Proof-of-principle Test of Continuous-Variable QKD in Free-Space Atmospheric Channel

Vladyslav Usenko[1], Christian Peuntinger[2,3], Ivan Derkach[1], Bettina Heim[2,3,4], Christoph Marquardt[2,3,4], Radim Filip[1] and Gerd Leuchs[2,3,4]

1. Department of Optics, Palacký University, Olomouc, Czech Republic
2. Max Planck Institute for the Science of Light, Erlangen, Germany
3. Institute of Optics, Information and Photonics, FAU, Erlangen, Germany
4. Graduate School in Advanced Optical Technologies, FAU, Erlangen, Germany

QCrypt'2015, Tokyo

Outline

- Continuous-variable QKD
- Fading channels
- Effect on security of CS CV QKD
- Post-selection
- Proof-of-principle test
- Further plans
- Summary

Continuous-variable (CV) QKD

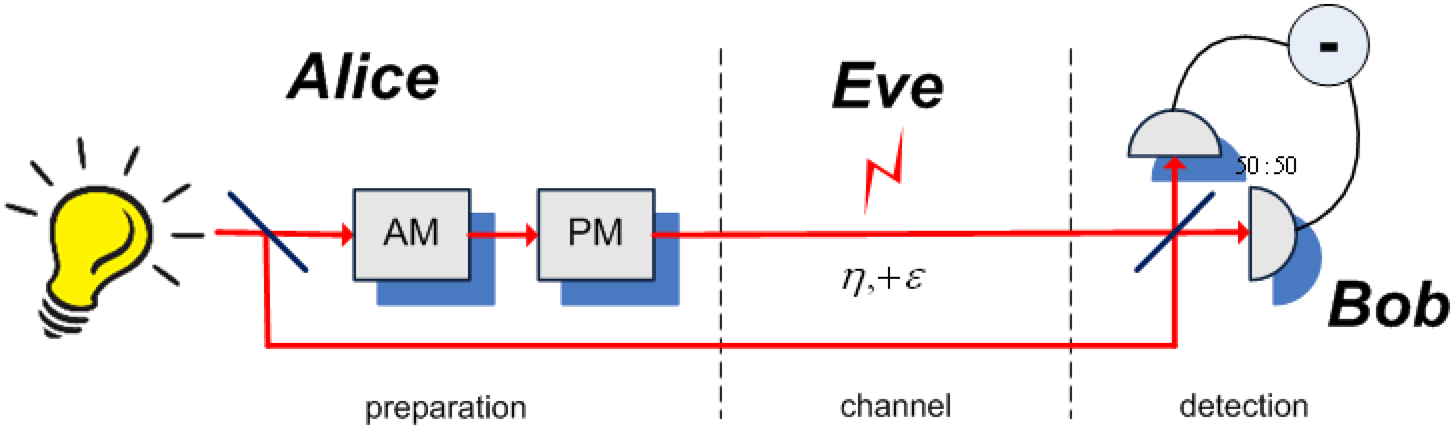
ALICE

Share a secret key between Alice & Bob for the one-time pad (Vernam, 1919; Shannon, 1949)

BOB

CV protocols – attempt to go beyond the single photon statistics and use the wave properties of light employing the multiphoton quantum states.

CV Quantum Key Distribution

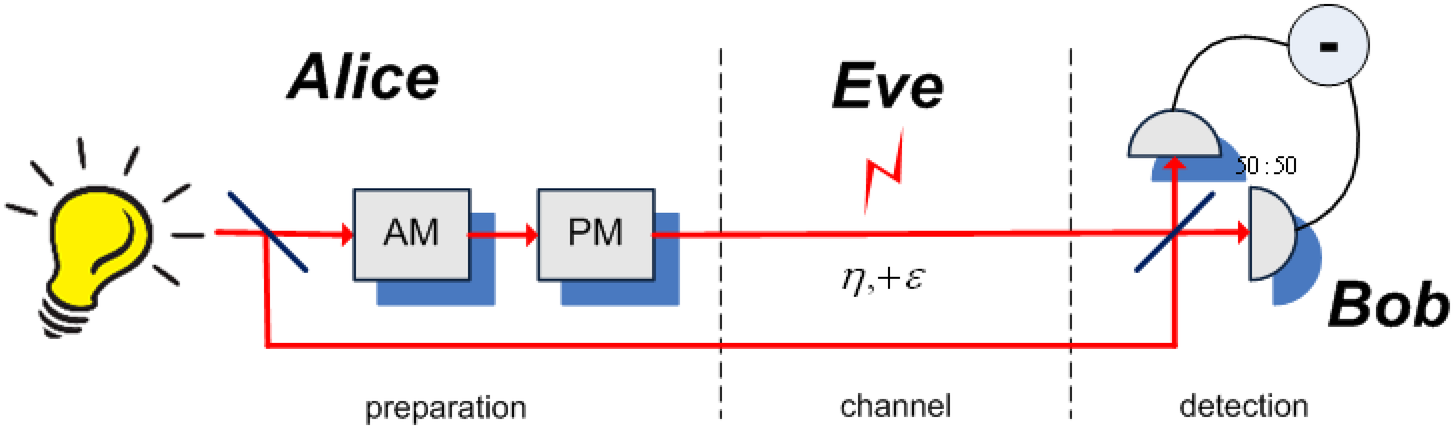


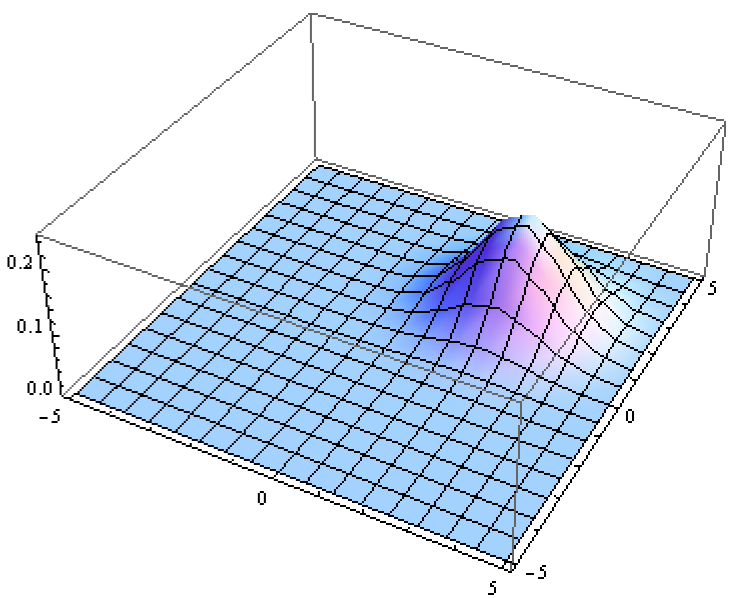
Coherent states-based protocol (GG02)

- Laser source
- Gaussian quadrature modulation
- Homodyne detection

F. Grosshans and P. Grangier. PRL 88, 057902 (2002);
F. Grosshans et al., Nature 421, 238 (2003)

CV Quantum Key Distribution

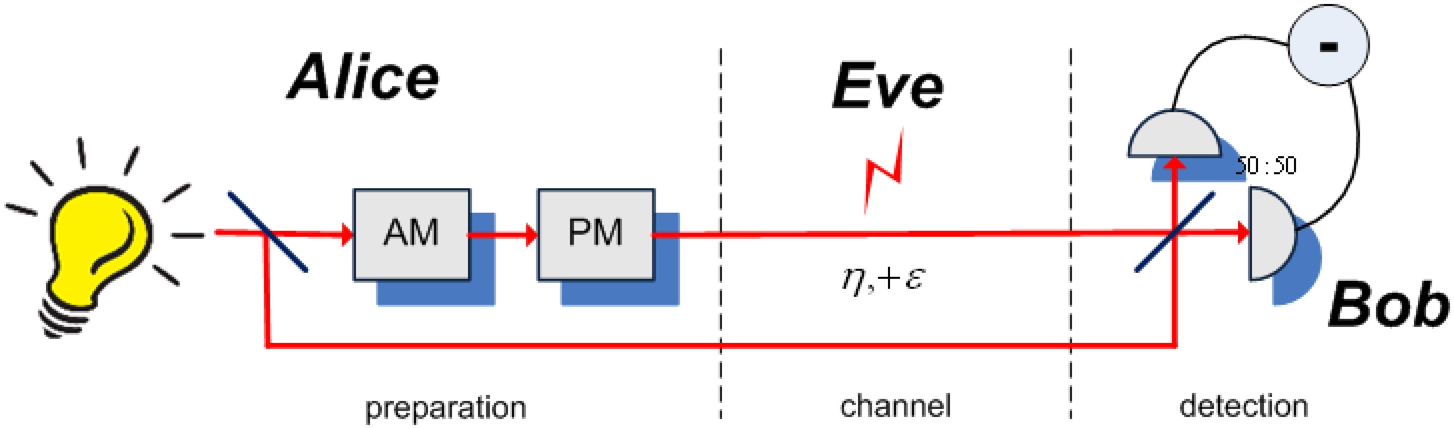


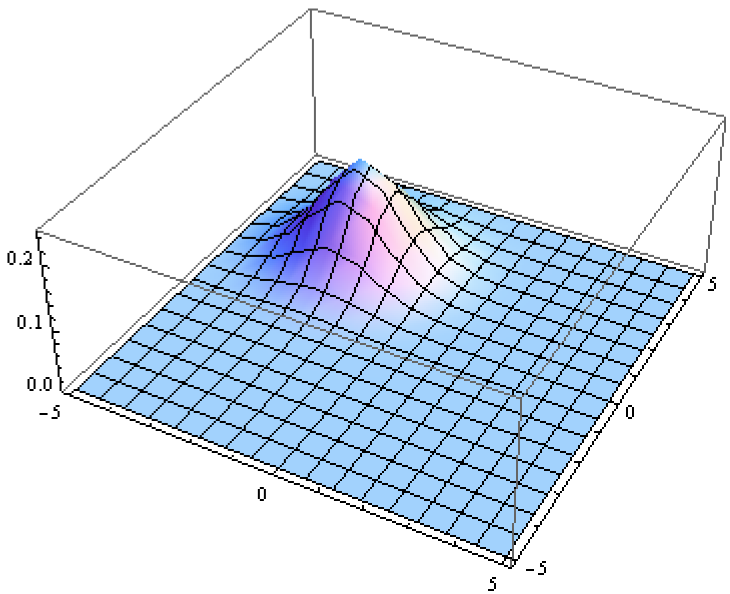


Coherent states-based protocol

- Alice generates two Gaussian random variables {**a,b**}
- Alice prepares a coherent state, displaced by {**a,b**}
- Bob measures a quadrature, obtaining **a** or **b**
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

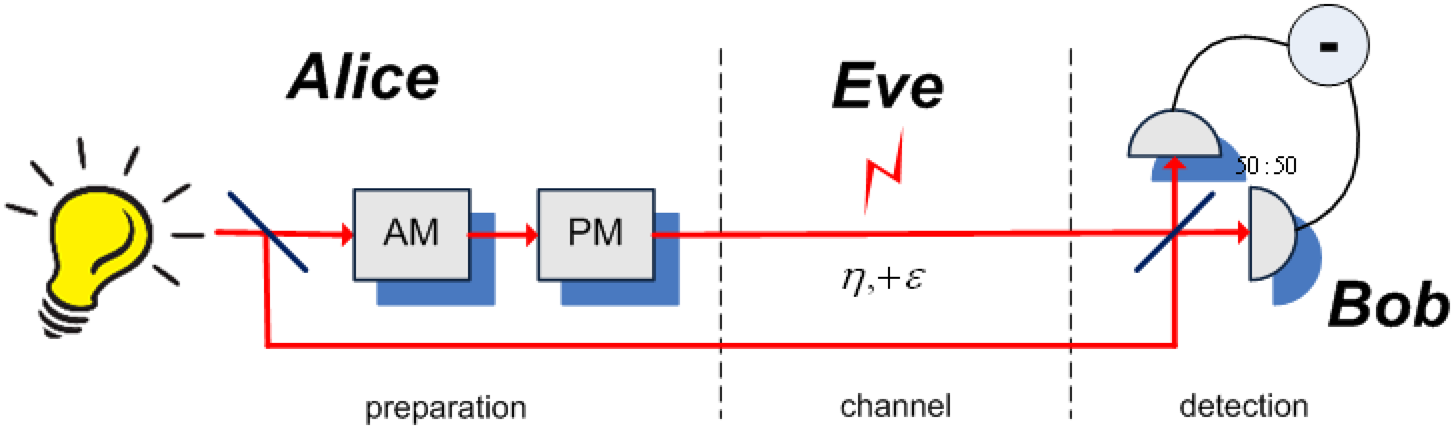


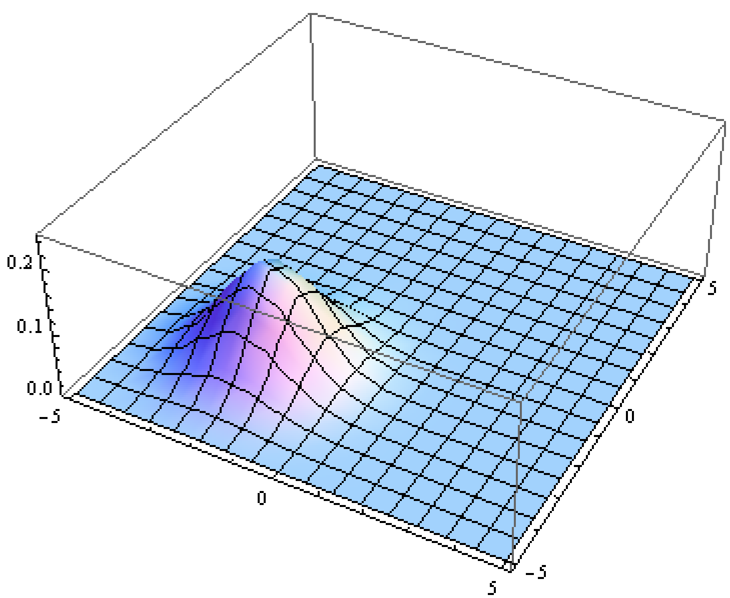


Coherent states-based protocol

- Alice generates two Gaussian random variables {**a,b**}
- Alice prepares a coherent state, displaced by {**a,b**}
- Bob measures a quadrature, obtaining **a** or **b**
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

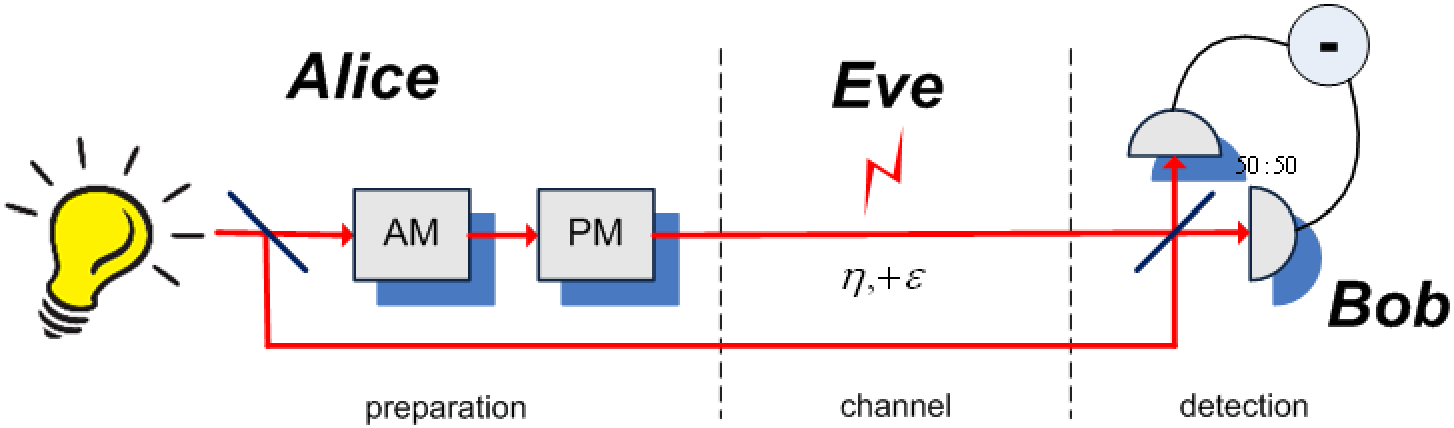


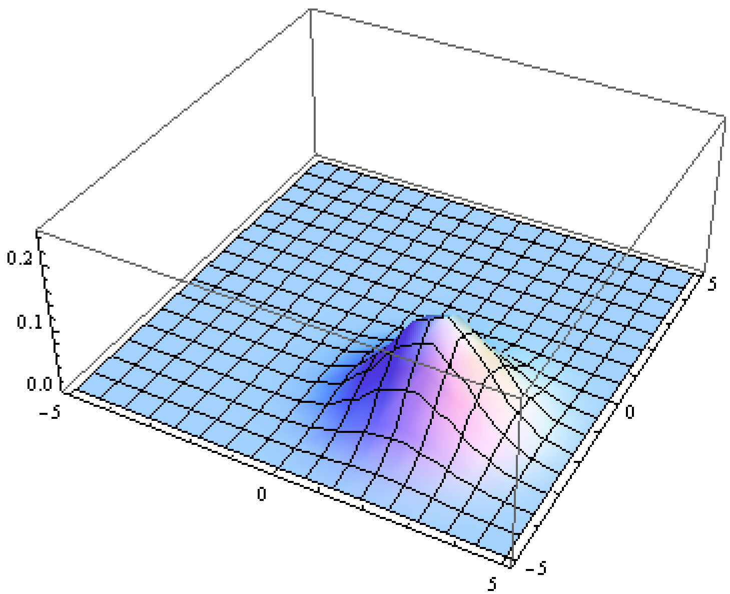


Coherent states-based protocol

- Alice generates two Gaussian random variables {**a,b**}
- Alice prepares a coherent state, displaced by {**a,b**}
- Bob measures a quadrature, obtaining **a** or **b**
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

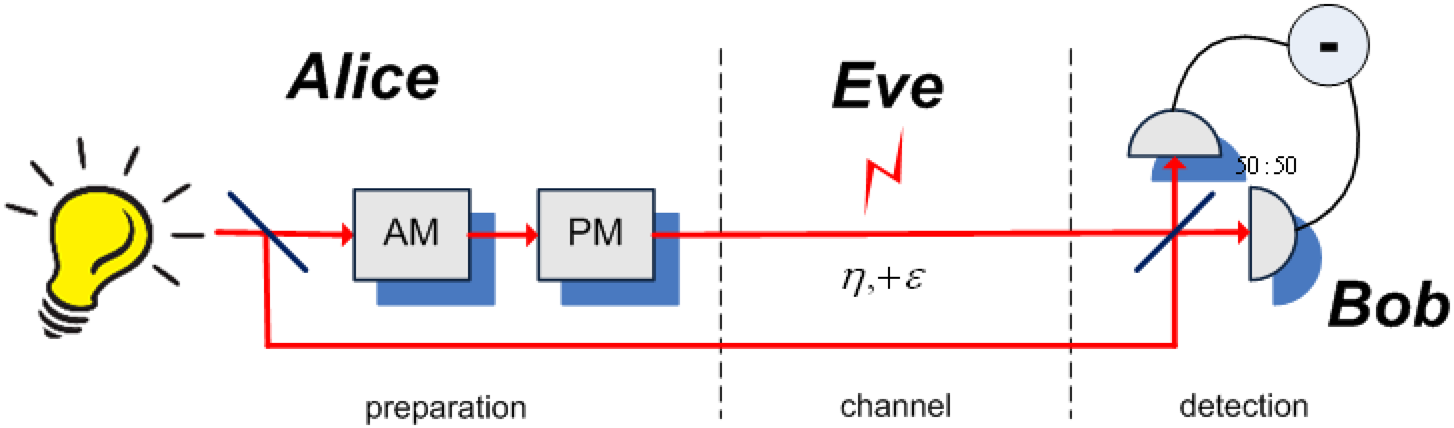


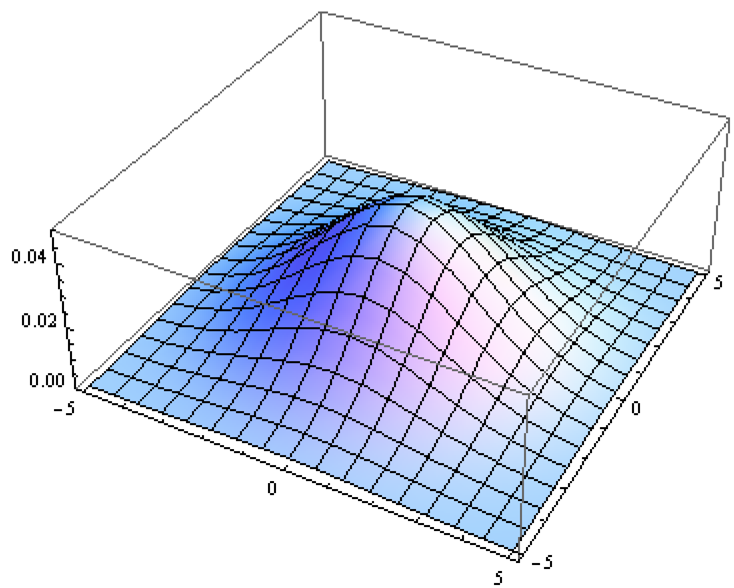


Coherent states-based protocol

•Alice generates two Gaussian random variables {**a,b**}
•Alice prepares a coherent state, displaced by {**a,b**}
•Bob measures a quadrature, obtaining **a** or **b**
•Bases reconciliation
•Error correction, privacy amplification

CV Quantum Key Distribution



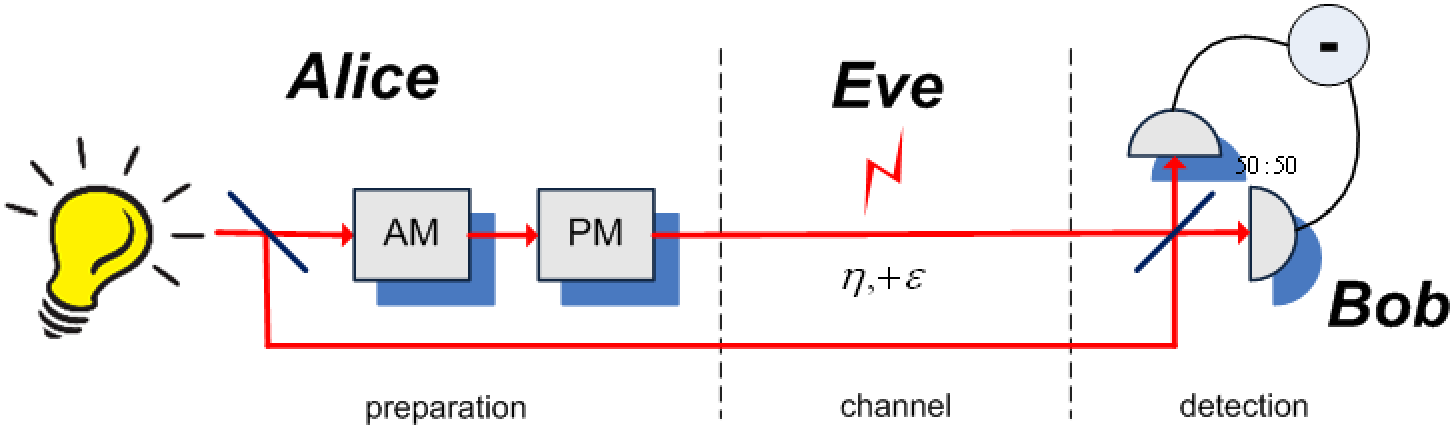


Mixture

Coherent states-based protocol

- Alice generates two Gaussian random variables {**a,b**}
- Alice prepares a coherent state, displaced by {**a,b**}
- Bob measures a quadrature, obtaining **a** or **b**
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution



Coherent states-based protocol: achievements

25 km, 2 kbps [*J. Lodewyck et al., PRA 76, 042305 (2007)]*

80 km, ~150 bps [*P.Jouguet et al., Nature Photonics 7, 378-381 (2013)]*

CV Quantum Key Distribution

SECURITY

Collective attacks: **asymptotic**

[Navascués et al. PRL 97, 190503;
Garcia-Patron & Cerf, PRL 97, 190503]

finite-size

[Leverrier & Grangier, PRA 81, 062314;
Leverrier et al. PRA 81, 062343;
Ruppert et al., PRA 90 062310]

General attacks: **asymptotic / finite-size**

[Leverrier et. al. PRL 110 030502]

Composable security: **asymptotic**

[Leverrier PRL 114, 070501]

CV Quantum Key Distribution

ADVANTAGES

- Large alphabet, no empty pulses, no need for decoy states
- Efficient mode-selective homodyne detection
- Relative simplicity (possible to do on a chip)

CV Quantum Key Distribution

ISSUES

- Continuous influence of channel imperfections (subject to analysis)
- Possible attacks on local oscillator (can be monitored/self-referenced/classically locked)
- Side channels and other loopholes ([M]DI CV QKD possible)
- Post-processing (mainly solved)

Environment for CV QKD

- Attenuating channels (fiber-optical links)
- Channels with excess noise (fiber links+noise)
- Fluctuating channels (atmospheric links)

Environment for CV QKD

- ✓ Attenuating channels (fiber-optical links)
- ✓ Channels with excess noise (fiber links+noise)
- ✗ Fluctuating channels (atmospheric links)

Environment for CV QKD

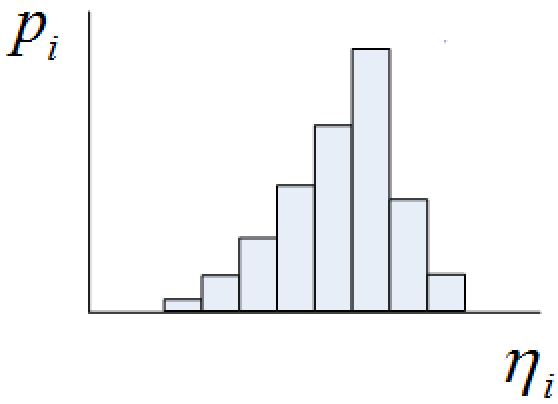
- ✓ Attenuating channels (fiber-optical links)
- ✓ Channels with excess noise (fiber links+noise)
- ✗ Fluctuating channels (atmospheric links)

Our study

Analysis of CV QKD in free-space channels, proof-of-principle test.

Fading channels

Described by the distributions of transmittance values $\{\eta_i\}$ and respective probabilities $\{p_i\}$:



Fading is typically observed in atmospheric channels, where it is caused by the turbulence effects.

Security of CV QKD

Individual attacks: $I_i = I_{AB} - I_{BE}$

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} \qquad I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E}}$$

Collective attacks: $I = I_{AB} - \chi_{BE}$

Holevo quantity: $\chi_{BE} = S_E - \int P(B) S_{E|B} dB$ $\quad \chi_{BE} = S(\rho_E) - S(\rho_{E|B})$

In case of channel noise Eve is assumed to be able to hold purification:

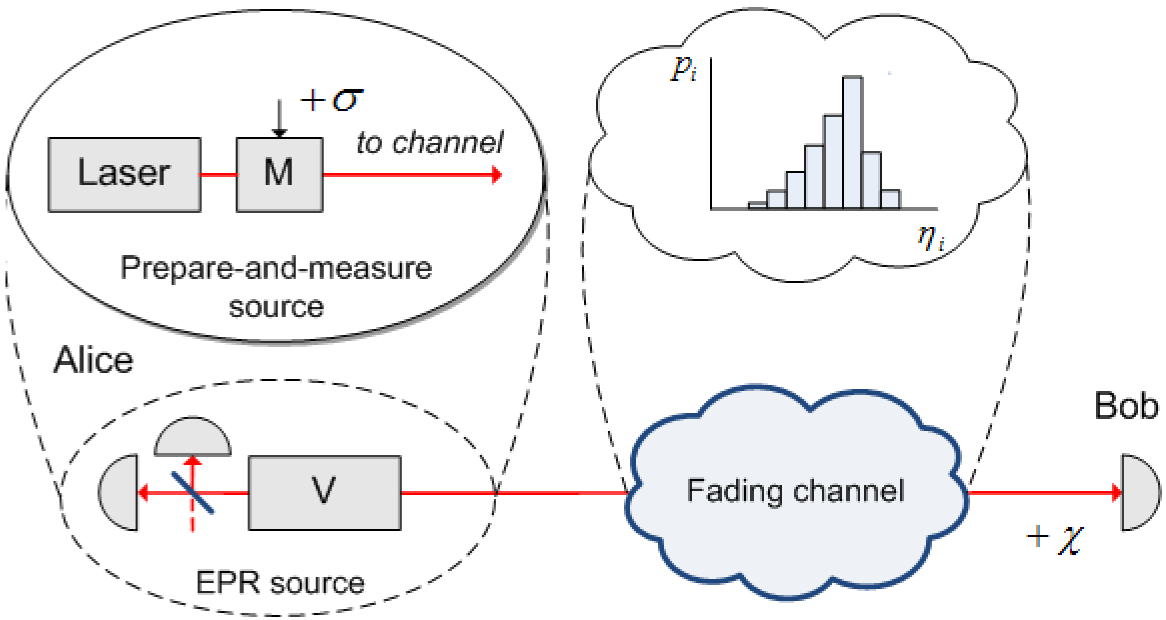
$$S(\rho_E) = S(\rho_{AB}) \qquad S(\rho_{E|B}) = S(\rho_{A|B})$$

von Neumann entropy is given by:

$$S_\gamma = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \quad G(x) = (x+1)\log_2(x+1) - x\log_2 x$$

Fading channels: effect on CV QKD

Equivalent entanglement-based scheme:



Effect of a fading channel upon individual attacks:

$$Var(\sqrt{\eta})_{max,ind} = \frac{\langle\sqrt{\eta}\rangle^2\sigma - 2(\sigma+1)(\chi+1) + \sqrt{\langle\sqrt{\eta}\rangle^4\sigma^2 + 4(\sigma+1)^2}}{2\sigma(\sigma+1)}$$

Where $\sigma = V - 1$ - modulation variance

Fading channels: effect on CV QKD

Initial two-mode covariance matrix:

$$\gamma_{AB}^{0} = \begin{pmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{pmatrix}$$

Effect of an *i*-th channel:

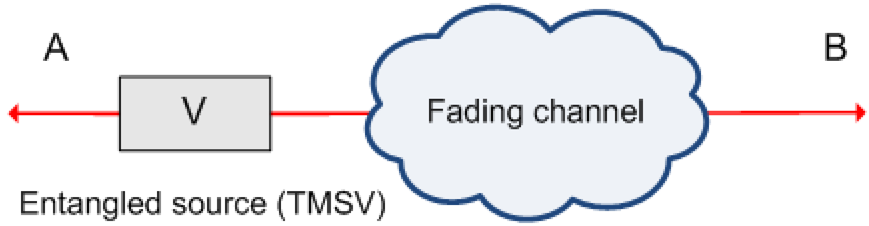
$$\gamma_{AB}^{i} = \begin{pmatrix} \gamma_A & \sqrt{\eta_i}\sigma_{AB} \\ \sqrt{\eta_i}\sigma_{AB} & \eta_i\gamma_B + [1-\eta_i]\mathbb{I} \end{pmatrix}$$

Effect of the fading channel:

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \langle\sqrt{\eta}\rangle\sigma_{AB} \\ \langle\sqrt{\eta}\rangle\sigma_{AB} & \langle\eta\rangle\gamma_B + [1-\langle\eta\rangle]\mathbb{I} \end{pmatrix}$$

[Dong et al. PRA 82 012312 (2010) / arXiv:1002.0280*]*

Fading channels: effect on CV QKD



Initial two-mode squeezed-vacuum state:

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{I} \end{pmatrix}$$

After a fading channel:

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

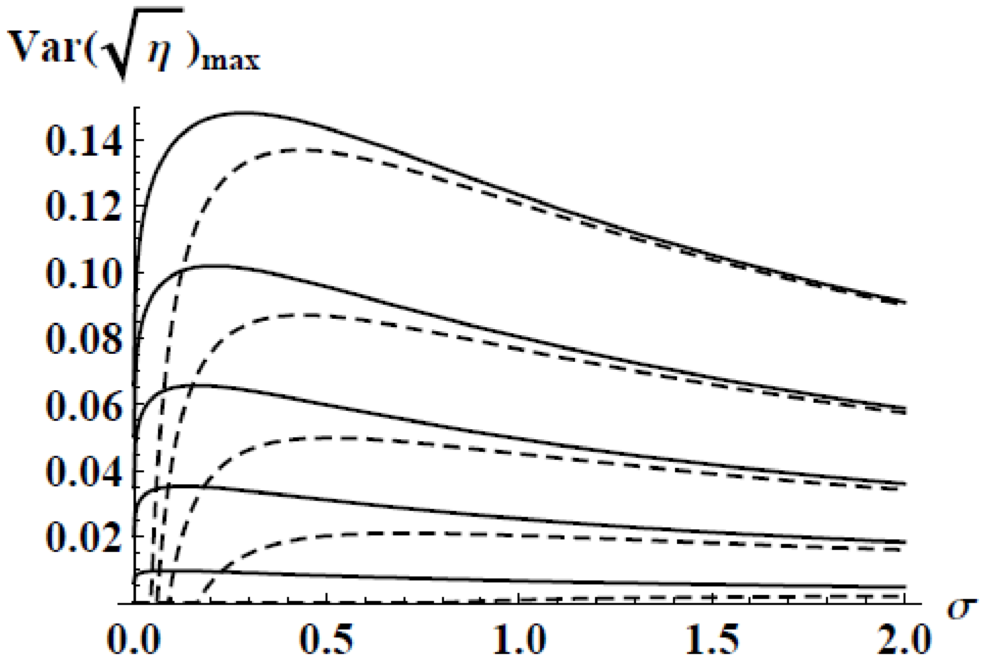
Is equivalent to a fixed channel with variance-dependent excess noise:

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

where $\epsilon_f = Var(\sqrt{\eta})(V-1)$ and $Var(\sqrt{\eta}) = \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2$

Fading channels: effect on CV QKD

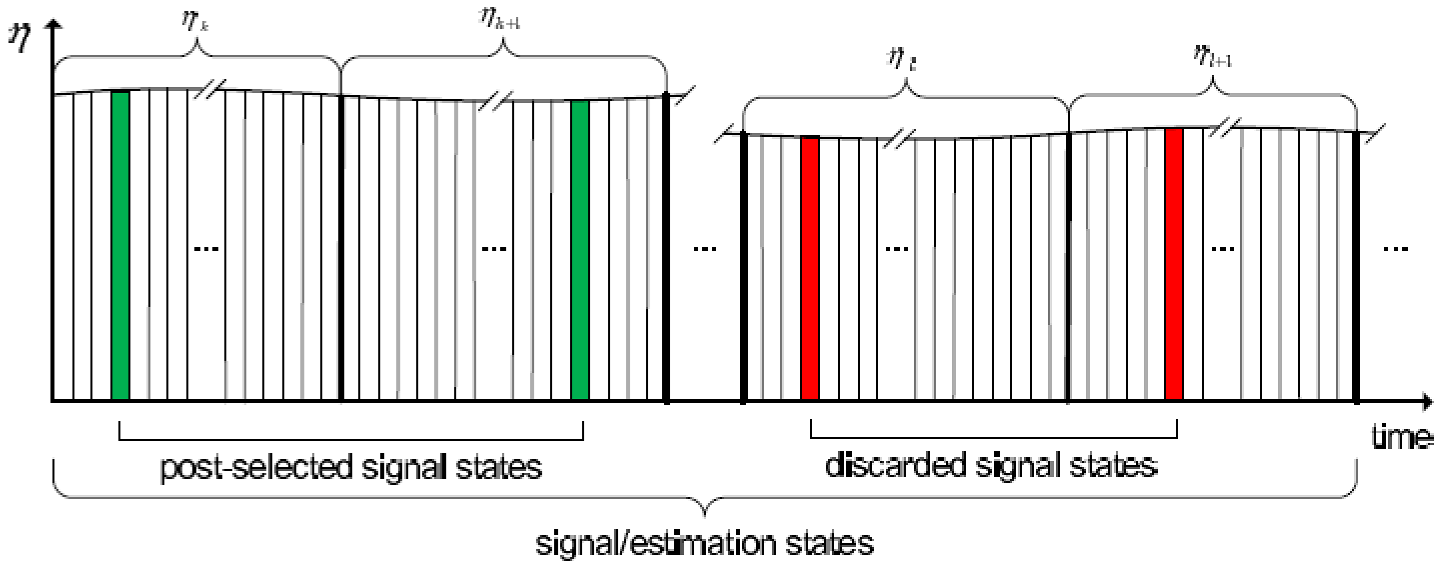
Security against collective attacks:



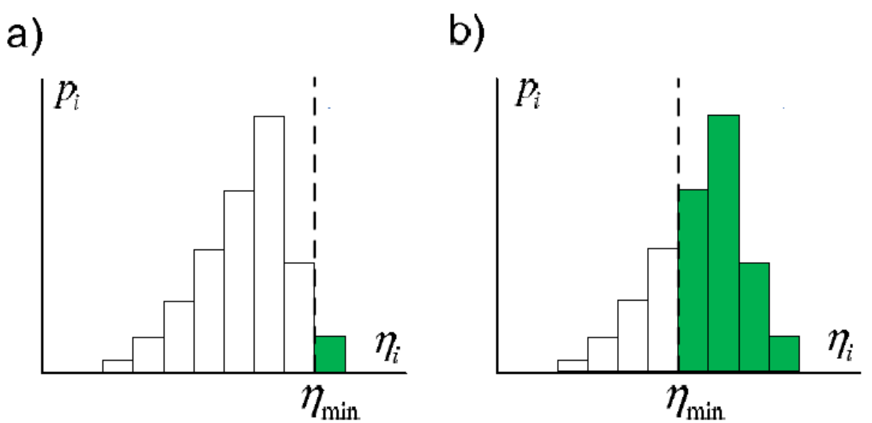
solid lines: no excess noise
dashed lines: excess noise $\chi = 1.2 \cdot 10^{-2}$

Post-selection of sub-channels

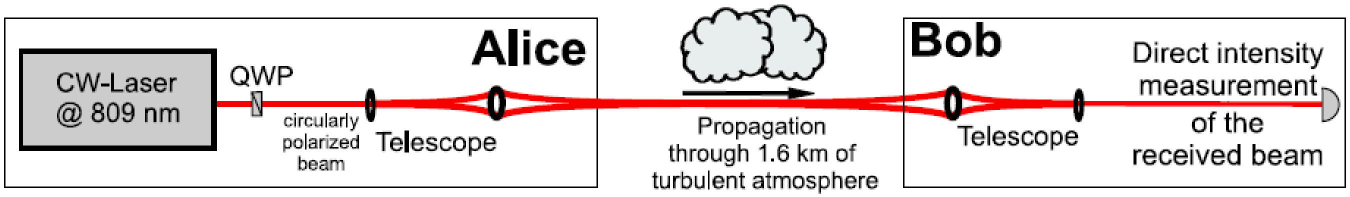
Post-selection time-flow:



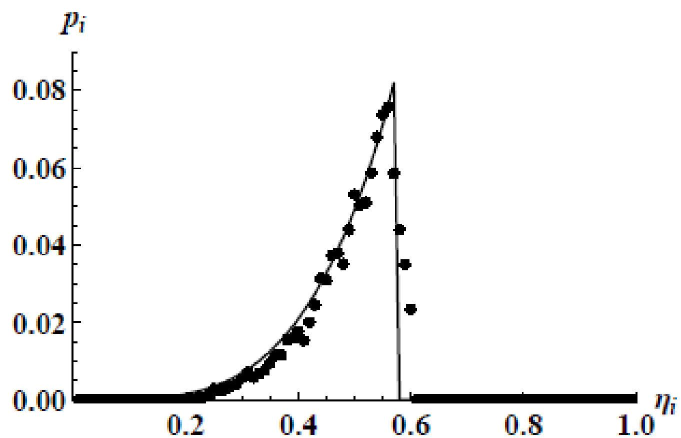
Post-selection of a single / multiple subchannels:



Real fading channel



Transmittance distribution obtained from a 1.6 km atmospheric link in Erlangen

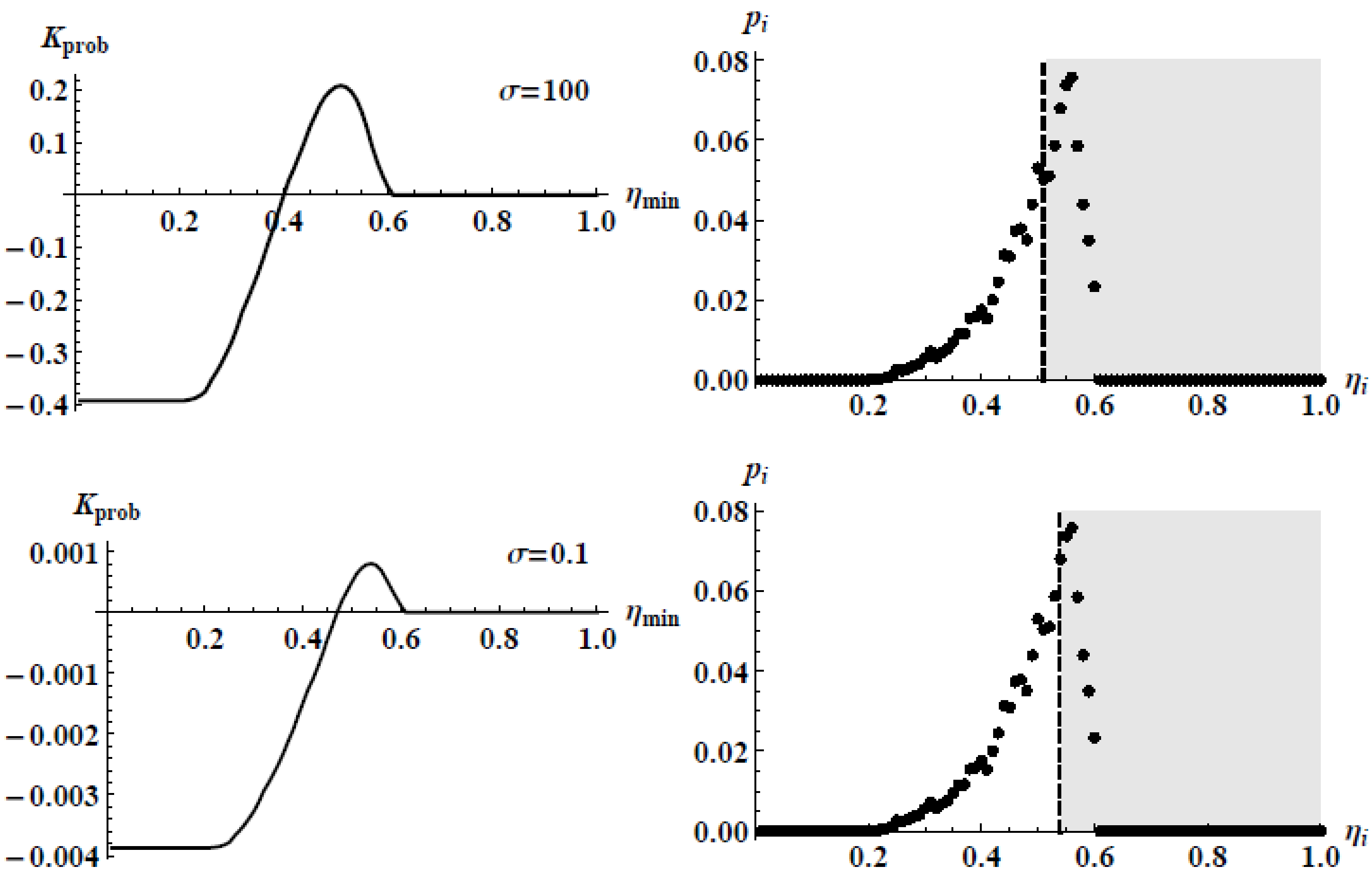


Sampling rate 150 kHz, bin size $\Delta\eta = 0.01$

Experimental distribution is well fitted by the log-normal.

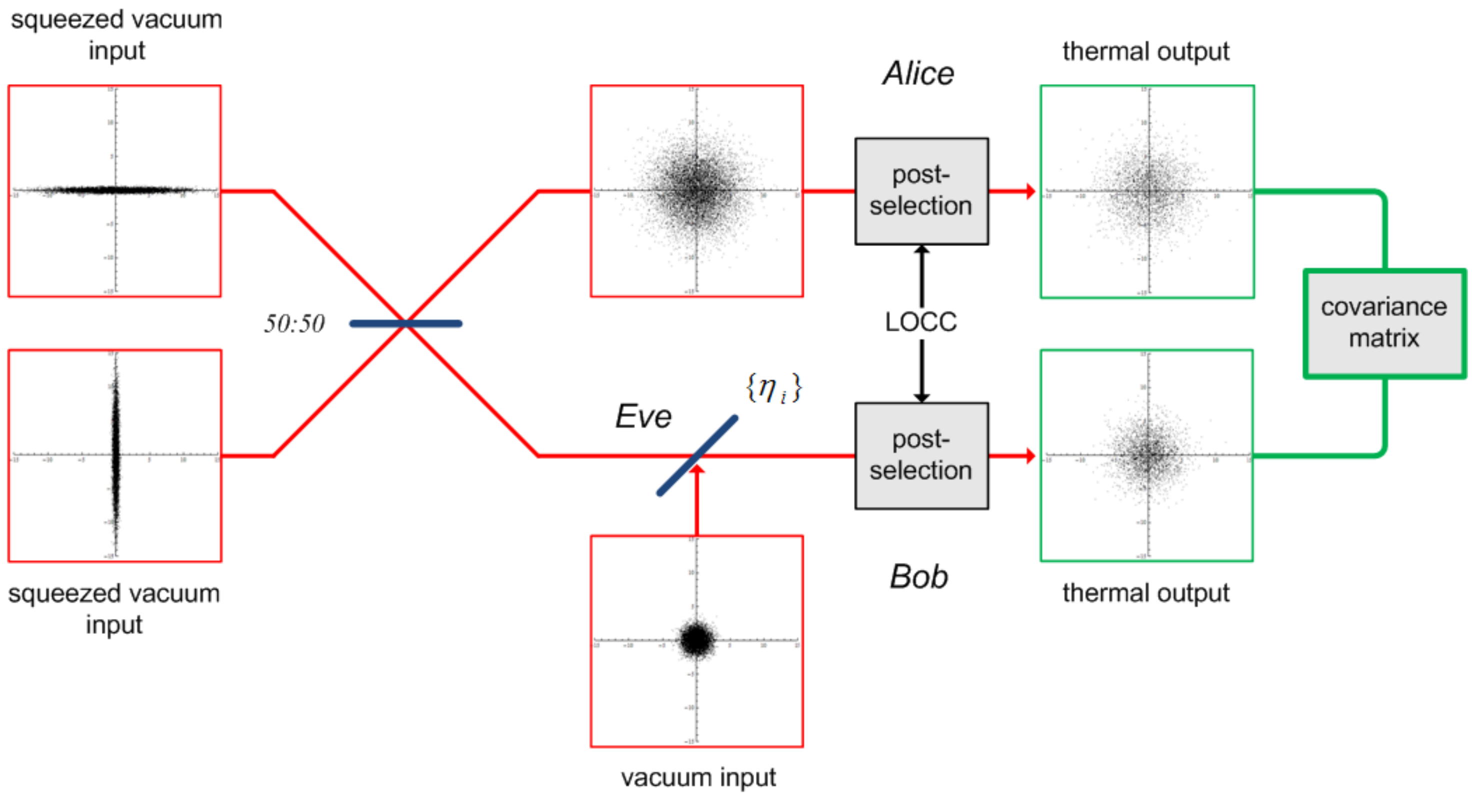
Channel is characterized by $\langle\sqrt{\eta}\rangle^2 \approx 0.492$ and $Var(\sqrt{\eta}) \approx 3 \cdot 10^{-3}$

Real fading channel



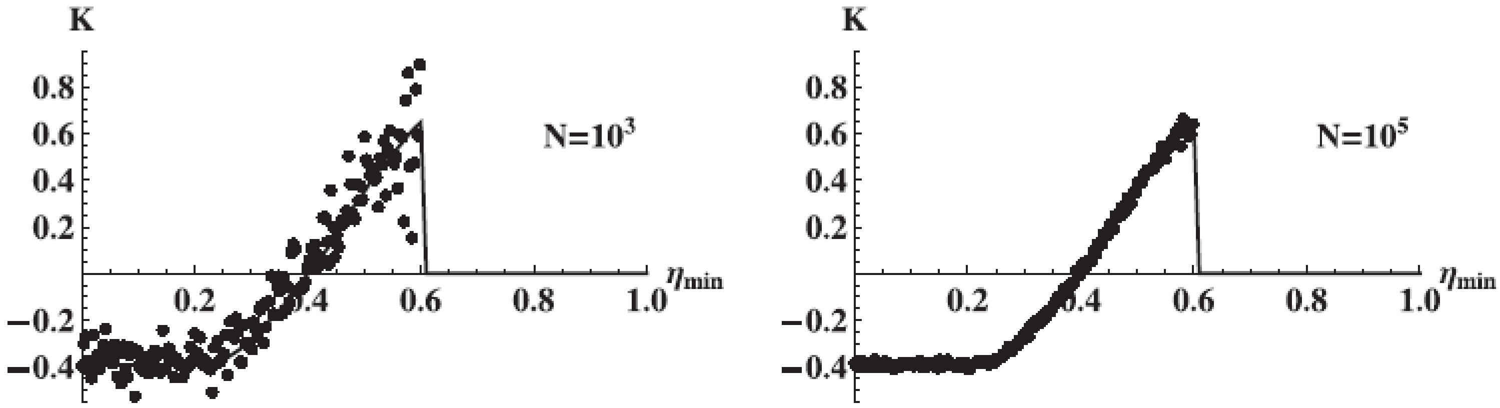
Effect of post-selection after the real fading channel on the security of the coherent-state protocol in terms of the weighted key rate (left). Corresponding optimal PS region is given at the right. Noise $\chi = 3.2 \cdot 10^{-2}$

Finite-size effects



Scheme for numerical modeling of the fading and post-selection effects.

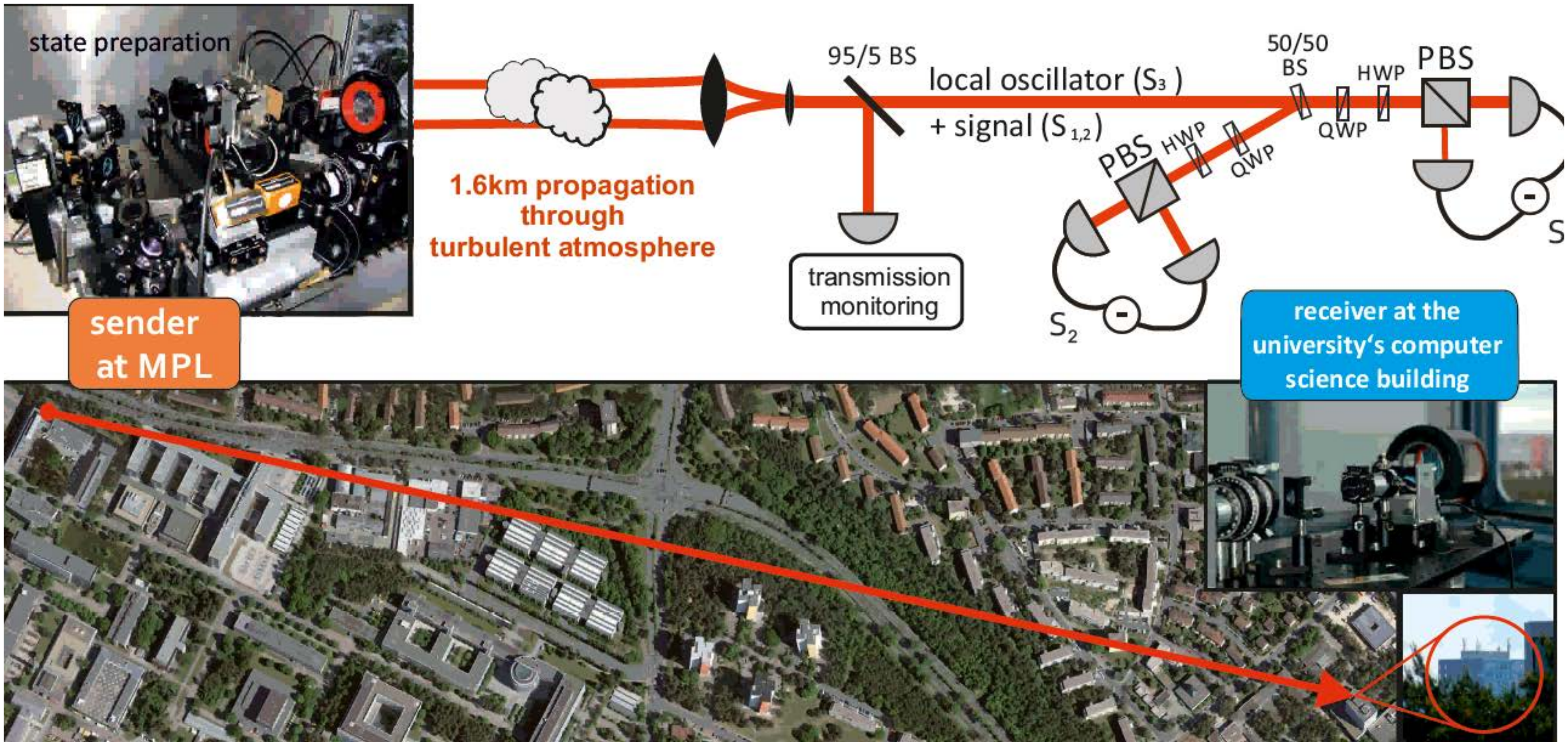
Finite-size effects



Effect of the finite ensemble size on the key rate upon post-selection.

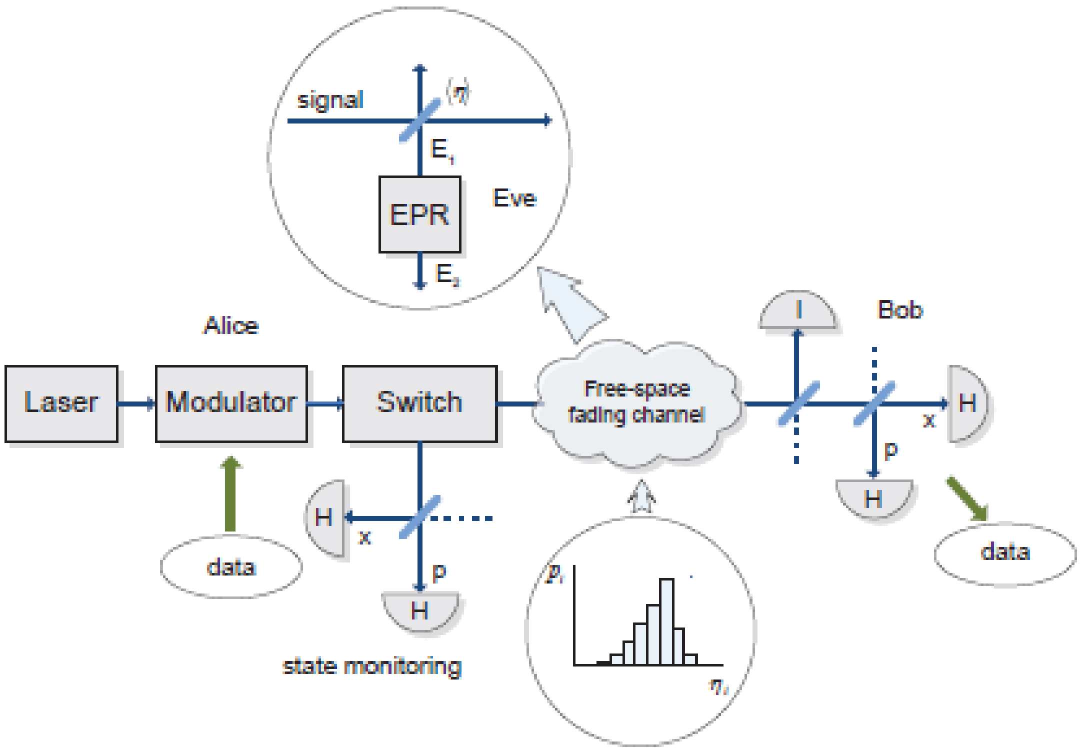
[VU, Heim, Peuntinger, Wittmann, Marquardt, Leuchs, Filip, New J. Phys., 14 093048 (2012)]

Proof-of-principle test



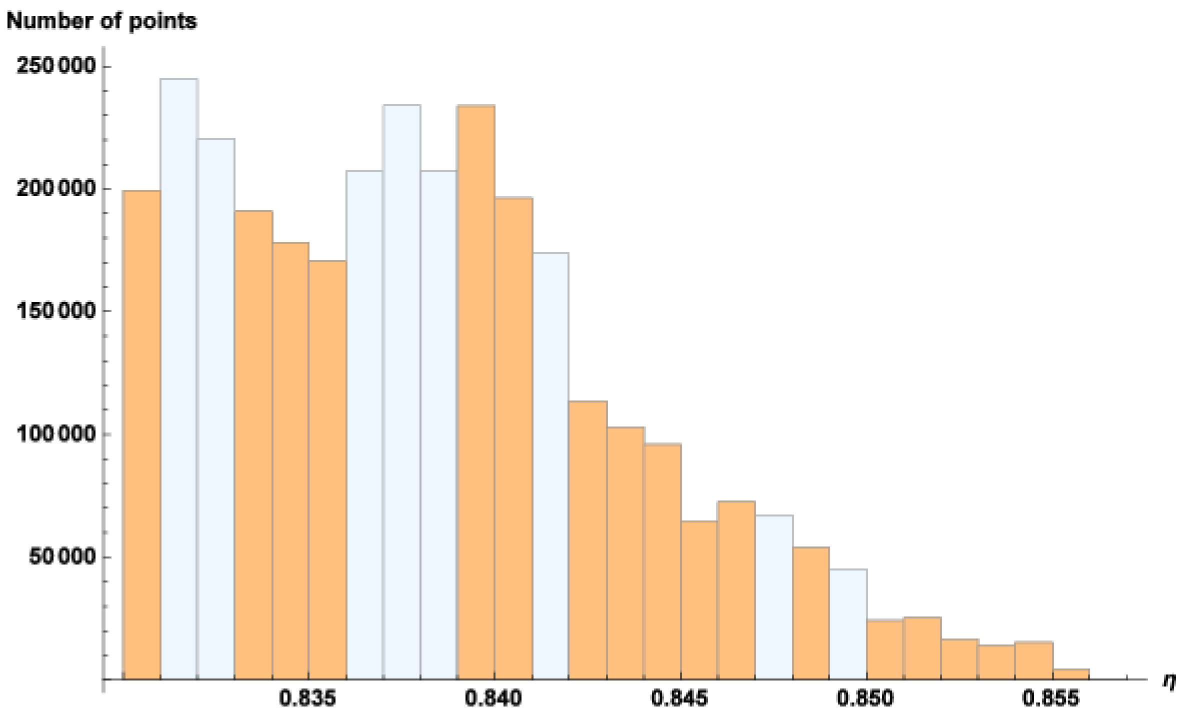
We illustrate the effect of sub-channel post-selection by testing Gaussian-modulated coherent-state CV QKD in the free-space link in Erlangen.

Proof-of-principle test



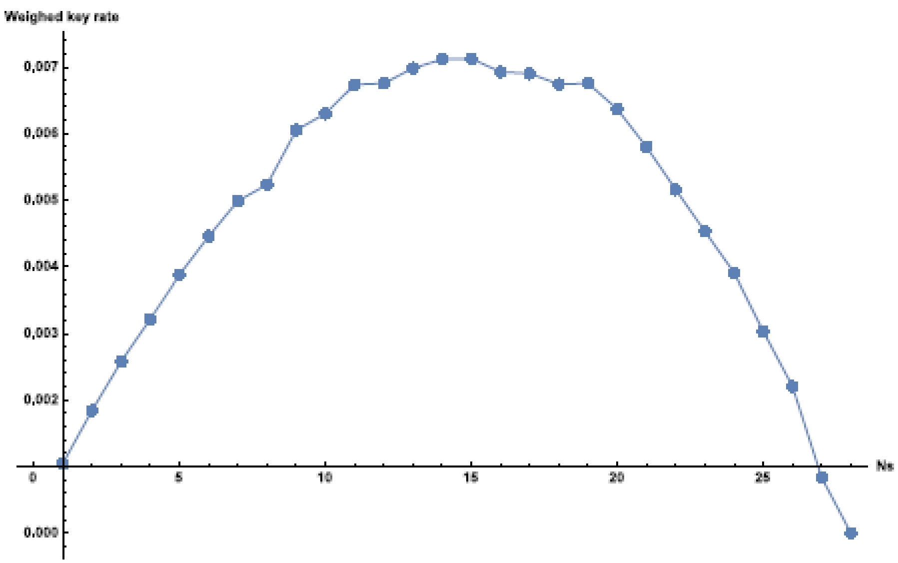
Sketch of the experiment with the Gaussian-modulated coherent states, free-space link and double-homodyne detection.

Proof-of-principle test



Sub-channels with the positive key rate (orange).

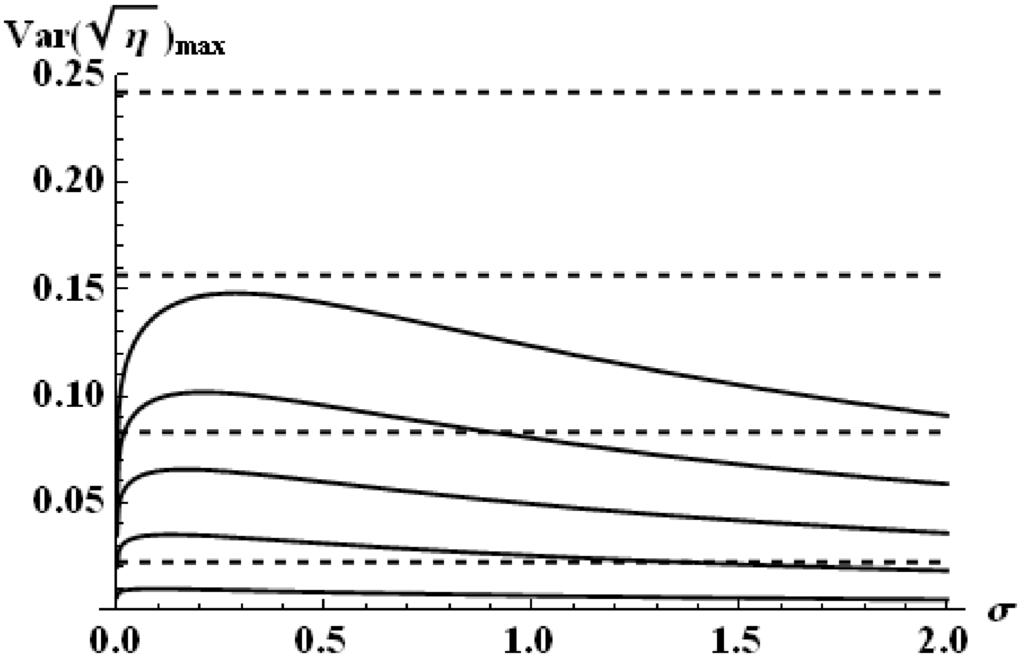
Proof-of-principle test



Lower bound of the key rate secure against collective attacks versus number of post-selected sub-channels.

Coming next

Realization of the squeezed-state protocol (following successful distribution of squeezing [Peuntinger et al. PRL 113, 060502 (2014)])



Coherent-state protocol (solid lines) and squeezed-state protocol (dashed lines) with -0.8 dB squeezing (V=1.2).

Summary

• Fading channels affect security of QKD protocols on the basis of the Gaussian states.

• States with the higher variance are more sensitive to fading, while presence of even small excess noise combined with fading strongly affects the states with lower variance.

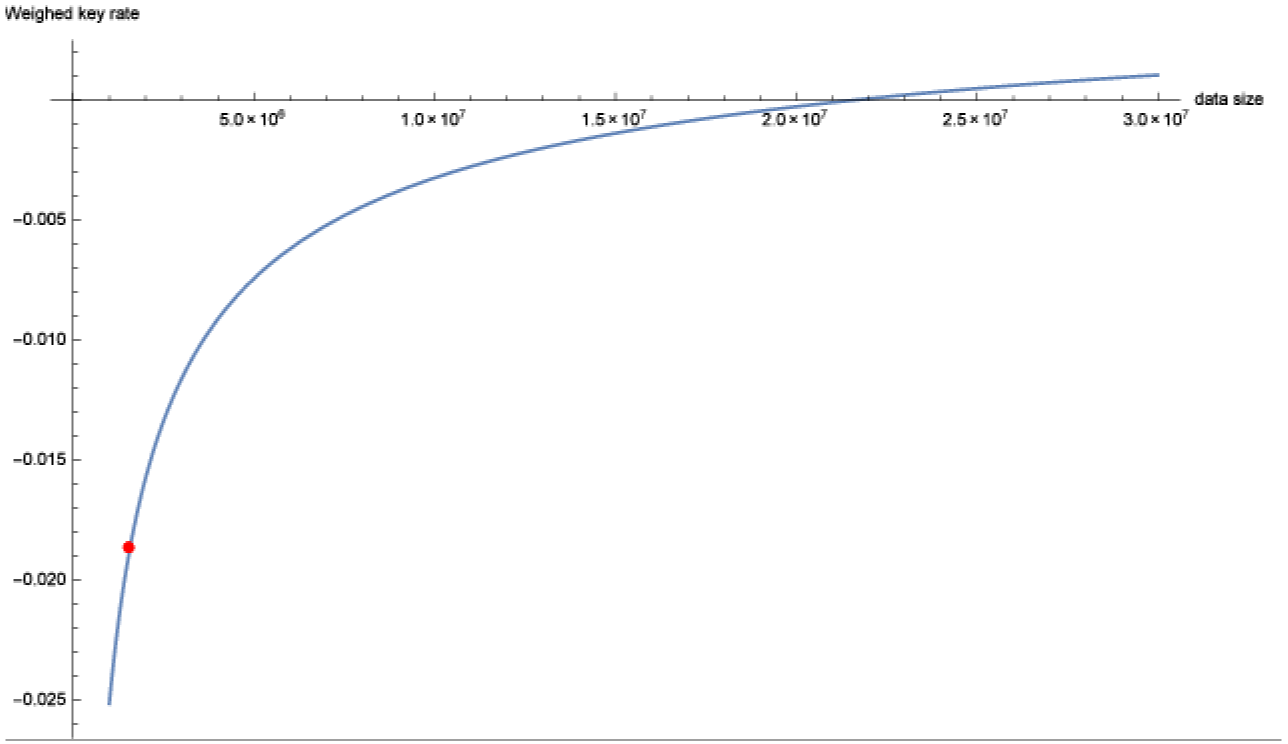
• Security can be restored by the use of post-selection.

• Alternatively, squeezed states can be used and are more robust to fading (even without sub-channel post-selection).

Thank you for the attention!

usenko@optics.upol.cz

Finite-size effects



Weighted key rate versus number of data points.