TOWARDS CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION IN REALISTIC CONDITIONS

Ivan Derkach, Vladyslav C. Usenko, Radim Filip

Department of Optics, Palacký University, Olomouc, Czech Republic

esf evropský sociální fond v ČR

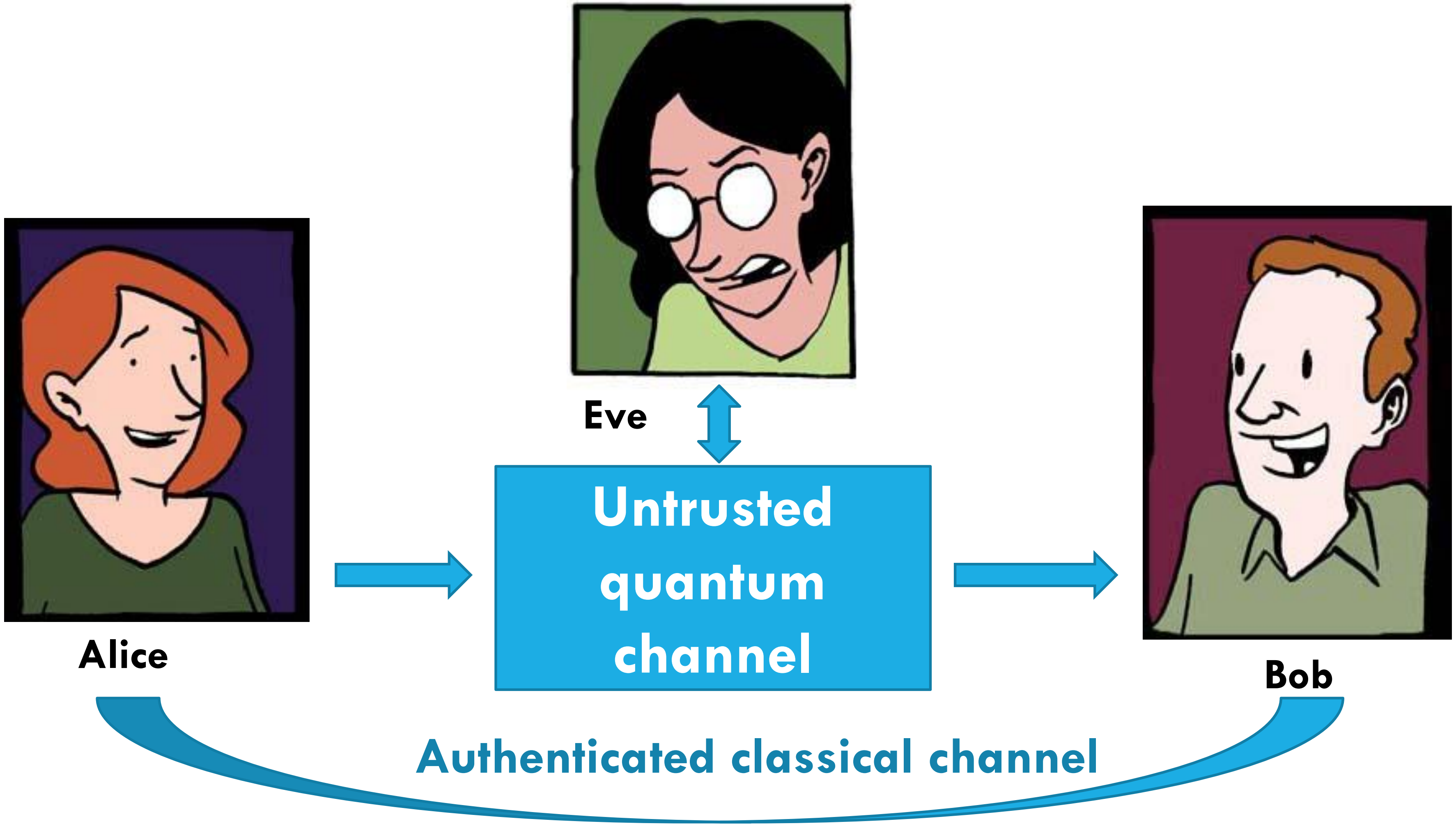
EVROPSKÁ UNIE

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

QUANTUM KEY DISTRIBUTION



Eve

Untrusted quantum channel

Alice

Bob

Authenticated classical channel

METHODS

- Covariance matrices

Weedbrook et al., Rev. Mod. Phys. 84, 621 (2012)
Wolf et al., Phys. Rev. Lett. 96, 080502 (2006)

- Shannon information and Holevo bound

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

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

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

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

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

García-Patrón and Cerf, Phys. Rev. Lett. 97, 190503 (2006)
Navascués et al., Phys. Rev. Lett. 97, 190502 (2006)

PRACTICAL ISSUES

- Losses are present in optical channel as well as at trusted sides
- Presence of excess and trusted (preparation, detection) noise
- Limited reconciliation efficiencies
- Transmittance fluctuations in atmospheric channels

Fading noise is multiplicative and quickly destroys Gaussian quantum features such as entanglement and purity.

R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. 102, 130501 (2009)

V. C. Usenko and R. Filip, Phys. Rev. A 81 022318 (2010)

Vladyslav C. Usenko, Bettina Heim, Christian Peuntinger, Christoffer Wittmann, Christoph Marquardt, Gerd Leuchs, Radim Filip, New J. Phys. 14, 093048 (2012)

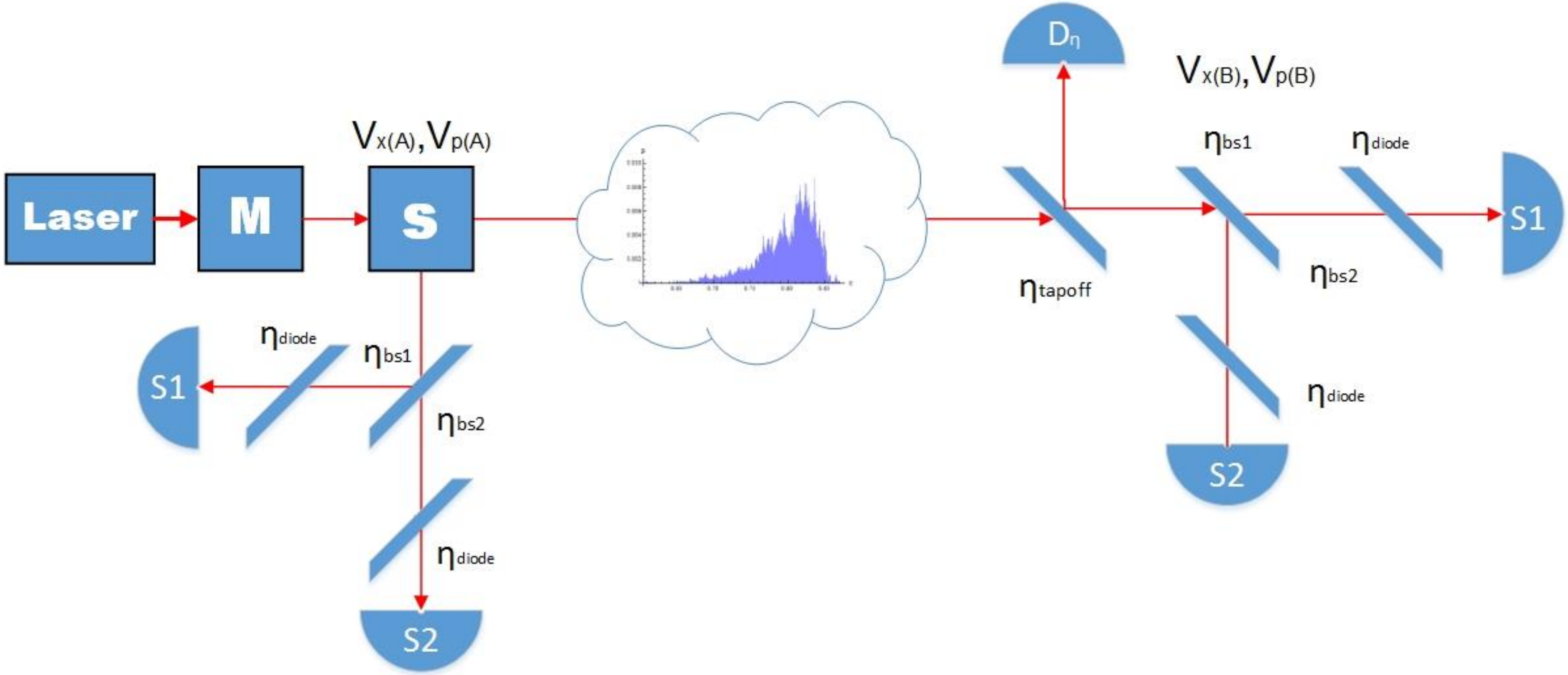
PART 1. TOWARDS CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION OVER ATMOSPHERIC CHANNELS.

Collaboration with MPI in Erlangen.

- The study of continuous-variable quantum key distribution in free-space fading channel
- Experimental data processing and state reconstruction
- Post-selection effect on excess noise and key rate

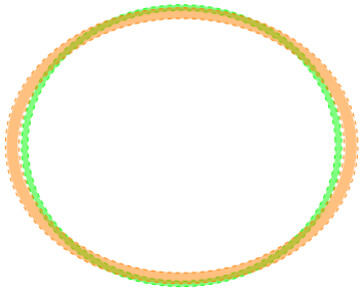
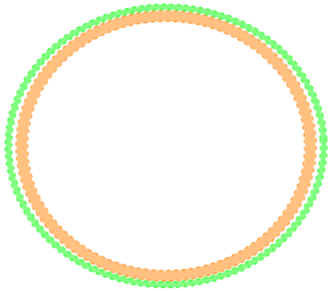
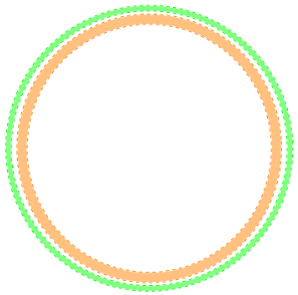
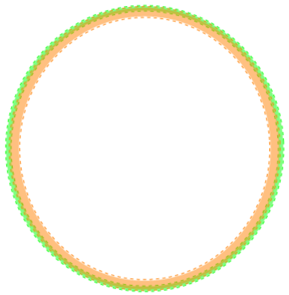
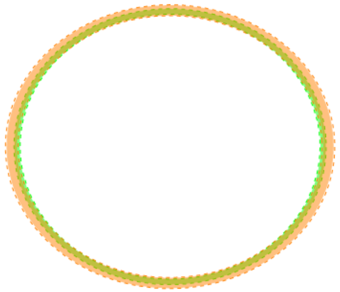
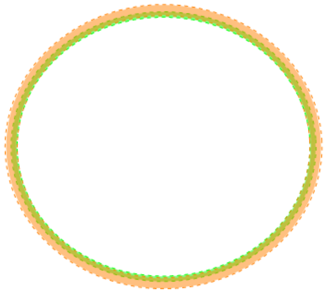
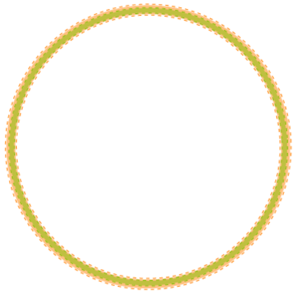
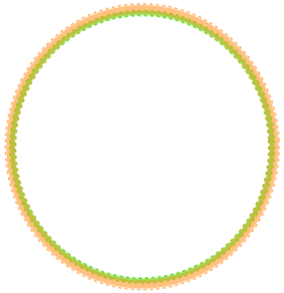
Experimental test was carried out by the group of Dr. Christoph Marquardt at Max Planck Institute for the science of light in Erlangen.

EXPERIMENTAL SCHEME



STATE RECONSTRUCTION

The detection efficiency had to be re-estimated in order to find equivalence between the prepared and the measured states. Corrections to the detection efficiencies were found.

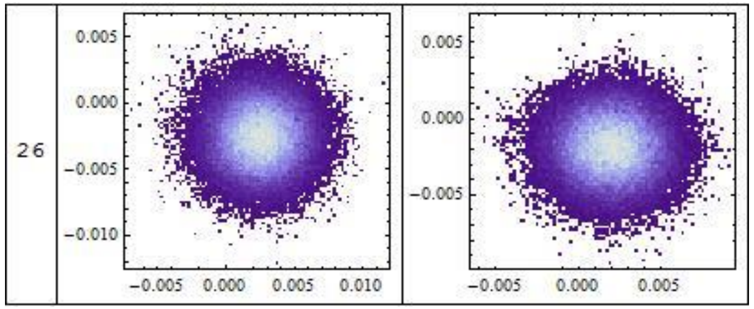
States from initial measurements				
States with corrected efficiencies				

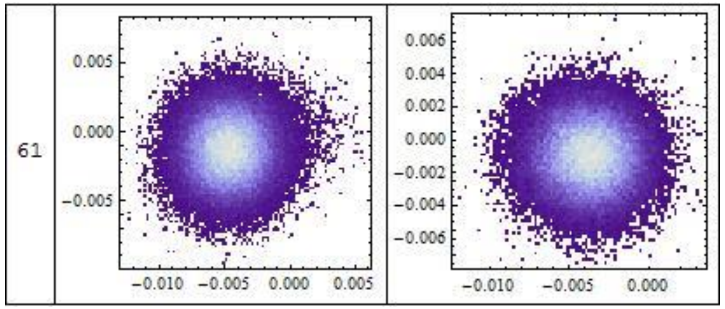
$$\frac{V_A^{S1}\text{-}1+\eta_A}{\eta_A} \approx \frac{V_B^{S1}-1+T\eta_B}{T\eta_B}$$

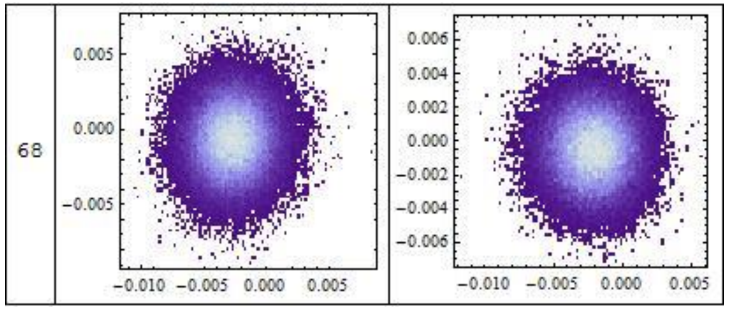
$\eta_A = \eta_{diode}\eta_{bs1},$

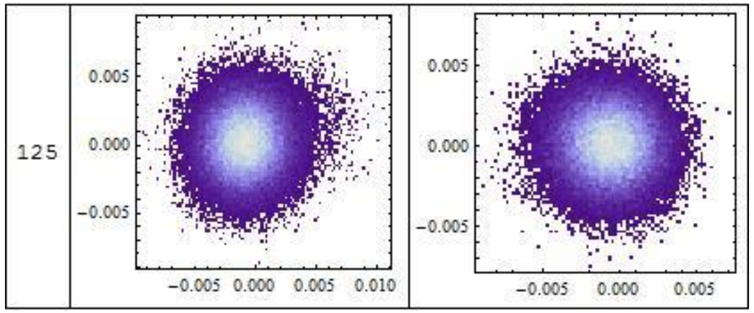
$\eta_B = \eta_{tapoff}\,\eta_{bs1}\,\eta_{diode};$

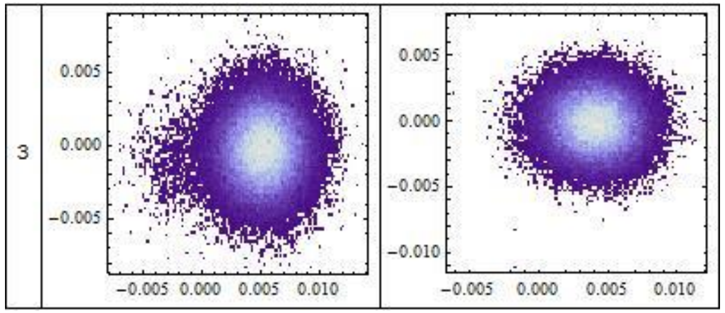
ALPHABET CHECK

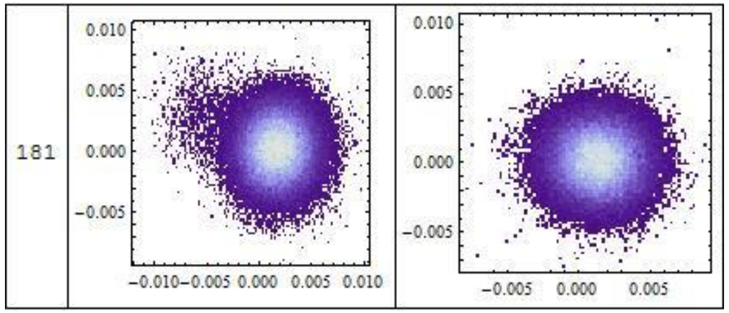


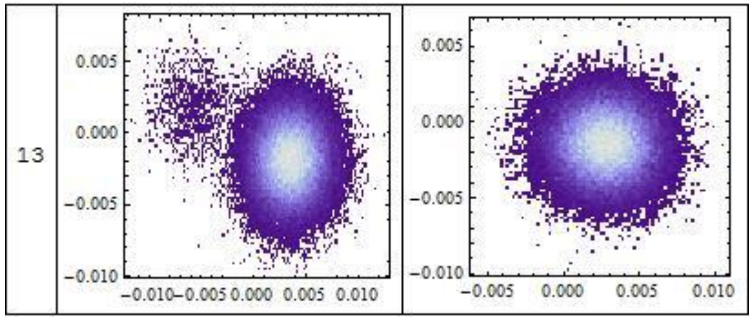


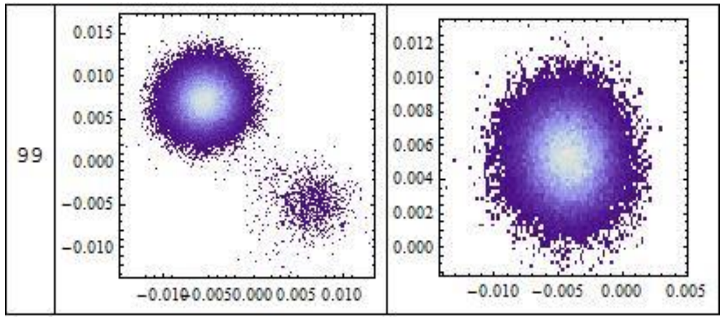


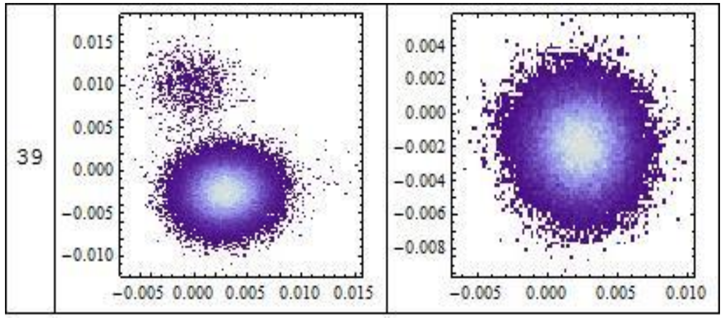




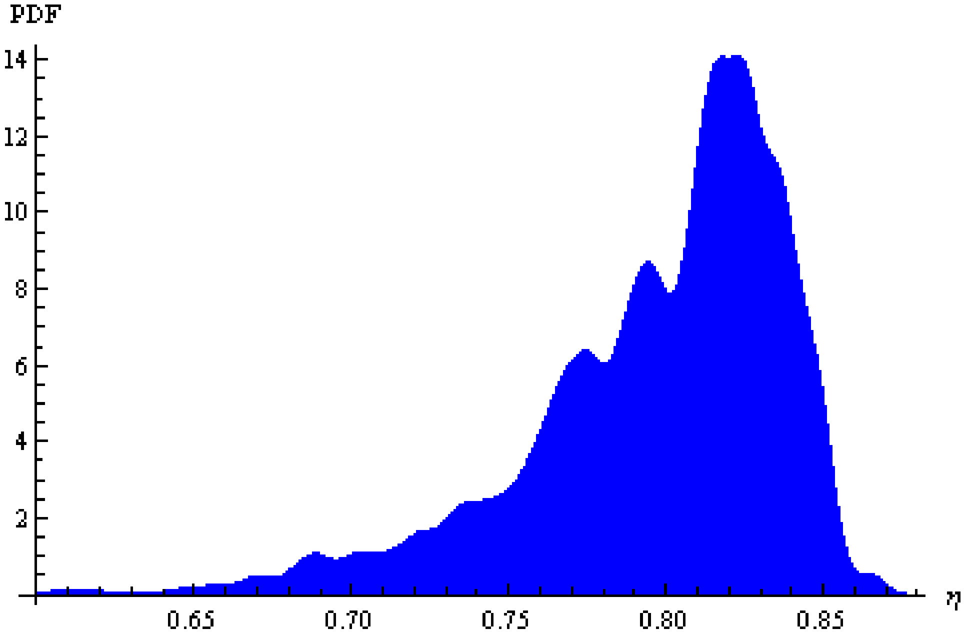


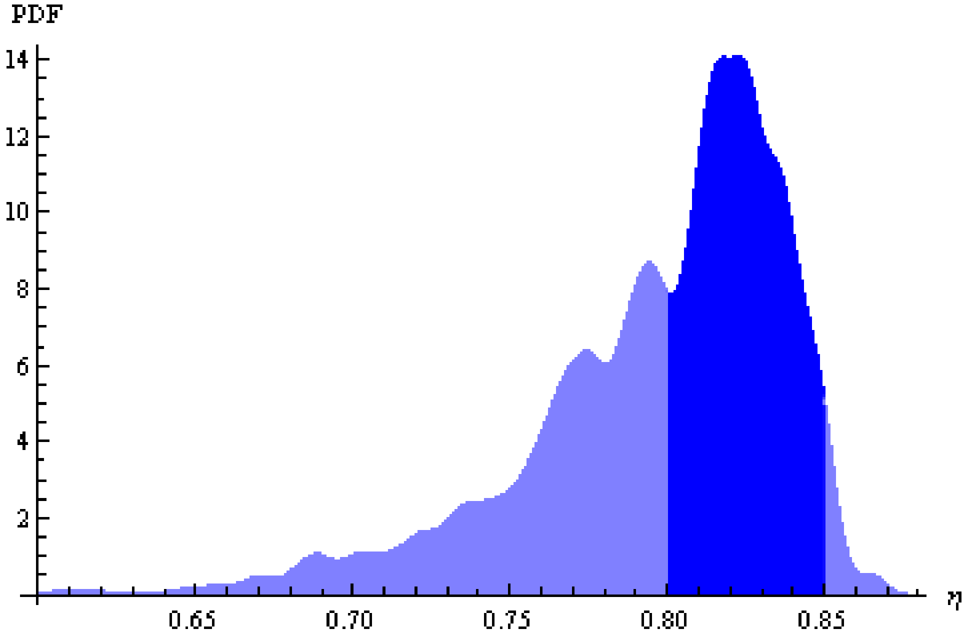






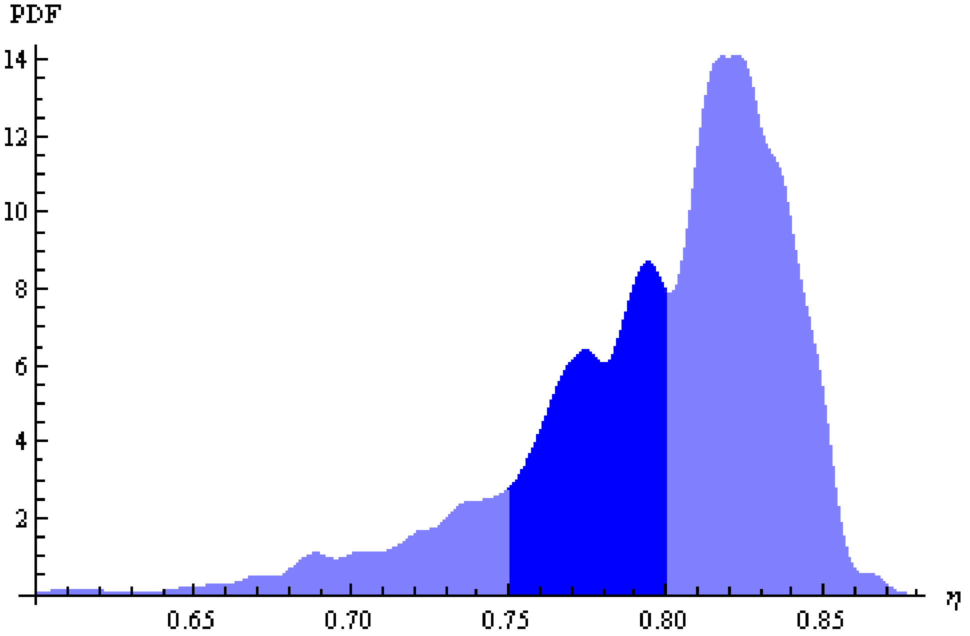
POST-SELECTION EFFECT ON NOISE

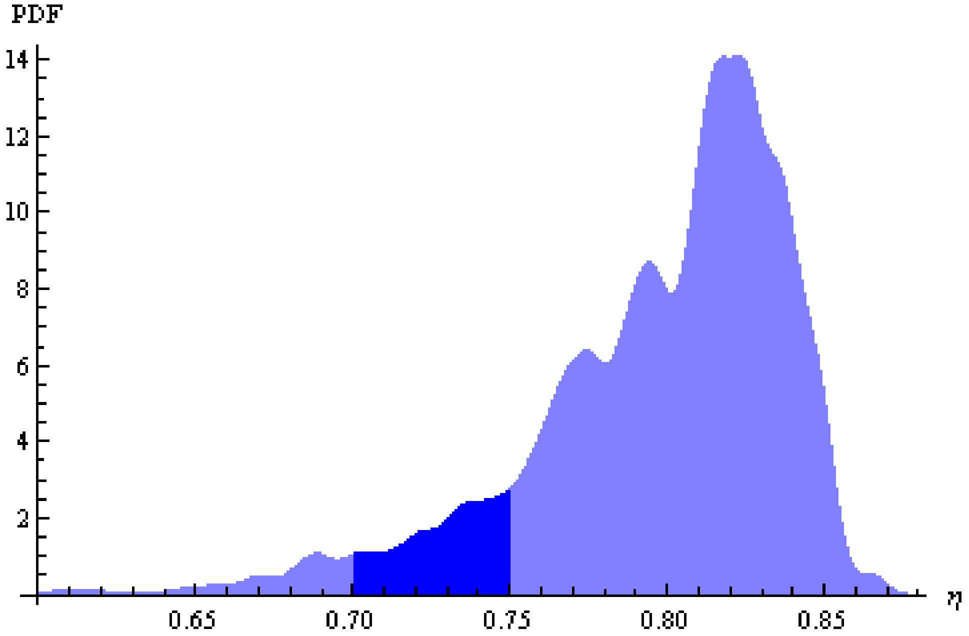




Transmittance window	**40%-90%**	**80%-85%**	75%-80%	70%-75%
Fraction of data	**100%**	**54,8%**	30,4%	8,9%
ε_x	$\mathbf{19,7 \cdot 10^{-4}}$	$\mathbf{1,79 \cdot 10^{-4}}$	$2,18 \cdot 10^{-4}$	$2,44 \cdot 10^{-4}$
ε_p	$\mathbf{16,7 \cdot 10^{-4}}$	$\mathbf{1,52 \cdot 10^{-4}}$	$1,85 \cdot 10^{-4}$	$2,05 \cdot 10^{-4}$

POST-SELECTION EFFECT ON NOISE





Transmittance window	40%-90%	80%-85%	**75%-80%**	**70%-75%**
Fraction of data	100%	54,8%	**30,4%**	**8,9%**
εx	$19{,}7 \cdot 10^{-4}$	$1{,}79 \cdot 10^{-4}$	$\mathbf{2{,}18 \cdot 10^{-4}}$	$\mathbf{2{,}44 \cdot 10^{-4}}$
εp	$16{,}7 \cdot 10^{-4}$	$1{,}52 \cdot 10^{-4}$	$\mathbf{1{,}85 \cdot 10^{-4}}$	$\mathbf{2{,}05 \cdot 10^{-4}}$

FURTHER PLANS

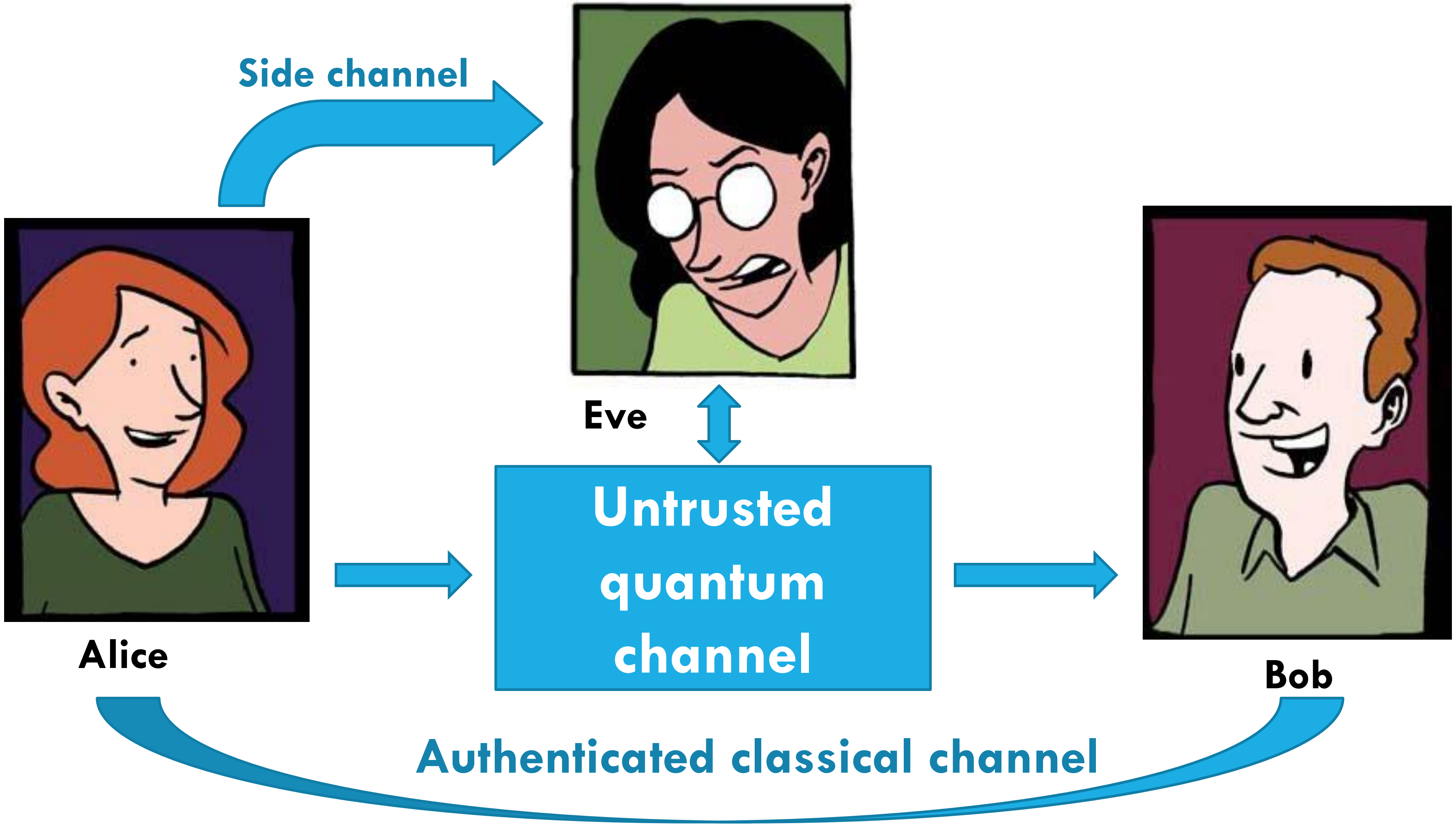
- Effect of post-selection on the key rate
- Confirmation of expected theoretical result
- Optimization of the post-selection

PART 2. TOWARDS CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION OF TRUSTED-SIDE LEAKAGE.

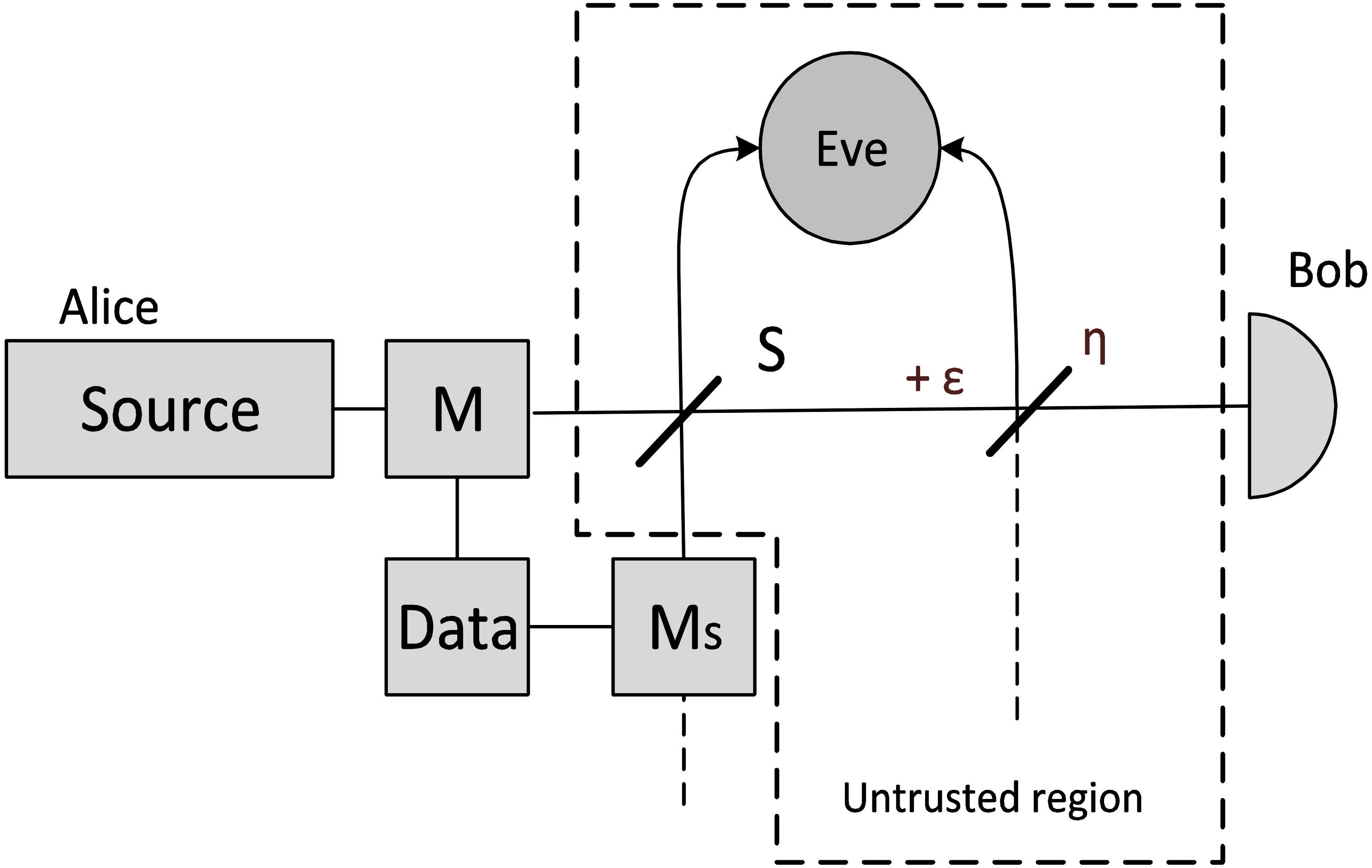
Work partly performed during the visit to DTU in Lyngby, experimental collaboration is planned.

- The study of side channel effect on the security of continuous-variable quantum key distribution protocols
- Determining security regions
- Suggestion of method for side channel decoupling
- Optimization of additional modulation

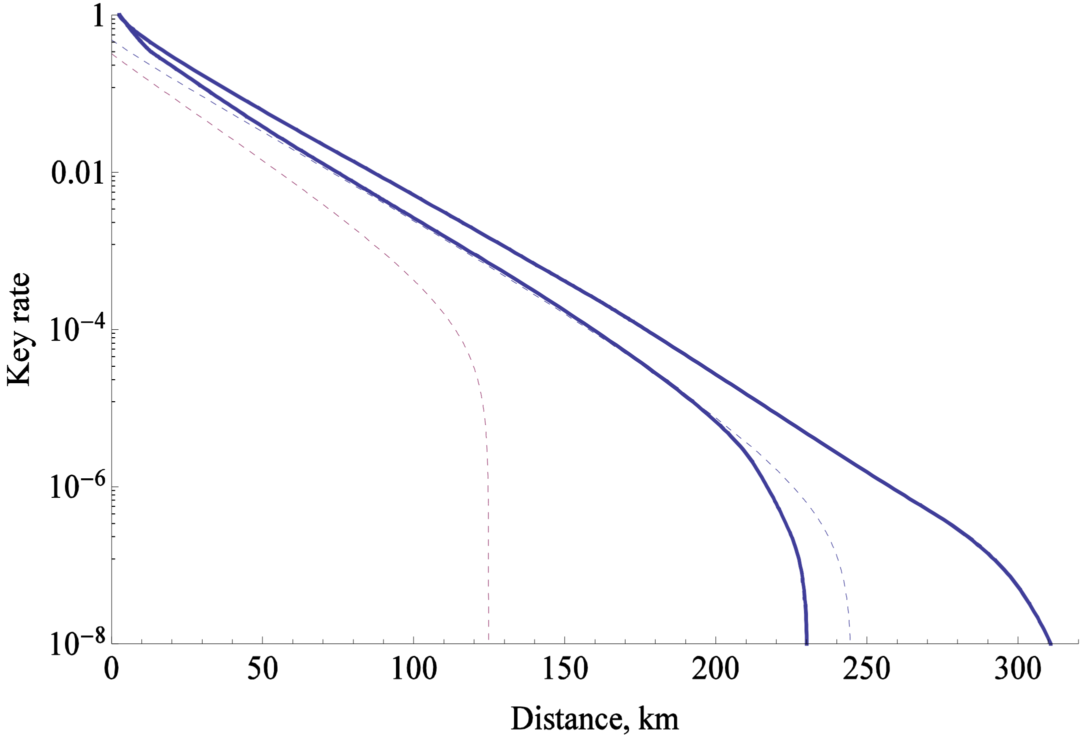
SIDE CHANNEL

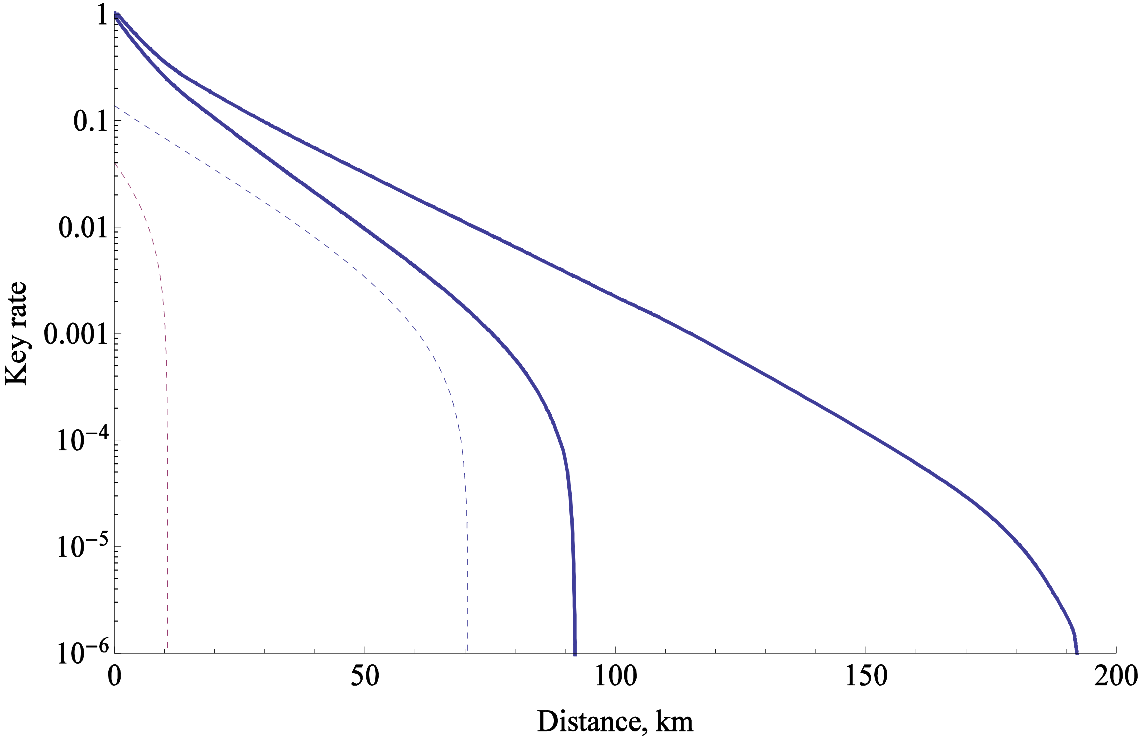


SIDE CHANNEL DECOUPLING

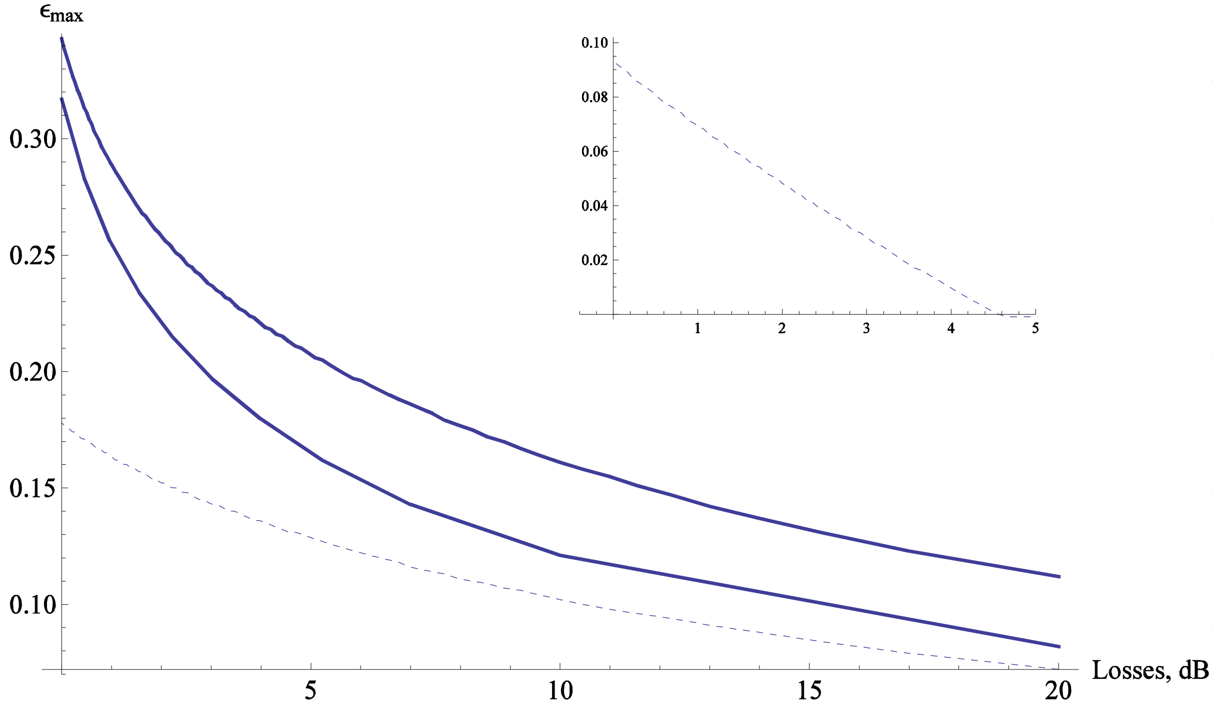


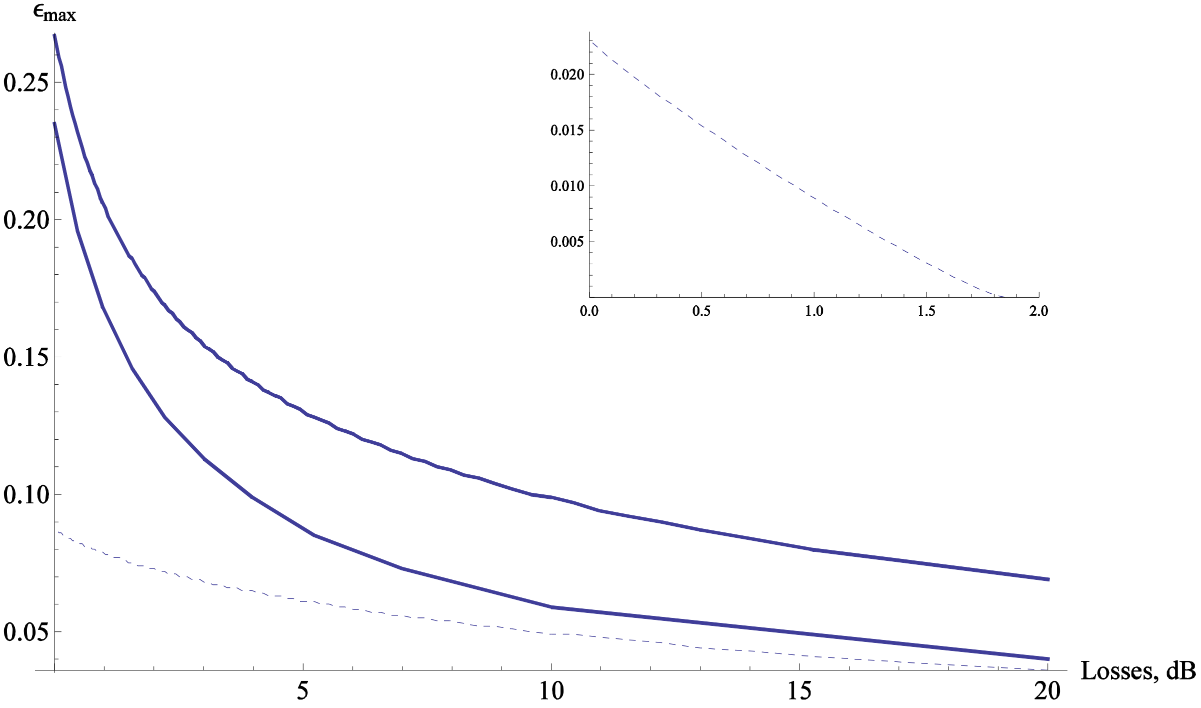
OPTIMAL ADDITIONAL MODULATION





OPTIMAL ADDITIONAL MODULATION





FURTHER PLANS

- Experimental check in collaboration with the group in Lyngby
- Theoretical study of other types of side channels

SUMMARY (PART 1)

- The data of experimental analysis of CV QKD security in free space fading channel was processed
- Corrections to detection efficiencies were made
- Initial check of theoretical predictions was carried out
- Further collaboration with experimental group is planned

SUMMARY (PART 2)

- The effect of side channel on the security of continuous-variable quantum key distribution was studied
- An optimized method of preventing of side-channel leakage was suggested
- Experimental collaboration is planned

THANK YOU FOR ATTENTION!