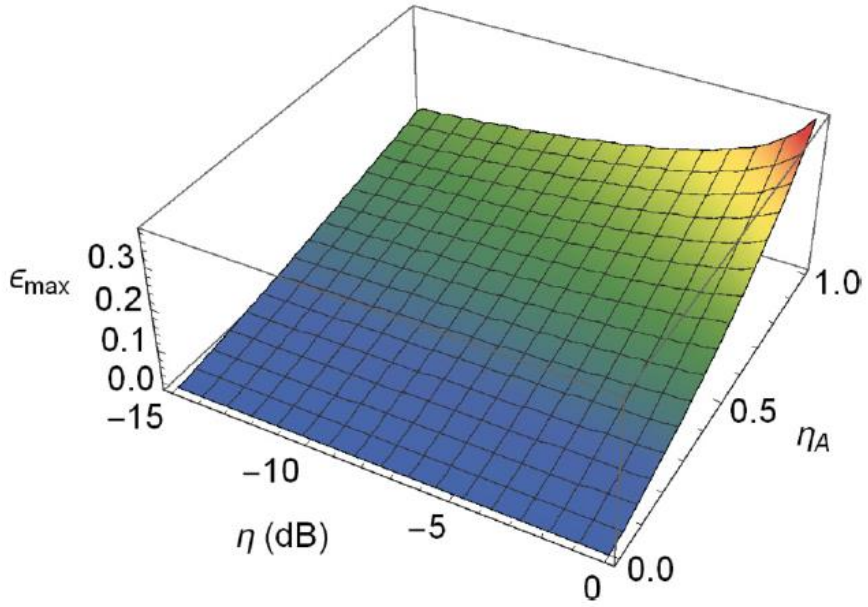

Fig. 3. Maximum tolerable channel noise versus channel attenuation and side-channel leakage for coherent-state CV QKD.

In the presence of side-channel leakage the maximum tolerable channel noise is $\varepsilon_{max} = \eta_A/2$ for coherent-state protocol with high modulation $V \to \infty$ and high channel loss $\eta \to 0$.

3. SIDE-CHANNEL DETECTION-SIDE NOISE

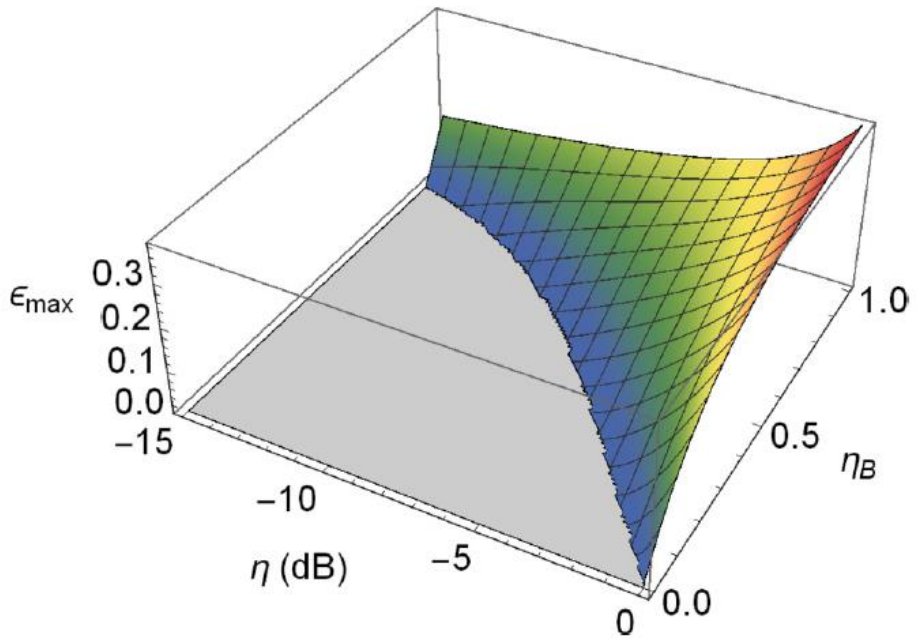

Fig. 4. Maximum tolerable channel noise versus channel attenuation and side-channel noise infusion with $V_N = 1.05$ for coherent-state CV QKD.

Maximum tolerable side-channel noise on detection side for coherent-state protocol with strong modulation and low channel transmittance $V_N^{max} = 1/(1-\eta_B)$.

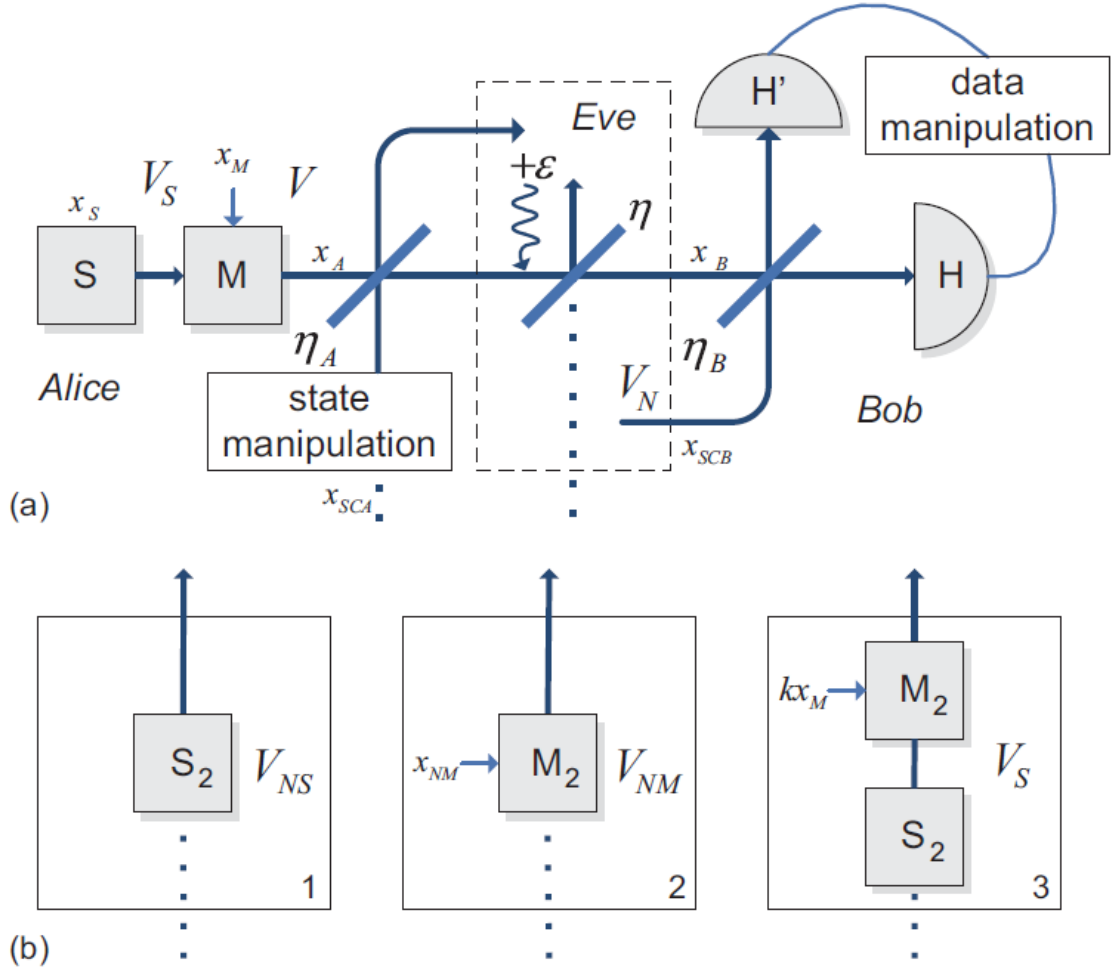

Fig. 5. a) Methods aimed at side channels compensation. b) Types of manipulation on sender-side leakage input (noise, uncorrelated/correlated modulation). Squeezer S_2 in b,3) is optional for squeezed-state protocols.

4. COMPENSATION OF SIDE CHANNELS

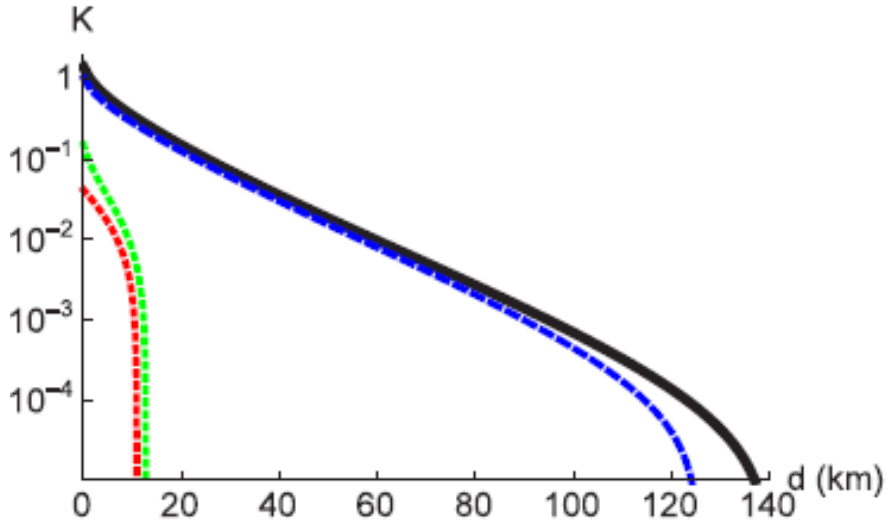

Fig. 5. Key rate versus channel distance for coherent-state protocol upon side-channel leakage with $\eta_A = 0.4$ *and no compensation (red), optimized uncontrolled noise on the leakage input (green), optimized uncorrelated modulation on the leakage input (blue) and optimized correlated modulation on the leakage input, which coincides with the case of side channel absence (black)*

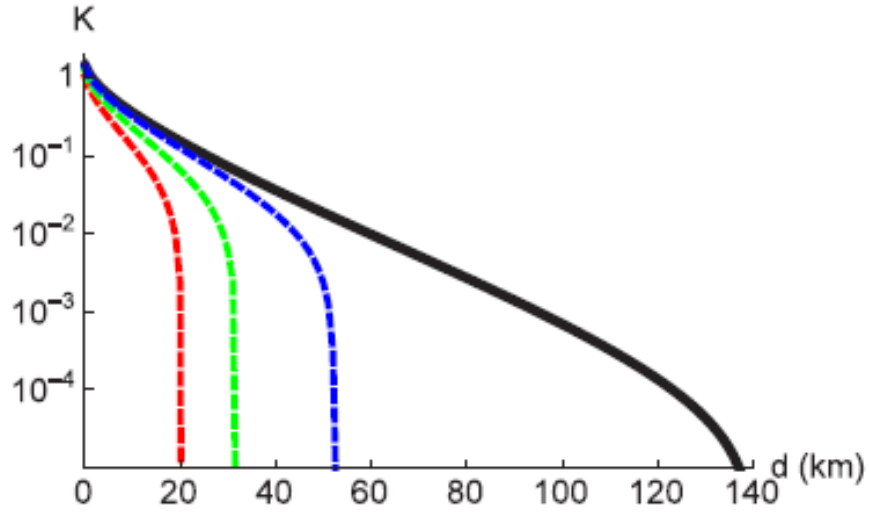

Fig. 6. Key rate versus channel distance for coherent-state protocol upon side-channel noise infusion with $\eta_B = 0.5, 0.7, 0.9$ *(from left to right) with no side-channel monitoring (dashed lines) and with optimized monitoring (coincides with black solid line for absence of side channel).*

5. MULTIMODE MODULATION

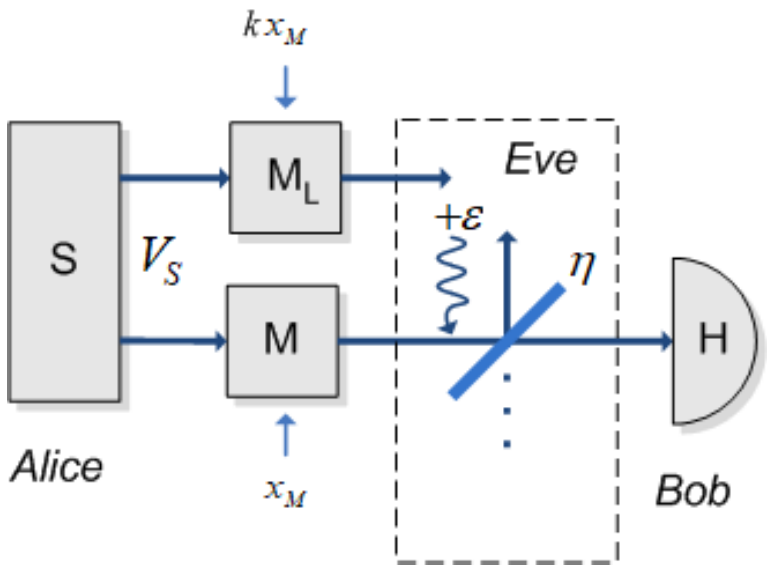

Fig. 6. Multimode modulation leakage in CV QKD.

Maximum tolerable amount of excess modulation is

$$k_{\max|V_M\to\infty} = \sqrt{\frac{V_S(\eta-2+V_S-\eta V_S)}{(\eta-1)(V_S-1)^2}},$$

where V_S is signal variance. Optimal amount of squeezing is given by

$$V_{S|V_M\to\infty}^{(opt)} = \sqrt{\frac{k^2}{1-k^2}}.$$

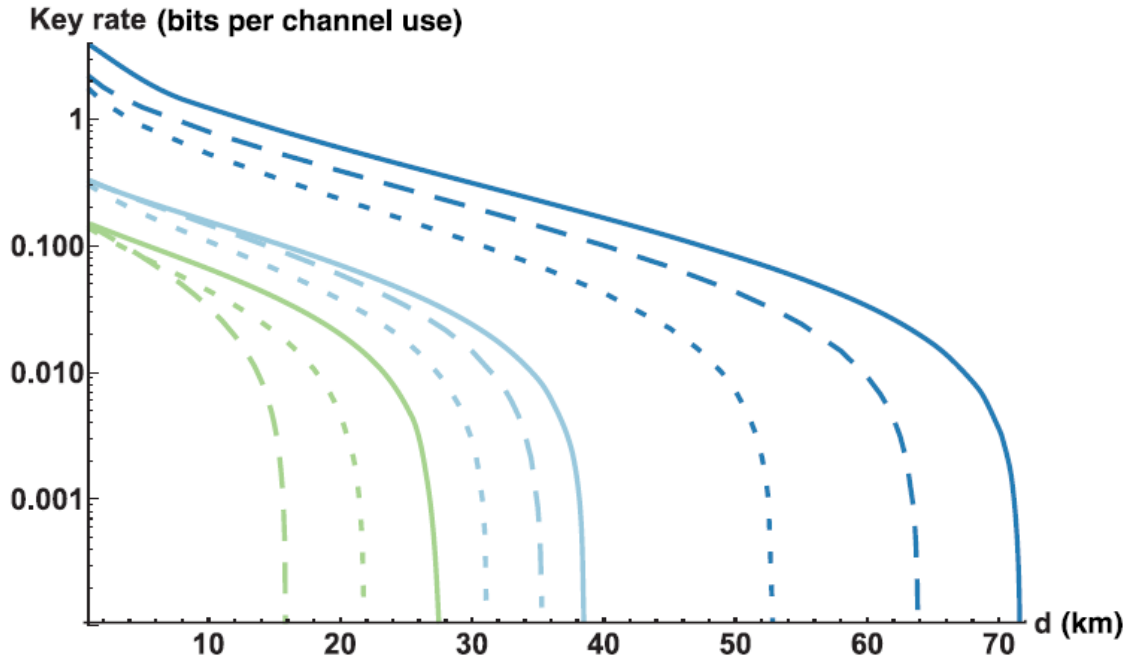

Fig. 7. Key rate versus channel distance in the presence of excess modulation with k=0,1,1.5 (blue, light blue, green lines) for optimized squeezing (solid), fixed -3dB squeezing (dashed) and coherent states (dotted).

6. PRE-MODULATION LEAKAGE

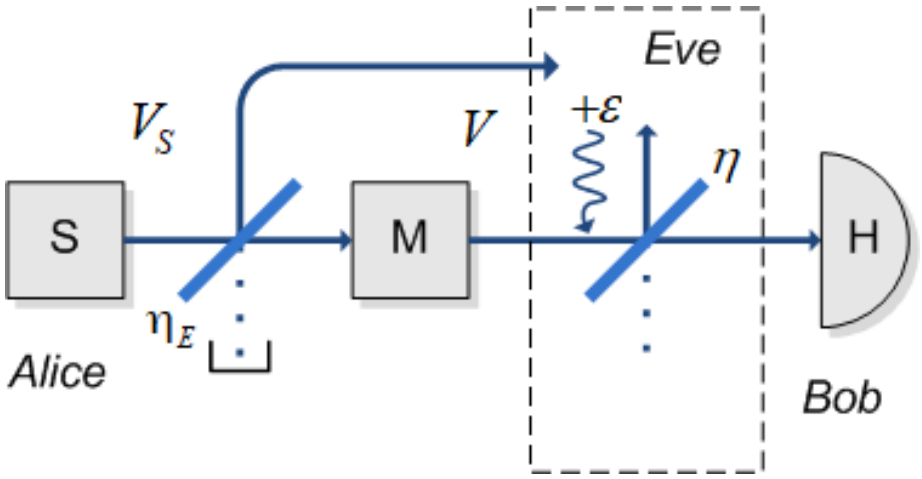

Fig. 8. Pre-modulation leakage η_E in CV QKD.

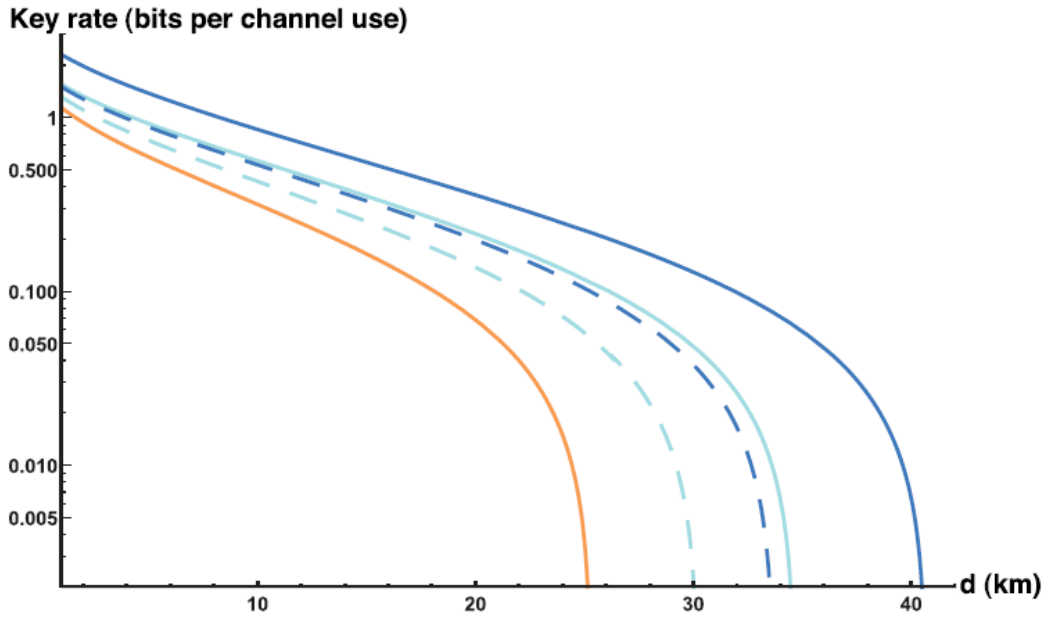

Fig. 9. Key rate versus channel distance for coherent-state protocol (orange) and squeezed-state protocol with -10 dB of squeezing (dark blue) and -3 dB of squeezing (light blue). Pre-modulation coupling is $\eta_E = 1$ (absence of side channel, solid) and $\eta_E = 0.5$ (dashed, coincides with the solid line for coherent-state protocol).

SUMMARY

Signal leakage on sender side based on linear loss can reduce robustness of the protocols, but can be optimally compensated by correlated modulation on the input. Noise infusion on receiver side undermines the security, but can be compensated by optimal monitoring of residual noise. Excessive multimode modulation and leakage prior to modulation undermine the security and may require optimization of signal squeezing. Coherent-state protocol is immune to leakage of the signal.

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] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
[3] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).
[4] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **93**, 032309 (2016).
[5] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **96**, 062309 (2017).

Acknowledgements

EU Horizon 2020 research and innovation programme grant agreement No. 820466 "CiViQ“, project P205/12/0694 of the Czech Science Foundation, project LTC17086 of the Czech Ministry of Education.