Side channel loss 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

We address security [1] of continuous-variable [2] quantum key distribution scheme based on Gaussian modulation of coherent states [3] with side channel and investigate how it is robust against excess noise and channel losses. While the presence of side channel does not destroy the security of protocol, it limits the robustness of protocol to noise in the quantum channel. We consider method of compensating the negative influence of side channel by adding known input noise. We show that an optimal value of noise that maximally compensate side channel influence for given setup parameters can be found.

Side channel

Timing information, power consumption, electromagnetic fields, dissipating heat or even sound can provide an extra source of information that can be exploited to break the system. All information leakage from trusted party side can be considered a side channel influence.

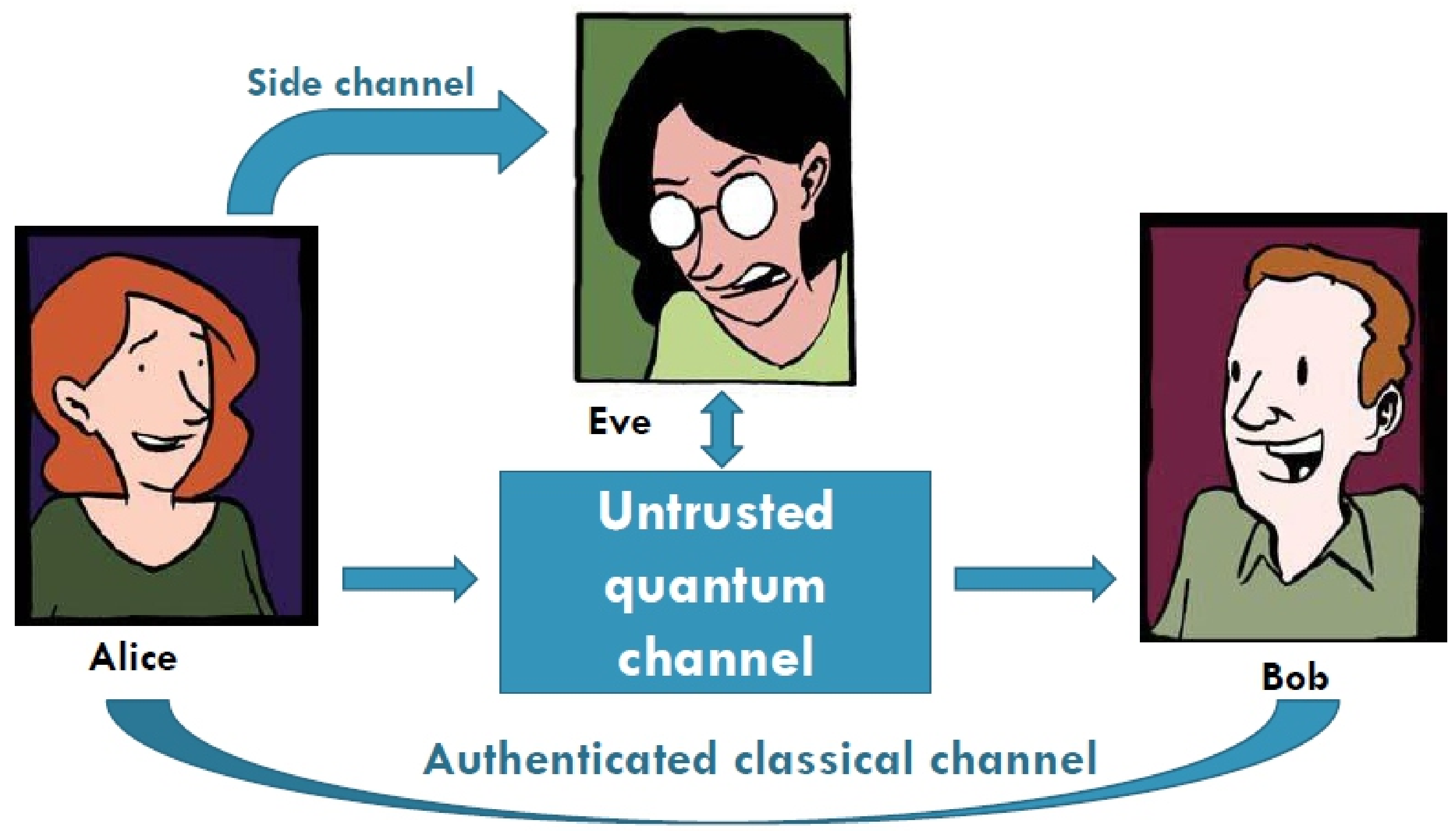


Fig.1Side channel in general QKD scheme

Side channel with vacuum input

We model side-channel loss by an additional beamsplitter on the Alice's side such that it's output is available to Eve.

The input of a side-channel is a vacuum state coupled to a signal with ratio S and is not by any means controlled by Eve.

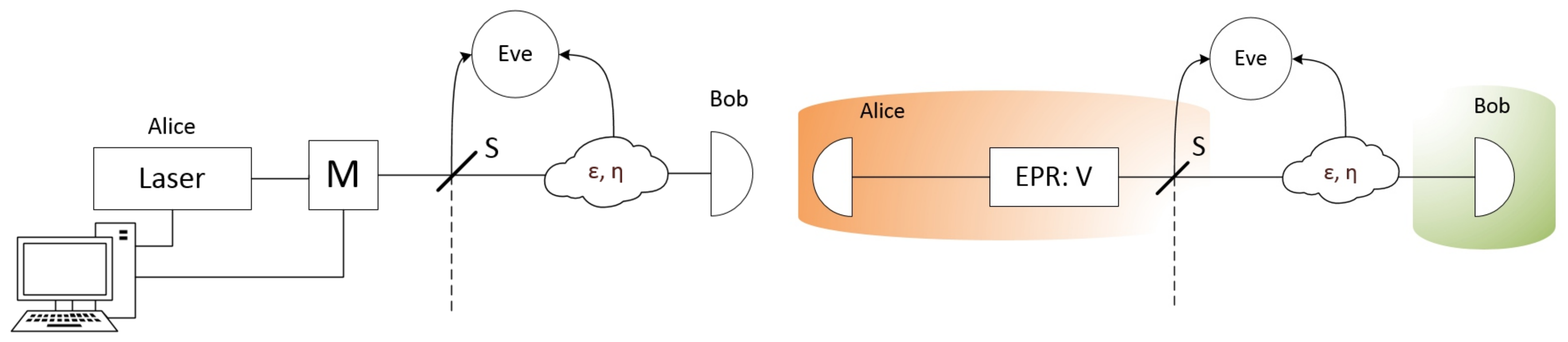
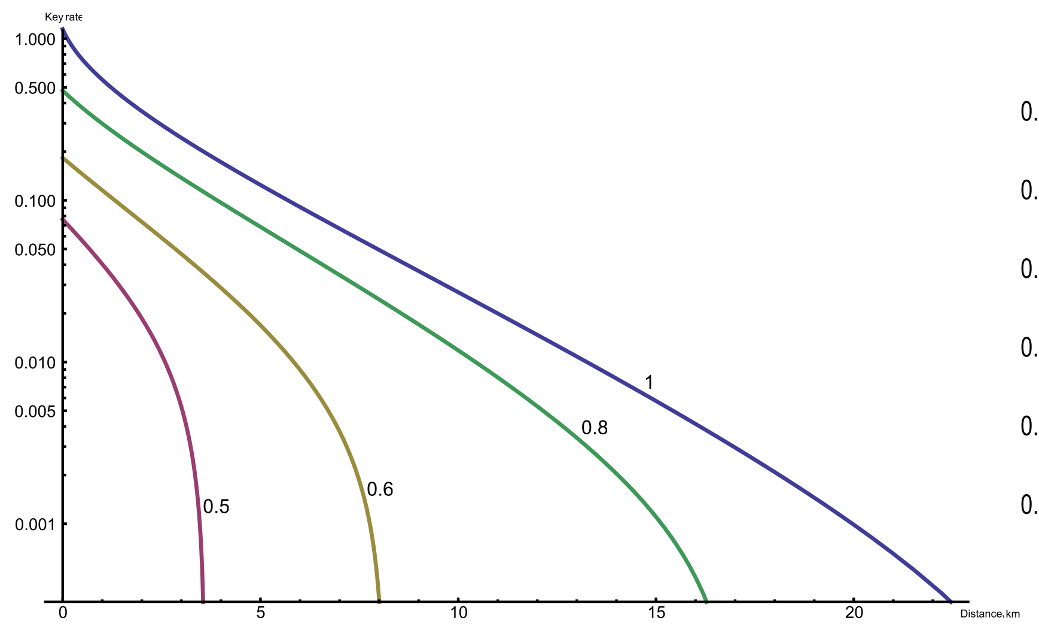
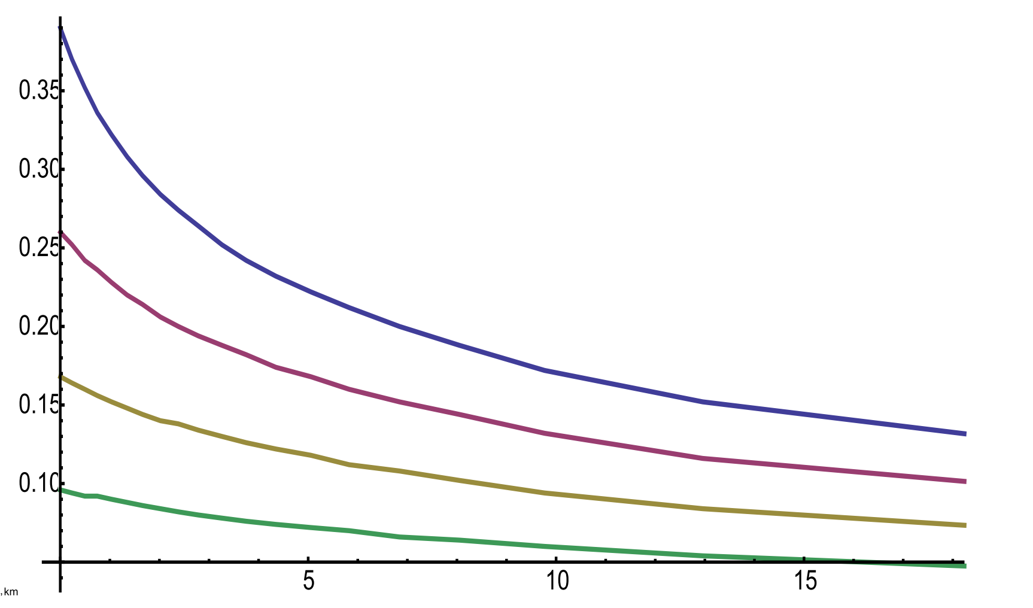


Fig.2 Prepare & Measure (left) and EPR (right) schemes with side channel vacuum input



Side channel limits the secure distance of the protocol, therefore side channel makes protocol less robust to noise influence.

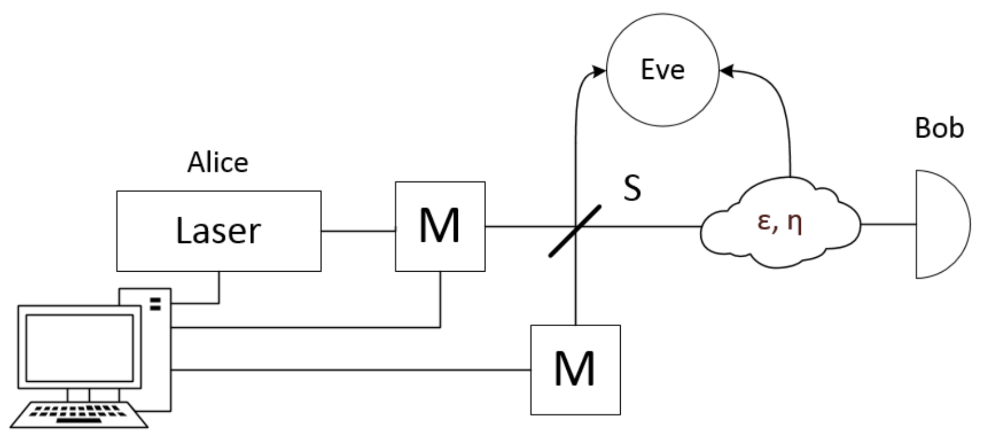


When side channel coupling ratio to signal is small more information flows into side channel, tolerance to channel excess noise decreases and eventually reaches zero therefore protocol is no longer secure for any values of excess noise.

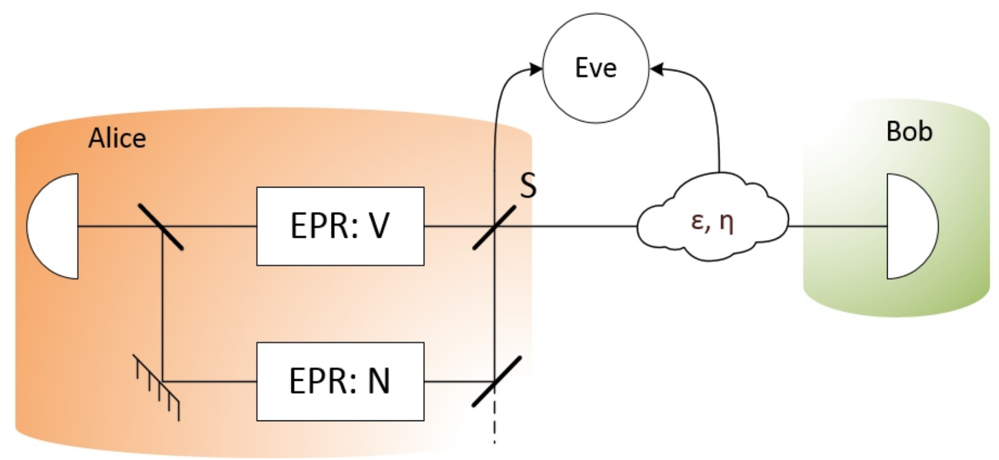
References

[1] Navascués et al., Phys. Rev. Lett. 97, 190502 (2006)
[2] Weedbrook et al., Rev. Mod. Phys. 84, 621 (2012)
[3] Grosshans et al, Nature 421, 238-241 (2003)
[4] Wolf et al., Phys. Rev. Lett. 96, 080502 (2006)
[5] García-Patrón,Ph.D. thesis, UL Brussels (2007)

Side channel decoupling

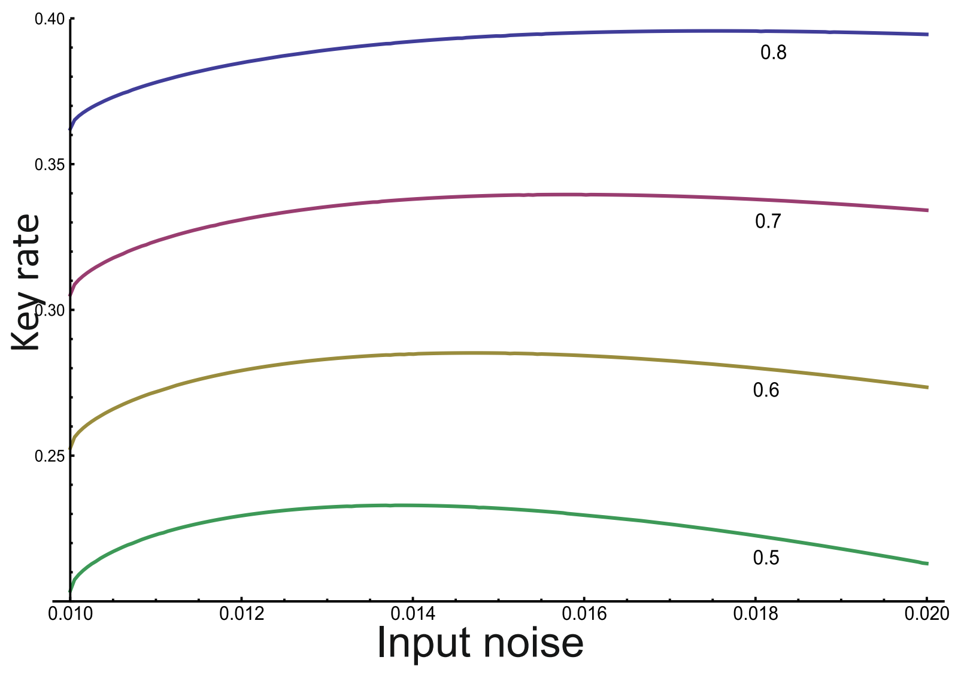


Let's assume that side-channel input can be controlled by Alice. In case of Prepare & Measure scheme, Alice can use an additional modulator to input a known value of noise into the side channel. Since Alice knows what noise she inputs into side channel, later she can use this information to decrease Eve knowledge about the transmitted key.

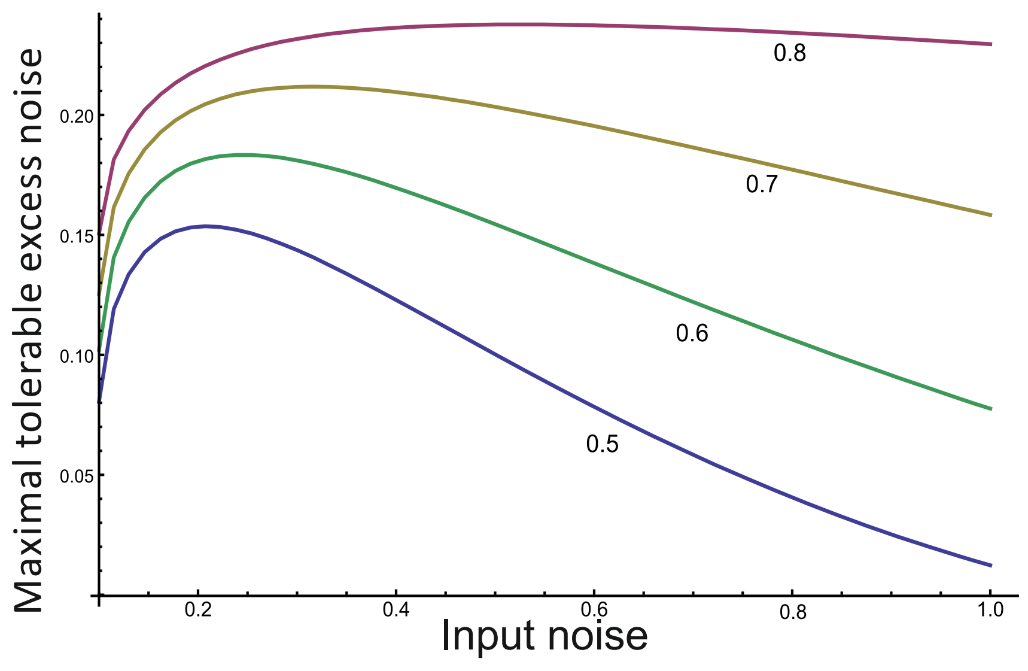


Equivalent EPR scheme includes additional EPR source under Alice's control in order to purify the side-channel input modulation.

Side-channel input noise can have positive impact on security of quantum key distribution. Turns out that for any value of excess noise and channel losses there is a corresponding optimal value of side-channel input noise that can partly compensate the effect of information leakage caused by the presence of the side channel.



Key rate depending on side-channel input noise for different side channel coupling ratios



Dependency of maximal tolerable excess noise on side-channel input noise for various coupling ratios

Conclusions

We have investigated the influence of side channel loss on the security of the quantum key distribution schemes based on Gaussian modulation of coherent states upon realistic conditions of channel loss and channel excess noise. While the presence of side channel was shown not to be destructive for the secure key transmission, side channel limits the robustness of protocol to noise in the quantum channel. We show the possibilitythe possibility to compensate the influence of side channel by inputting known and trusted noise into it and consequently finding its optimal value. Optimal input noise maximally decreases the negative effect of side channel on security of the protocol. Moreover, such noise can increase the robustness of protocol to noise in the quantum (untrusted) channel. Further noise optimization should be considered. The investigation of additional realistic conditions can result in more effective optimization and may be the subject for further research.

Methods

- Covariance matrices formalism [1,4,5]
- Shannon information and Holevo bound [2,3]

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

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

$$\chi_{BE} = S_E - S_{E|B}$$

$$S = \sum G\left(\frac{\lambda - 1}{2}\right)$$

K –	key rate,
I –	mutual information,
χ –	Holevo bound,
S –	Von Neuman entropy,
G(x) –	bosonic entropy function,
λ –	symplectic eigenvalues for respective covariance matrix

Acknowledgements:
The work was supported by Project 205/12/0694 of Czech Science Foundation and Project PrF_2012_019 of Palacky University