PREVENTING SIDE-CHANNEL LEAKAGE IN CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

Ivan Derkach, Vladyslav Usenko, Radim Filip

Department of Optics, Faculty of Science, Palacký University, 17. Listopadu 12, 77900 Olomouc, Czech republic

ABSTRACT

The role of the side-channel leakage in continuous-variable quantum key distribution [1,2] is studied. It is shown that the information leakage from the trusted sender station increases the vulnerability of the protocols to the eavesdropping in the main quantum communication channel. As a method to compensate the effect noise infusion to the side-channel input, being under control of a trusted sender party, is suggested. It is shown that such noise can reduce the negative impact of a side-channel and must be optimized for a given set-up.

SIDE CHANNEL EFFECT

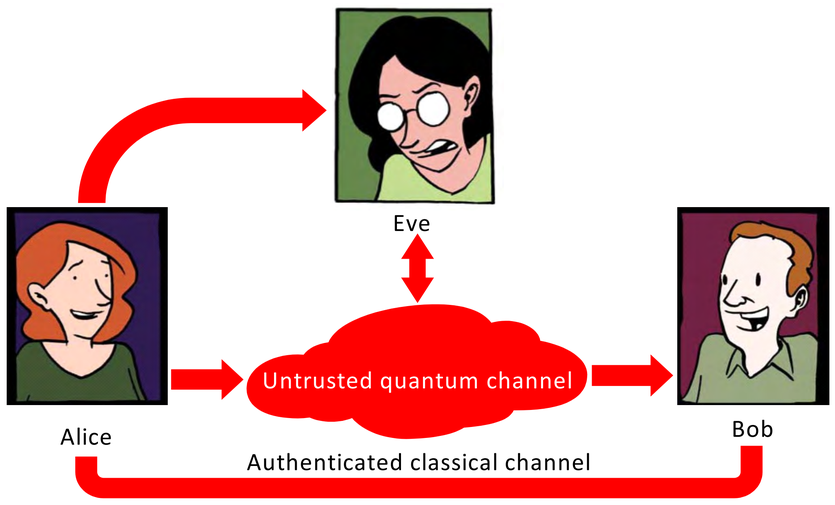

Fig. 1 QKD scheme with side channel

There are numerous potential sources of side information in the classical communication such as: timing, power monitoring, electromagnetic, acoustic etc. Some of these sources can also exist in the quantum domain especially timing or side-band attacks. We summarize all possible sources of side information and define them altogether as a side channel.

Alice on her side uses light **source** to prepare a state, encodes information into it using modulator **M** and sends the state to Bob through quantum channel where it suffers from excess noise and channel losses. Information leakage on Alice's side due to the presence of side channel is modeled by loss caused by additional beamsplitter with transmittivity **S**.
Alice can also use modulator $\mathbf{M_s}$ to control the input of side channel.

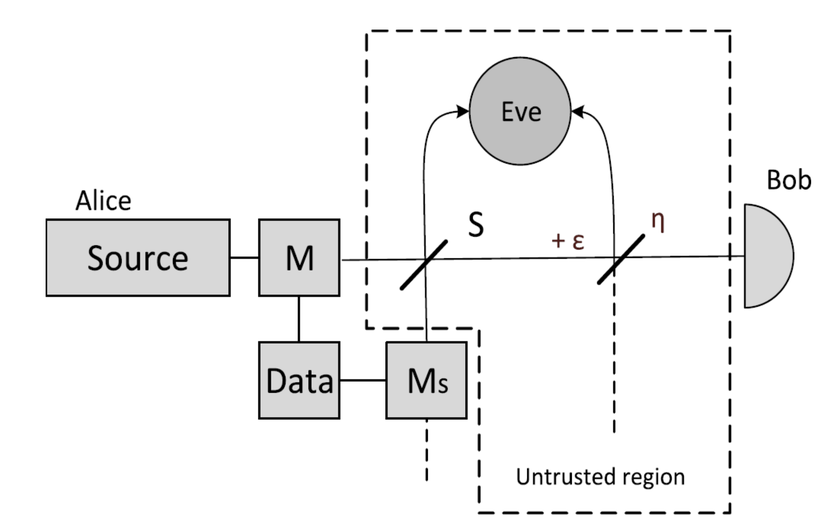

Fig. 2 Continuous-variable Quantum Key Distribution prepare-and-measure setup including side channel with trusted controlled input.

Initially we investigate the influence of side channel for the case of individual attacks with pure losses (ε= 0) to estimate security region. In this case the input of side channel is vacuum i.e. eavesdropper has no control on side channel input, but receives its output similarly to non-invasive passive attacks in classical cryptography.
In the limit of infinite squeezing and modulation (V→∞) key rates for the squeezed and coherent state protocols can be respectively written as:

$$K^{c}_{V\to\infty} = \frac{1}{2}\log_2\left(\frac{1}{1-\eta S}\right) \qquad K^{s}_{V\to\infty} = \log_2\left(\frac{1}{1-\eta S}\right)$$

Side channel decreases mutual information between trusted parties and increases Eve's information,therefore limiting the key rate already for individual attacks with pure losses.
The effect of side channel leakage in case of collective attacks taking into account excess noise presence as well as generalized efficiency of post-processing algorithms is similar to previous case, side channel leads to the degradation of the key rate and also to increases vulnerability of the protocol to the excess noise.

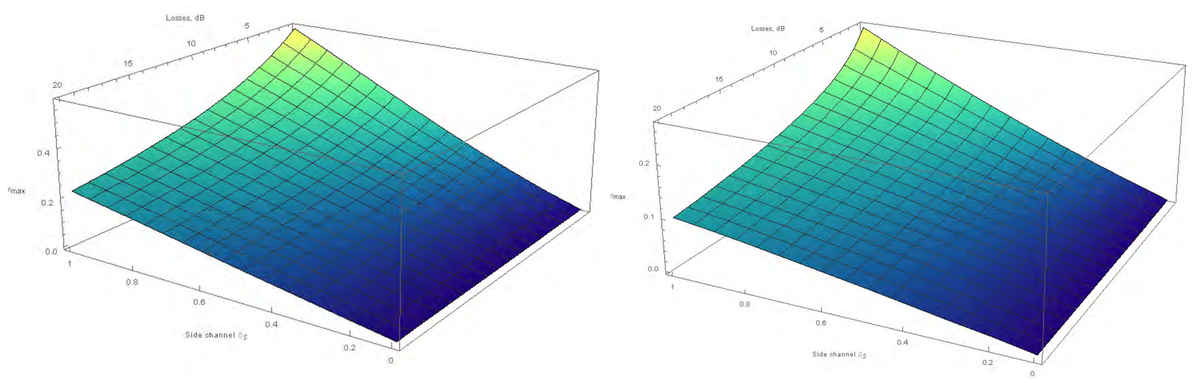

Fig. 3 Maximal tolerable excess noise on channel losses and side channel coupling ratio for squeezed (left) and coherent (right) state protocols.

METHODS

- Covariance matrix formalism [1,3,4]
- Shannon information and Holevo bound [2]

$$K_{Ind.} = I_{AB} - I_{BE(AE)}$$
$$K_{Col.} = I_{AB} - \chi_{BE(AE)}$$

K – key rate,
I – mutual information,
χ – Holevo bound,

$$\chi_{BE} = S_E - S_{E|B}$$
$$S = \sum G\left(\frac{\lambda - 1}{2}\right)$$

S – Von Neuman entropy,
G(x) – bosonic entropy function,
λ – symplectic eigenvalues respective covariance matrix

SIDE CHANNEL DECOUPLING

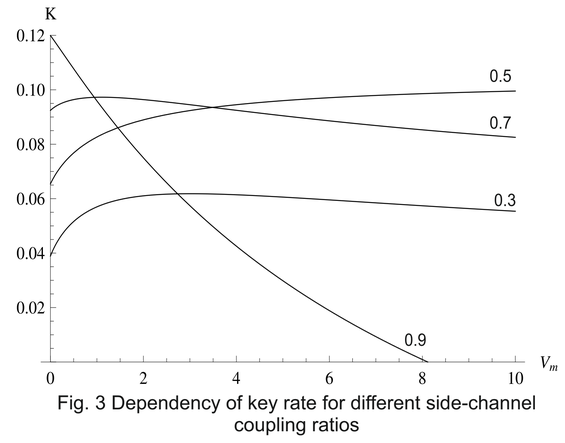

Fig. 3 Dependency of key rate for different side-channel coupling ratios

We consider additional modulation applied to the input of side channel by trusted party. This additional modulation can play positive or negative role depending on the region of side channel coupling ratio.
For S< 0.8 a range of additional modulation values Vm that effectively increase the key rate comparing to the vacuum input of side channel can be found.
Depicted on Fig. 3 is the key rate for collective attacks on additional modulation on the input of side channel $\mathbf{V_M}$ for different side-channel coupling ratios. Evidently addition of noise for the case of minor side channel presence is harmful, however for S<0.8 noise addition positively affects key rate and optimal modulation value can be found.

By applying modulation optimized over all parameters of the protocol maximal key distribution distance can be increased as well as the tolerance to noise in the channel.

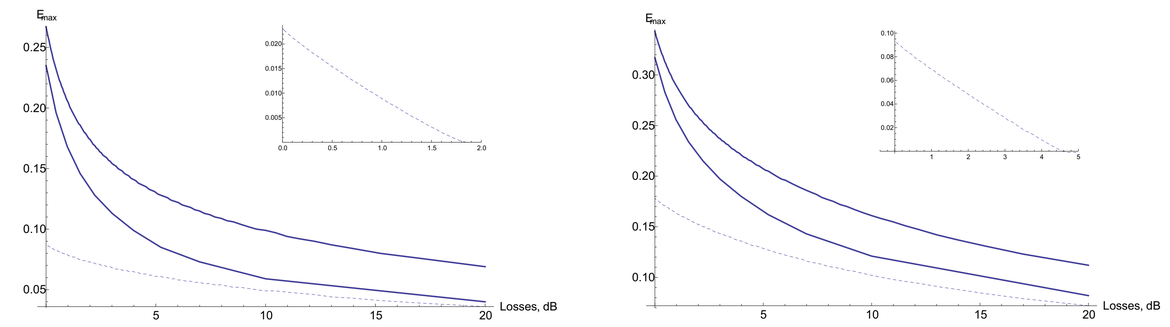

Fig. 4 Maximal tolerable excess noise for sqeezed (right) and coherent (left) state protocols.

Comparison of maximal tolerable excess noise dependency on channel losses for squeezed (right) and coherent (left) state protocols with optimal source variance V and additional modulation V_M for collective attacks: β= 100% (upper thick line), β= 95% (lower thick line) and protocols without additional modulation: β= 100% (dashed line), β= 95% (upper right plot). Channel losses correspond to optical fiber with -0.2 dB per km. S= 0.3.

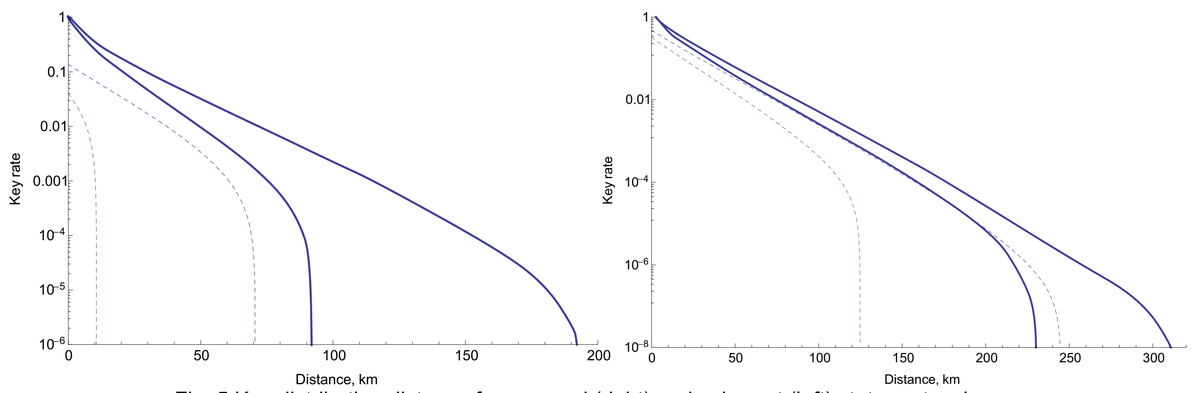

Fig. 5 Key distribution distance for sqeezed (right) and coherent (left) state protocols.

Comparison of key distribution distance for squeezed (right) and coherent (left) state protocols with optimal source variance V and additional side-channel modulation V_M for collective attacks: β= 100% (upper thick line), β= 95% (lower thick line) and protocols without optimal additional modulation: β= 100% (upper dashed line), β= 95% (lower dashed line). Channel losses correspond to optical fiber with -0.2 dB per km. S = 0.4, ε= 5%.

CONCLUSIONS

We have studied the effect of side-channel leakage on the trusted sender side on the continuous-variable quantum key distribution protocols. The negative effect of side-channel leakage leads to the degradation of key rate and to increased sensitivity of the protocol to the channel noise. We suggested and examined the method of additional modulation applied to the side-channel input being under the control of a trusted sending party. We show the positive effect from such additional modulation and the possibility to optimize the method for the given conditions of the protocol. Our result describes the promising method of shielding the quantum side-channels in continuous-variable quantum key distribution.

References

[1] Navascués et al., Phys. Rev. Lett. 97, 190502 (2006)
[2] Grosshans et al, Nature 421, 238-241 (2003)
[3] Wolf et al., Phys. Rev. Lett. 96, 080502 (2006)
[4] García-Patrón,Ph.D. thesis, UL Brussels (2007)

Acknowledgments

The research leading these results has received funding from the EU FP7 under Grant Agreement No. 308803 (project BRISQ2). I.D. acknowledges Palacky University project IGA PrF 2014008, I.D. and V.C.U. acknowledges the project 13-27533J of GACR.