Faculty
of Science

Palacký University
Olomouc

MAX-PLANCK-INSTITUT
für die Physik des Lichts

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

SPIE. SECURITY+
DEFENCE

Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere

Ivan D. Derkach, Christian Peuntinger, László Ruppert, Bettina Heim, Kevin Gunthner Vladyslav C. Usenko, Dominique Elser, Christoph Marquardt, Radim Filip, Gerd Leuchs.

Atmospheric free-space or fiber-optical channel?

- Suffer from atmospheric effects (turbulence)
- Channel fading

✓Quickly deployable

✓Require only a line-of-sight location of the stations

vs

✓Stable and predictable transmittance

✓Noise is characterizable and in some cases can be negligible

- Requires prepared and ad justed network
- Higher cost

Fading channel

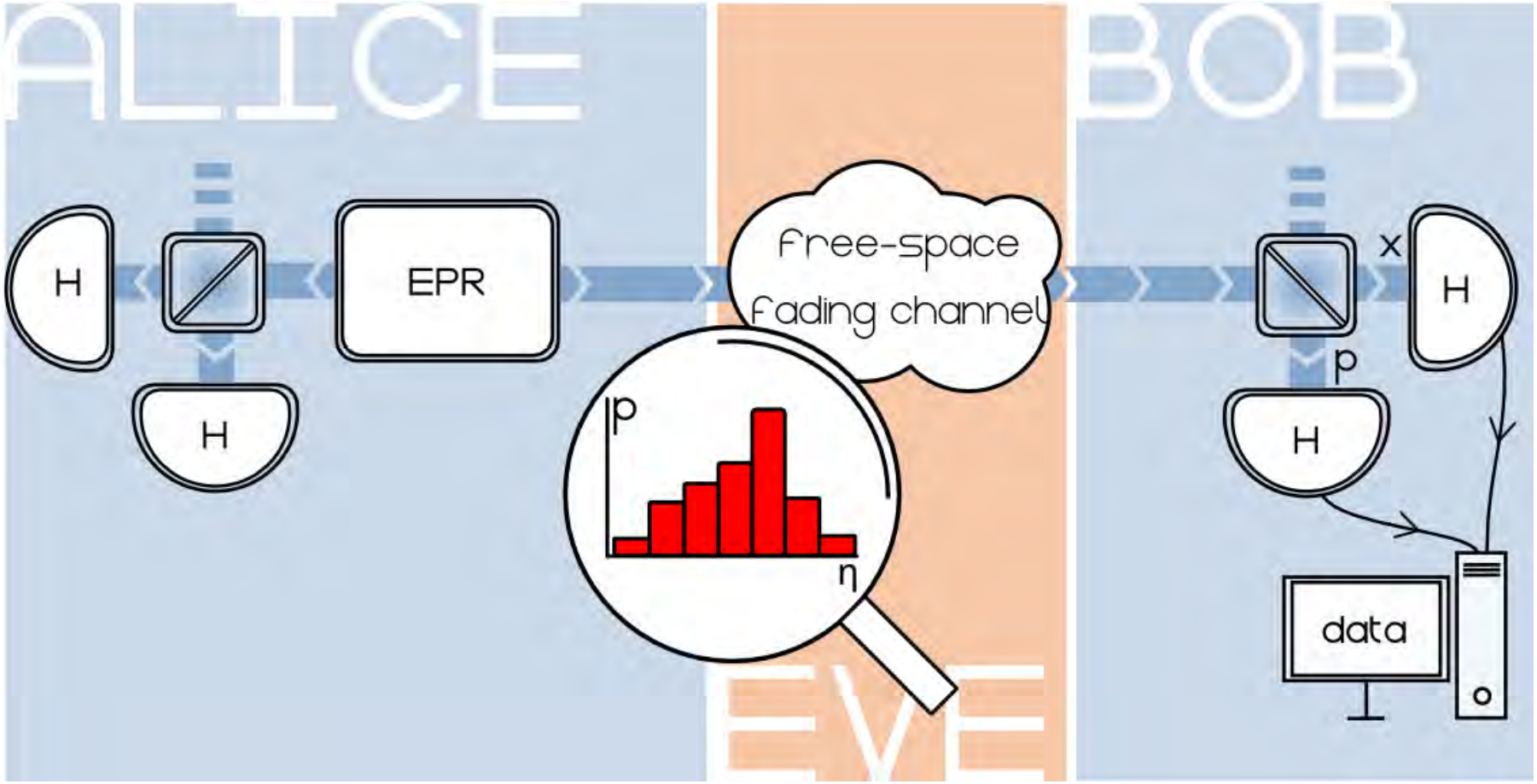
[1] Usenko et al., New. J. Phys. 14,093048 (2012)

[2] Dong et al., Phys. Rev. A 82, 012312 (2010)

Evolution of Gaussian state after single sub-channel (relatively stable transmittance window).

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_Z \\ \sqrt{V^2-1}\sigma_Z & V\mathbb{I} \end{pmatrix} \rightarrow \gamma_{AB}^{i} = \begin{pmatrix} V\mathbb{I} & \sqrt{\eta_i}\sqrt{V^2-1}\sigma_Z \\ \sqrt{\eta_i}\sqrt{V^2-1}\sigma_Z & (V\eta_i + 1 - \eta_i + \chi)\mathbb{I} \end{pmatrix}$$

Fading channel



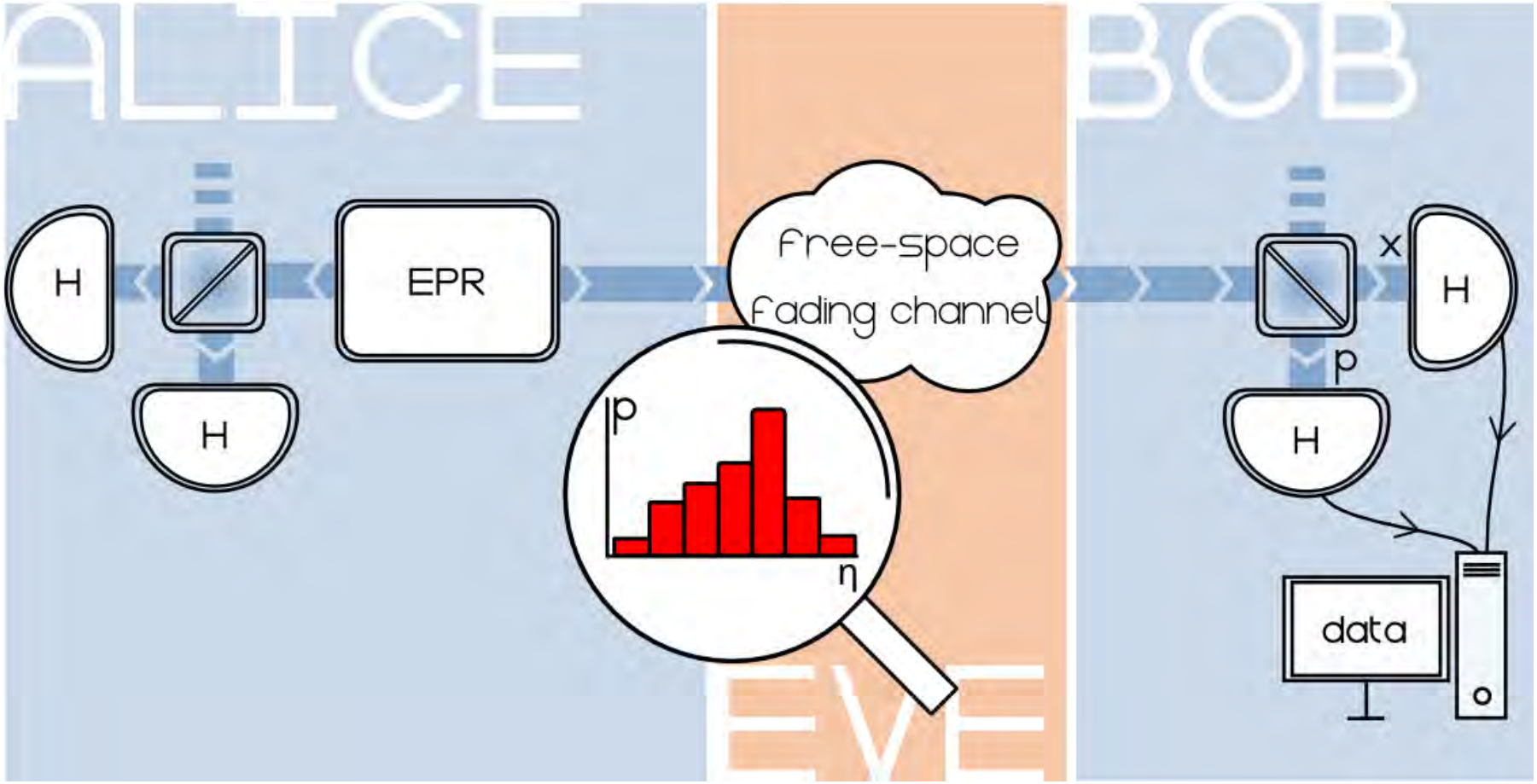
[1] Usenko et al., New. J. Phys. 14,093048 (2012)

[2] Dong et al., Phys. Rev. A 82, 012312 (2010)

The overall state after fading channel is the mixture of states after individual sub-channels.

$$\gamma_{AB}^{i} = \begin{pmatrix} V\mathbb{I} & \sqrt{\eta_i}\sqrt{V^2-1}\sigma_Z \\ \sqrt{\eta_i}\sqrt{V^2-1}\sigma_Z & (V\eta_i + 1 - \eta_i + \chi)\mathbb{I} \end{pmatrix} \Rightarrow \gamma'_{AB} = \begin{pmatrix} V\mathbb{I} & \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_Z \\ \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_Z & (V\langle\eta\rangle + 1 - \langle\eta\rangle + \chi)\mathbb{I} \end{pmatrix}$$

Fading channel



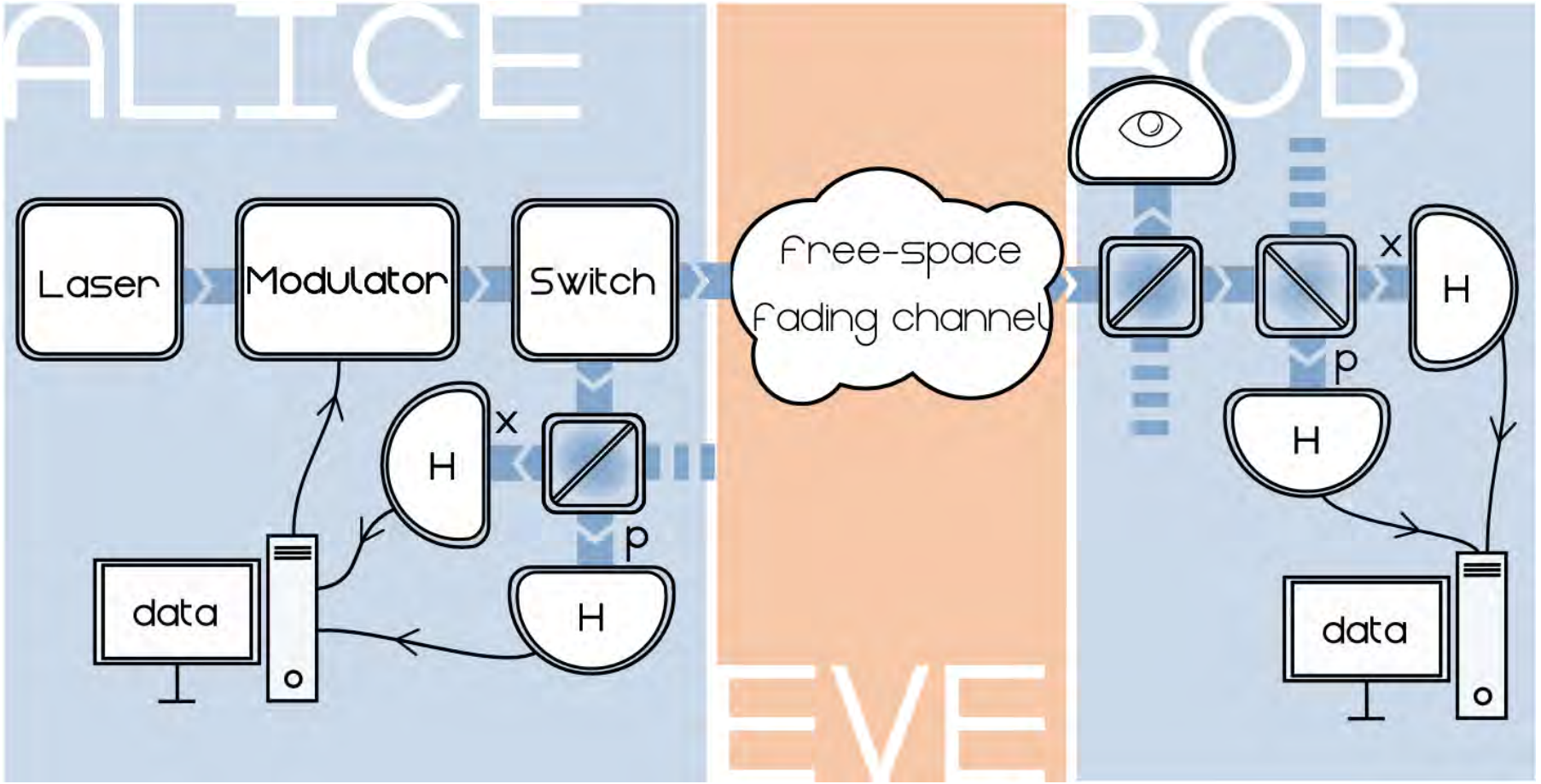
[1] Usenko et al., New. J. Phys. 14,093048 (2012)

[2] Dong et al., Phys. Rev. A 82, 012312 (2010)

Channel can be considered as a non-fading with transmittance $\langle\sqrt{\eta}\rangle^2$ and excess noise caused by fading $\varepsilon_f = Var(\sqrt{\eta})(V-1)$. The variance of the signal mode after channel becomes $V_B' = \langle\sqrt{\eta}\rangle^2(V-1) + \varepsilon_f + \chi + 1$.

ε_f - variance dependent noise!

Setup sketch. Key rate.



R_{col} - key rate

β – post-processing efficiency

I_{AB}- mutual information between trusted parties

χ_E - Holevo bound

V_X - state variance

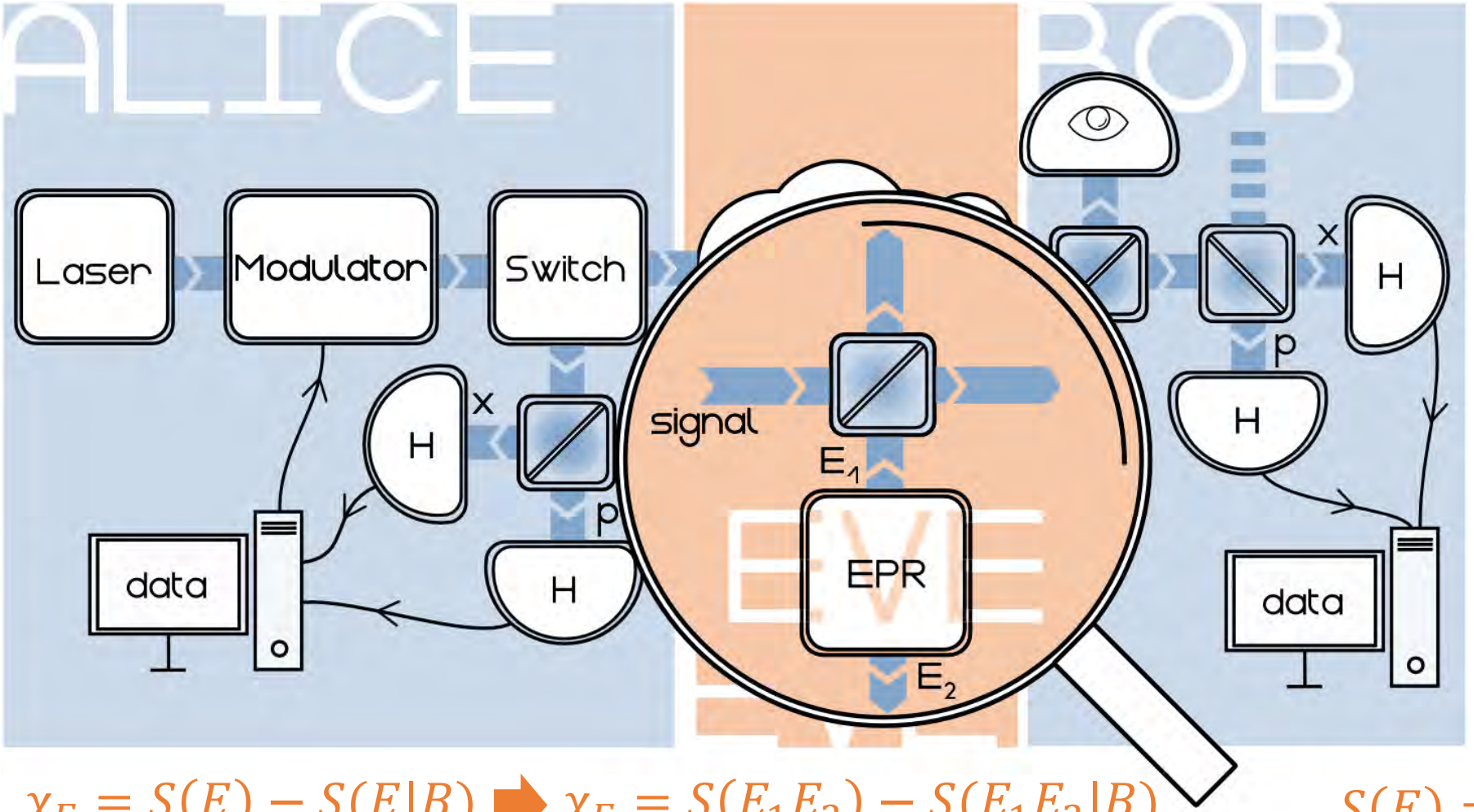
$V_{X|Y}$ - conditional state variance

C_{XY}- correlations

$$R_{col} = \beta I_{AB} - \chi_E; \quad I_{XY} = \frac{1}{2}\log_2\left[\frac{V_X}{V_{X|Y}}\right]; \quad V_{XY} = V_X - \frac{C_{XY}^2}{V_B};$$

«Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere» Ivan D. Derkach. SPIE 2016. (Edinburgh)

Setup sketch. Eve.



χ_E - Holevo bound

$S(X)$ - Von Neumann entropy

$G(x)$ - bosonic entropy function

λ_i - covariance matrix symplectic eigenvalues

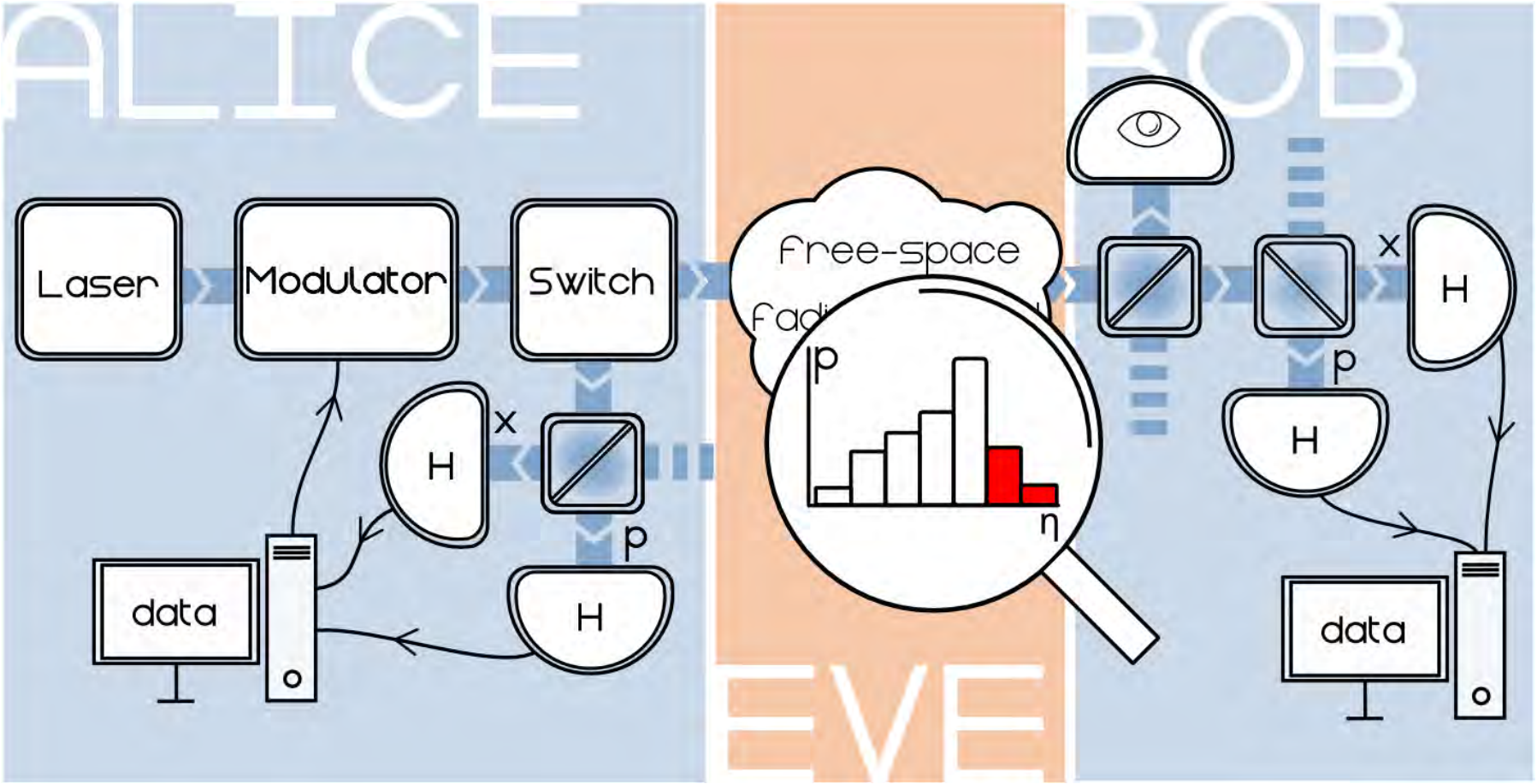
$$\chi_E = S(E) - S(E|B) \Rightarrow \chi_E = S(E_1E_2) - S(E_1E_2|B)$$

$$G(x) = (x+1)\log_2[x+1] - x\log_x x$$

$$S(E) = \sum_{i=1}^{N} G\left(\frac{\lambda_i - 1}{2}\right)$$

«Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere» Ivan D. Derkach. SPIE 2016. (Edinburgh)

Setup sketch. Post-selection.



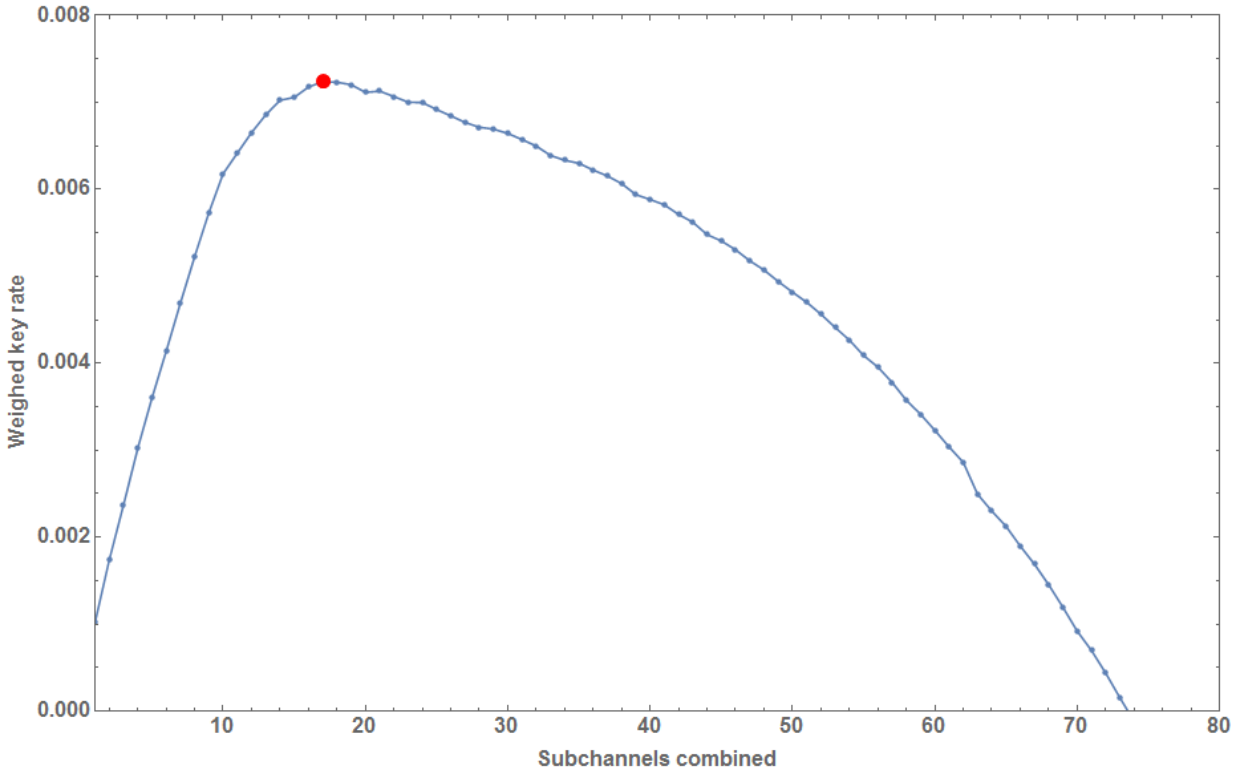
We create post-selected state by choosing a subset of channel transmittance distribution.

This allows us maximize lower bound of the secure key rate of the coherent-state CV QKD protocol.

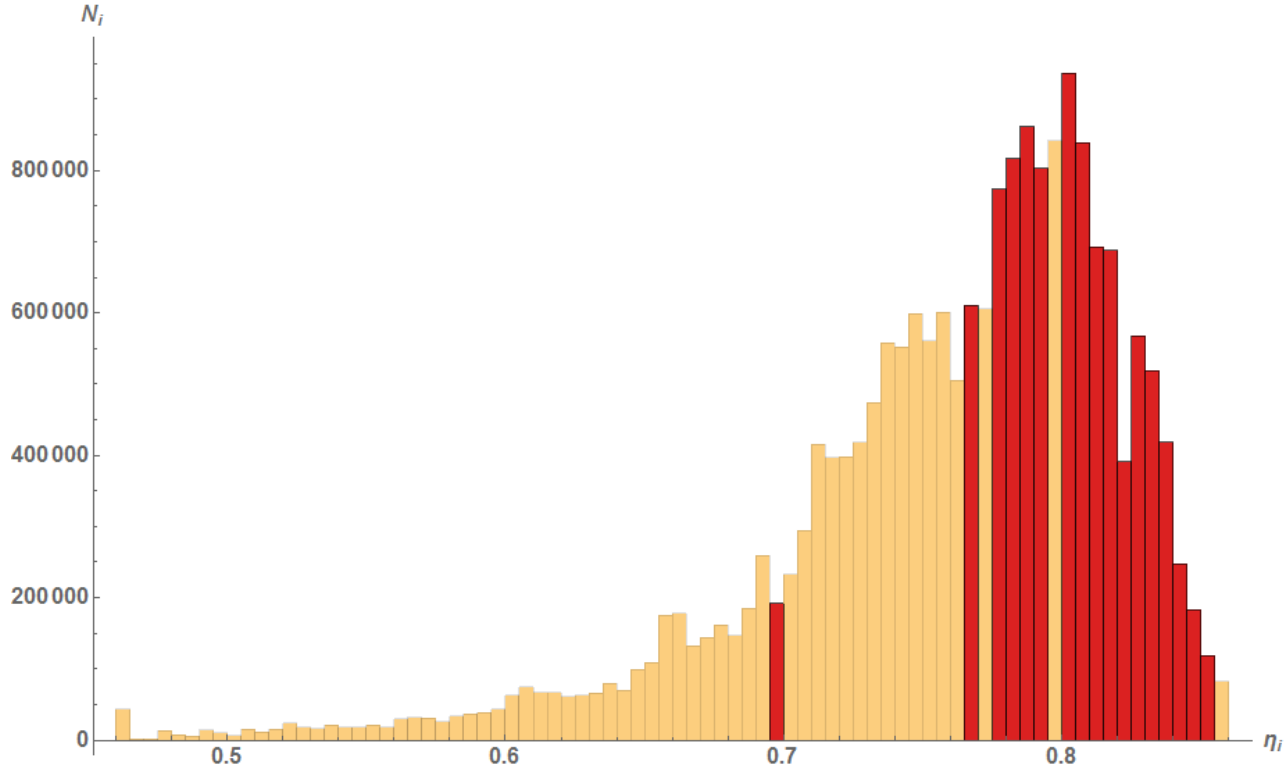
«Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere» Ivan D. Derkach. SPIE 2016. (Edinburgh)

Results. Vm=0.51

Key rate for the post-selected state



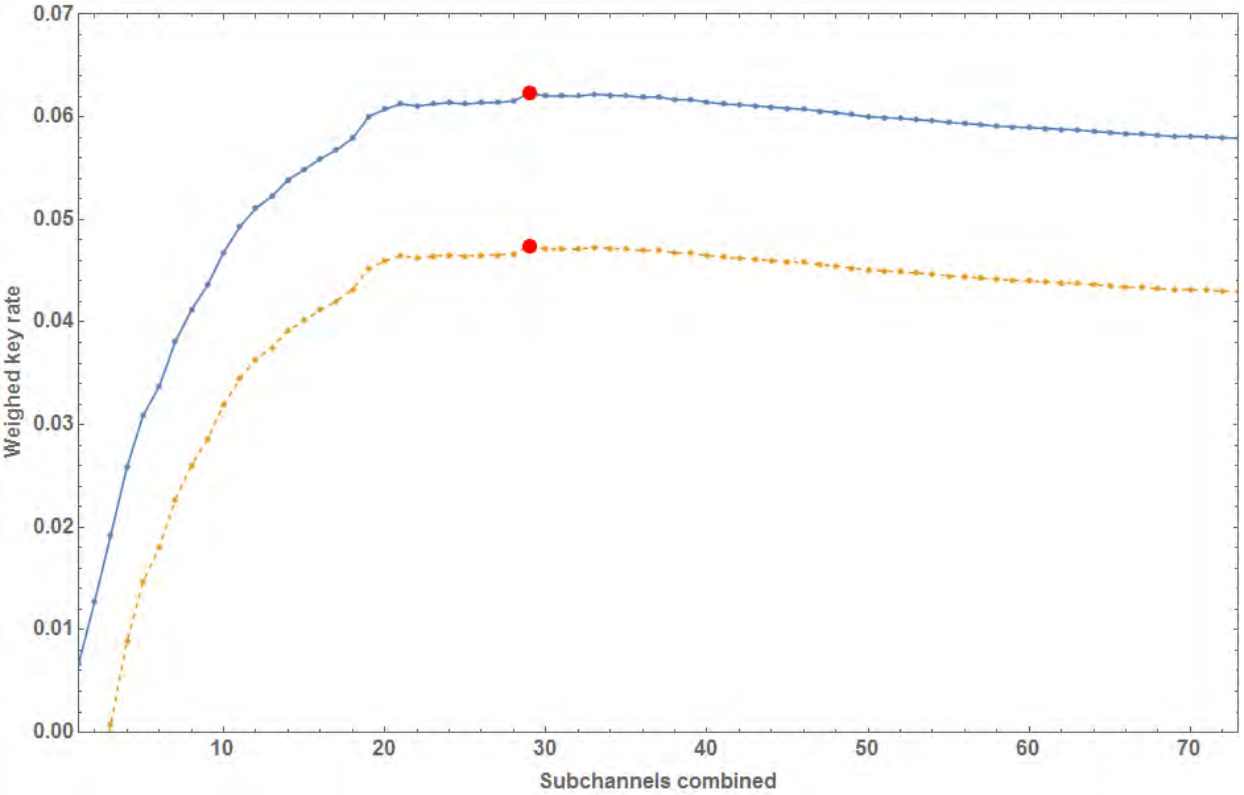
Atmospheric channel transmittance distribution



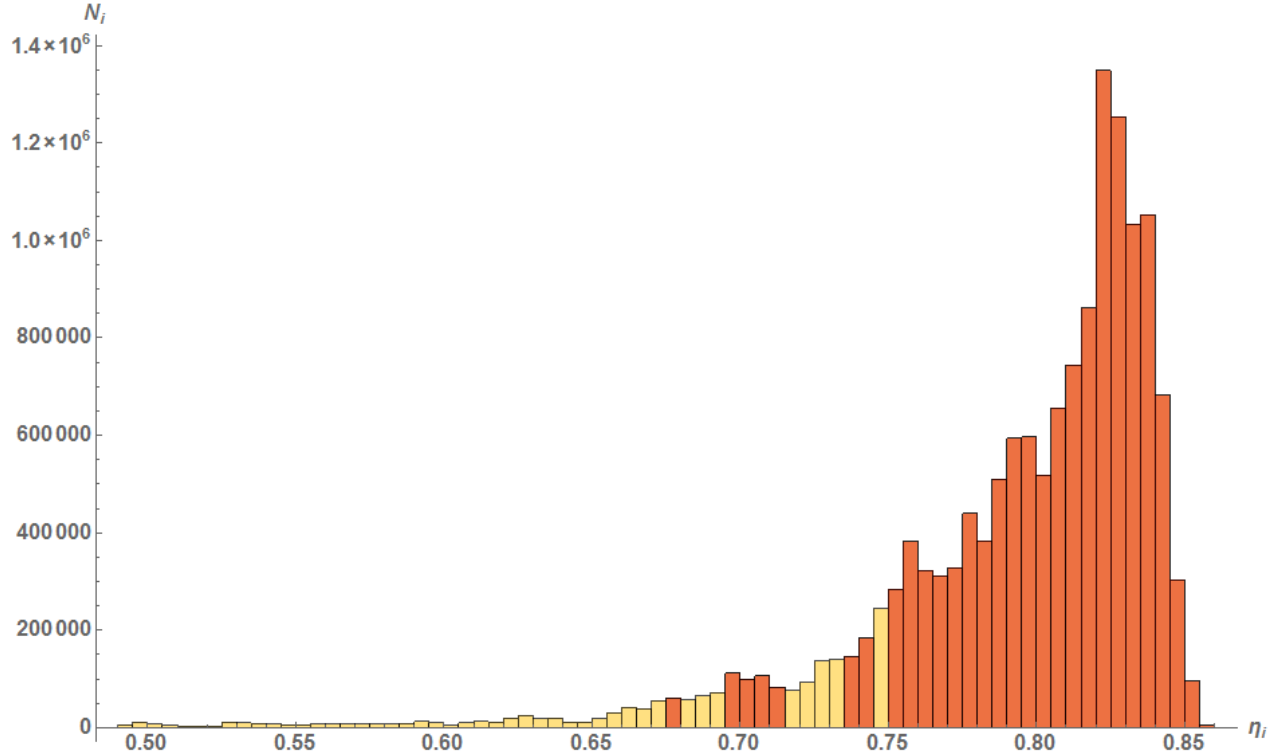
«Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere» Ivan D. Derkach. SPIE 2016. (Edinburgh)

Results. Vm=1.44

Key rate for the post-selected state



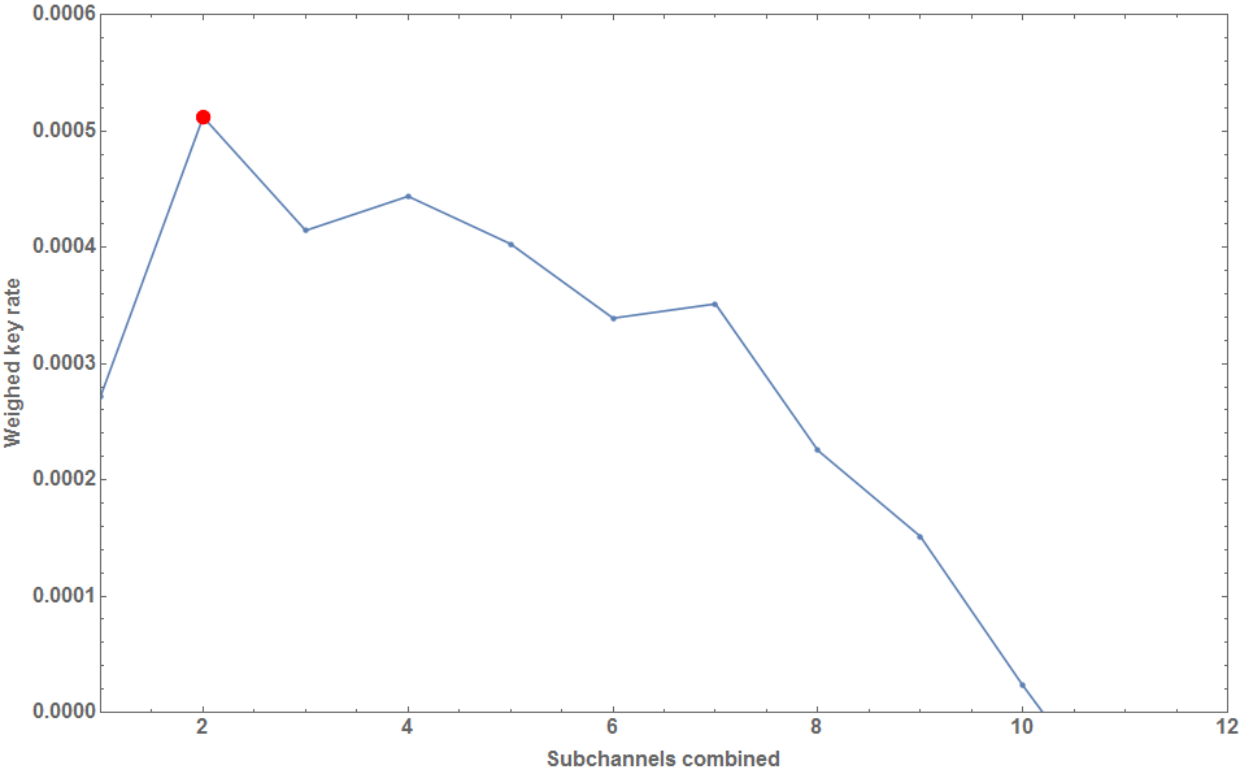
Atmospheric channel transmittance distribution



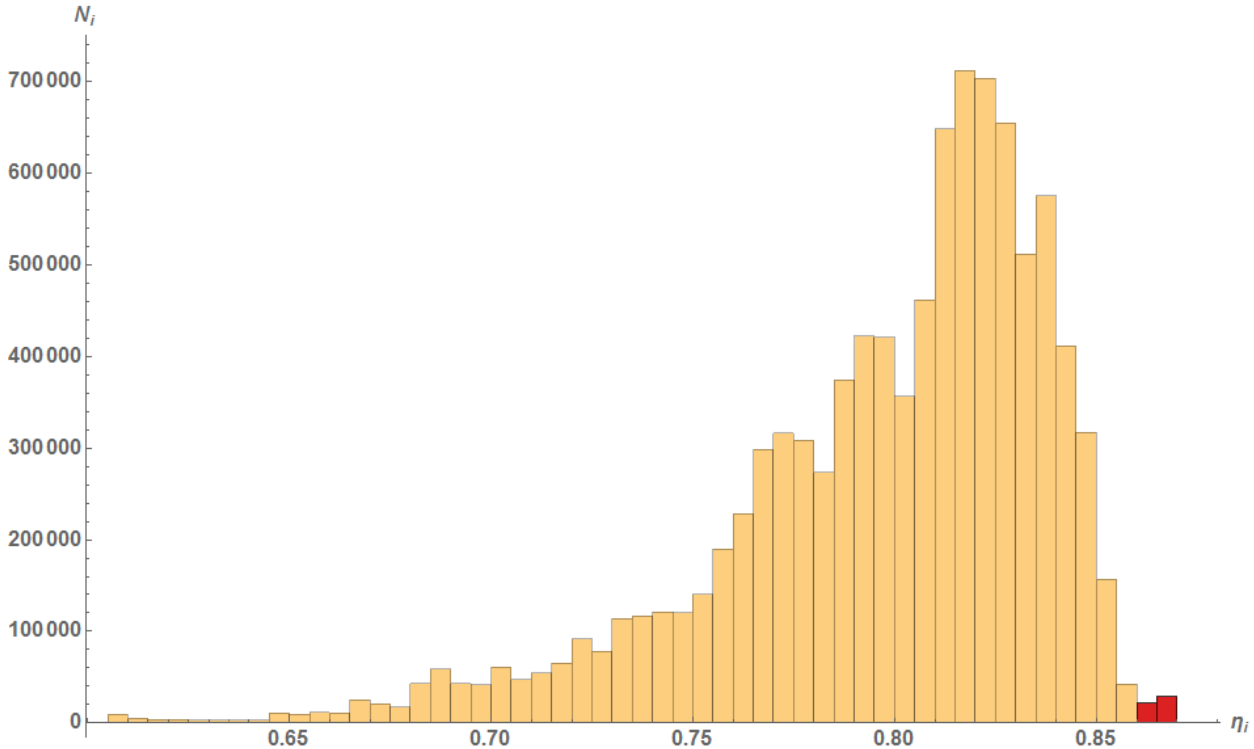
[3] Leverrier, Grosshans, Grangier, Physical Review A 81, 062343 (2010).

Results. Vm=3.6

Key rate for the post-selected state



Atmospheric channel transmittance distribution



«Proof-of-principle test of coherent-state continuous-variable quantum key distribution through turbulent atmosphere» Ivan D. Derkach. SPIE 2016. (Edinburgh)

Conclusions

- We have demonstrated the possibility to perform continuous-variable quantum key distribution over the real atmospheric channel with the transmittance fluctuations
- Considering the optimal state modulation coherent-state protocol can overcome finite-size effects and limited post-processing efficiency
- The post-selection of sub-channels can quantitatively improve the key rate and even restore it
- The post-selection can be advantageous even for optimal modulation considering more turbulent atmospheric channels

Further steps

- Compensation of beam wandering effects in atmospheric free-space channels

  [Preparing publication]

- Side channels effects in CV QKD

  [Derkach, Usenko, Filip, Phys. Rev. A **93**, 032309 (2016)]

- Source attacks, multimode modulation effects and advantages of coherent-state protocol in CV QKD

  [Preparing publication]

Thank you!