european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
INVESTMENTS IN EDUCATION DEVELOPMENT

Scientific visits to foreign research groups in 2013

Vladyslav C. Usenko

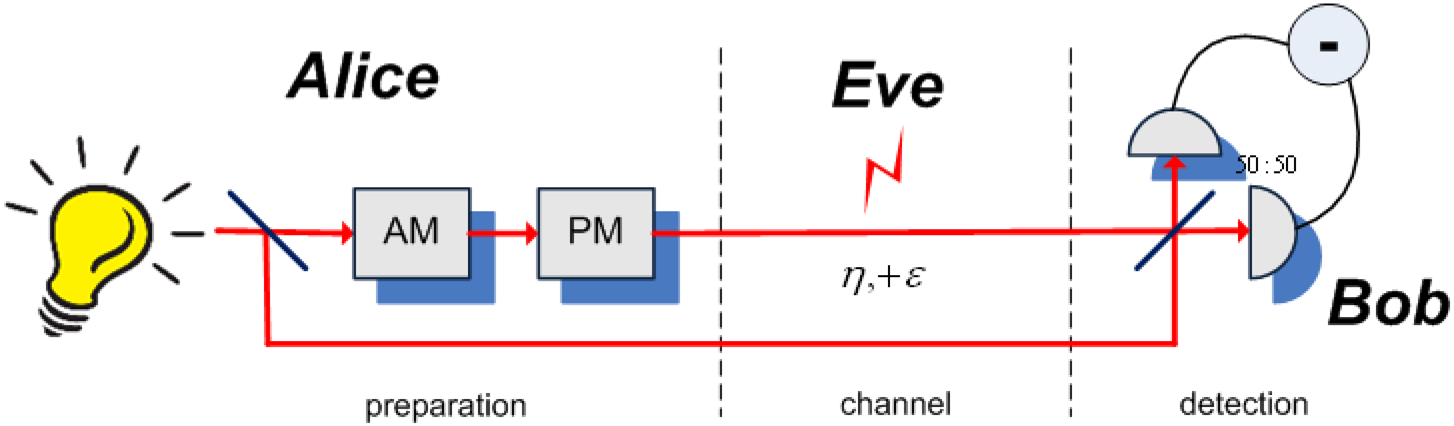
Department of Optics, Palacký University, Olomouc, Czech Republic

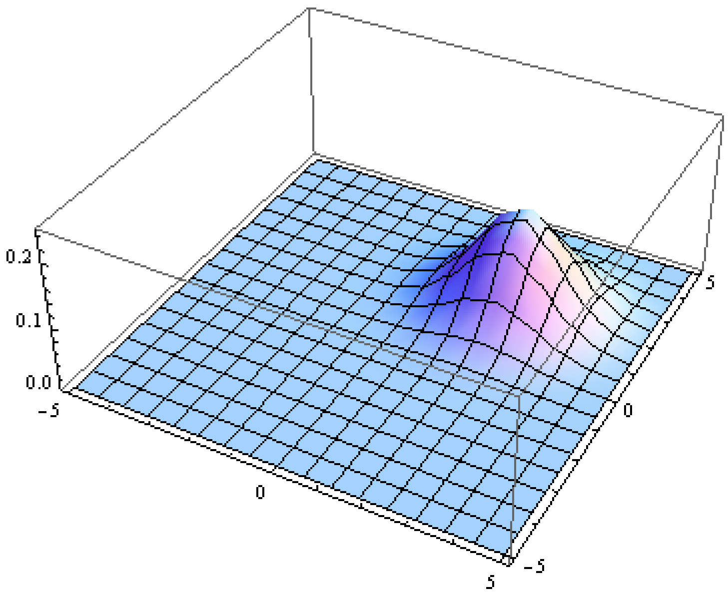
UPOL, 2013

Outline

- Introduction
- Single-quadrature CV QKD protocol (ENC Cachan, Univ. Paris-Sud)
- Weakly modulated squeezed states (DTU, Lyngby)
- Quantum key distribution over fading channels (MPI, Erlangen)

CV Quantum Key Distribution

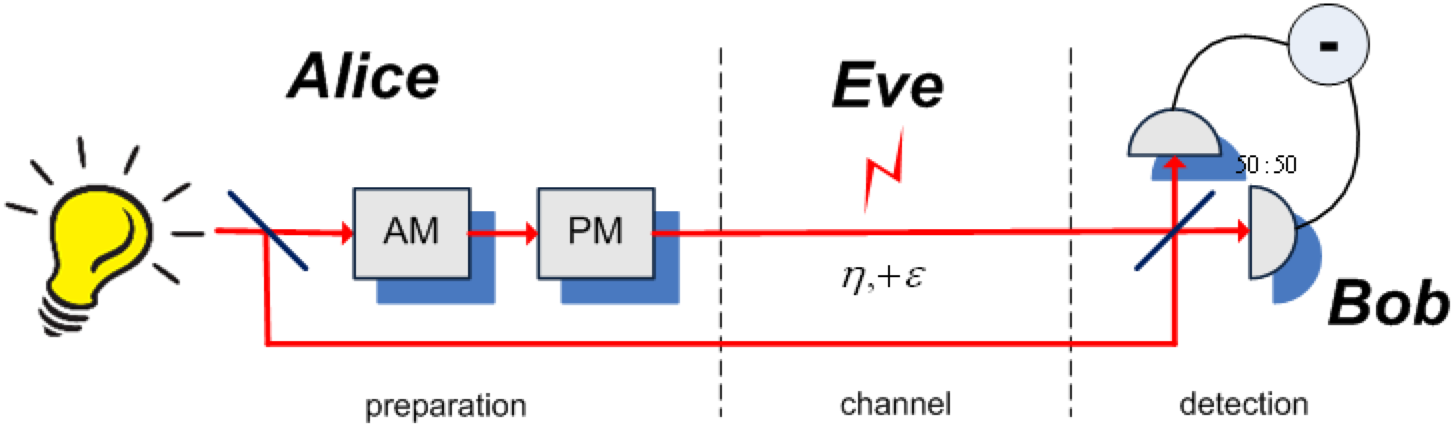


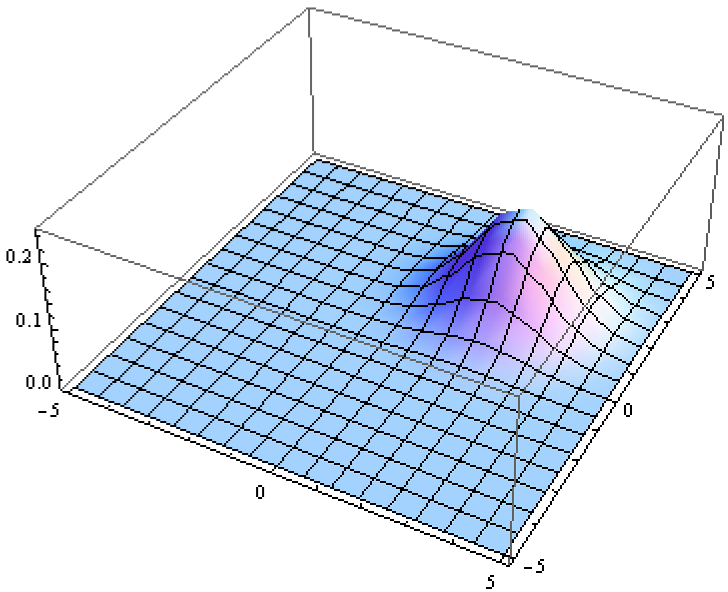


Coherent states-based protocol:
Laser source, modulation

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

CV Quantum Key Distribution

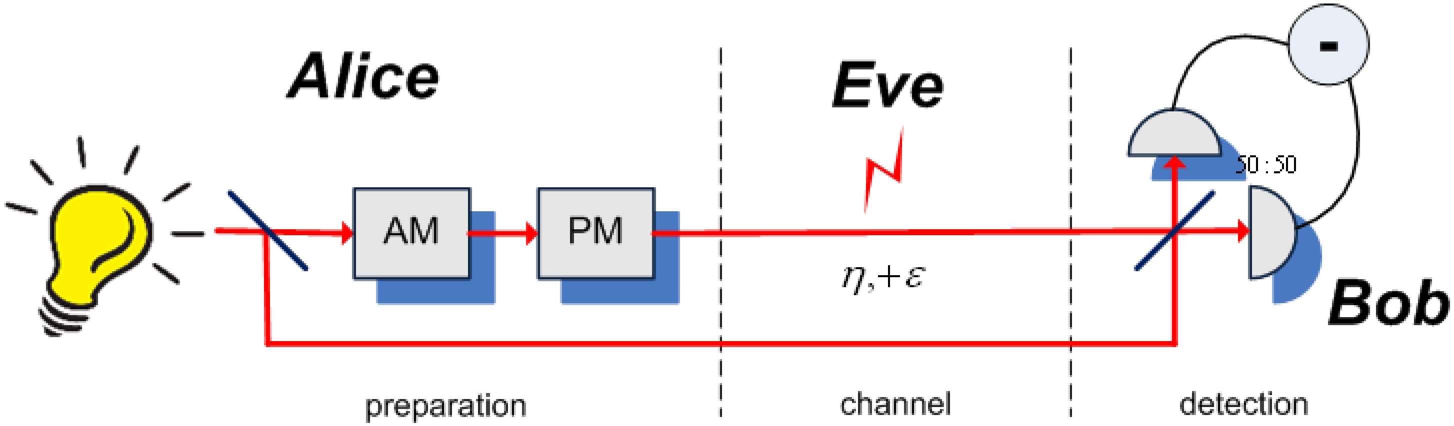


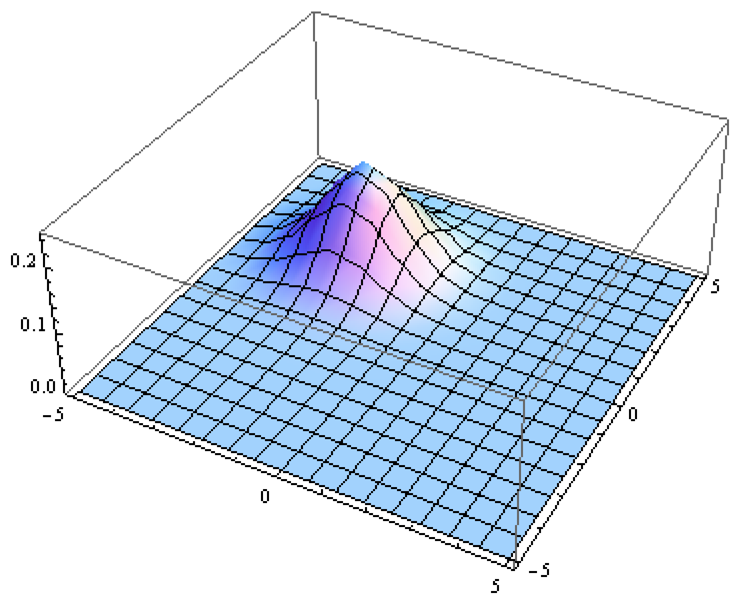


Coherent states-based protocol:

•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

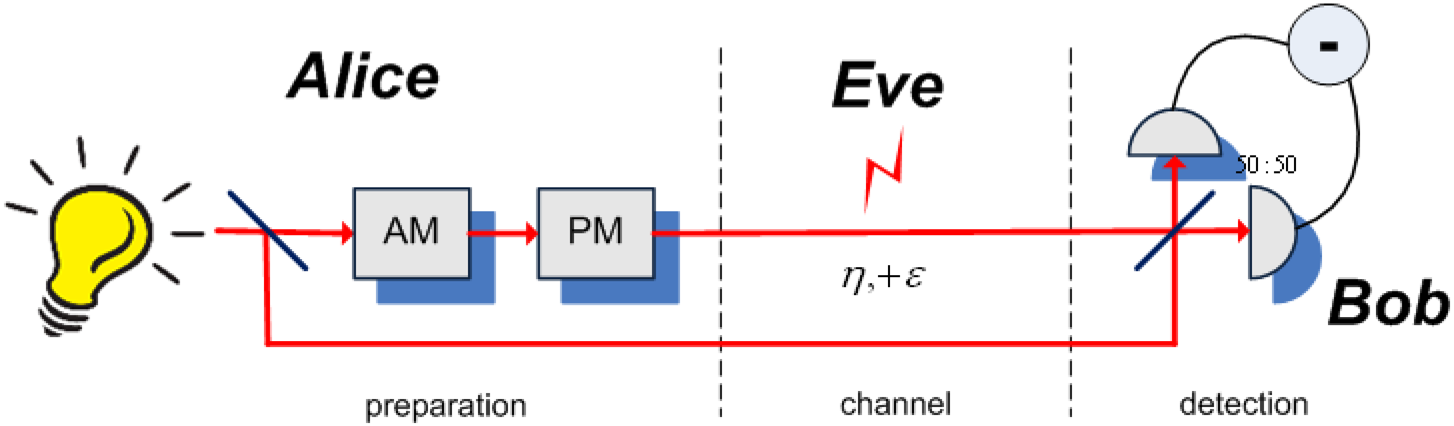


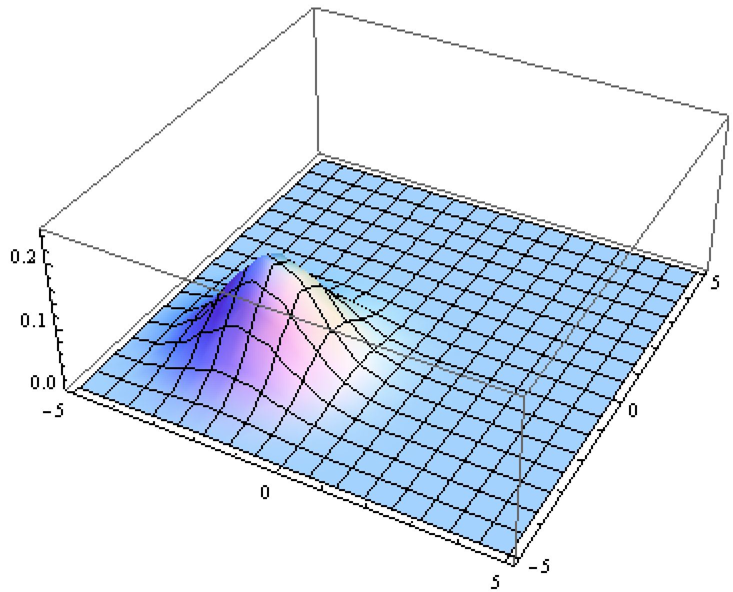


Coherent states-based protocol:

- 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

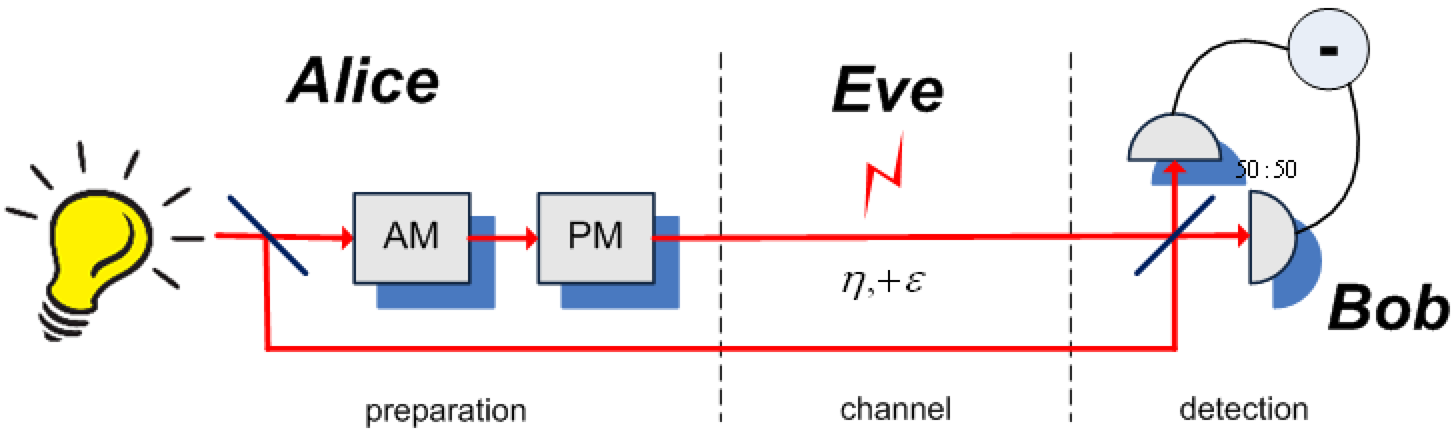


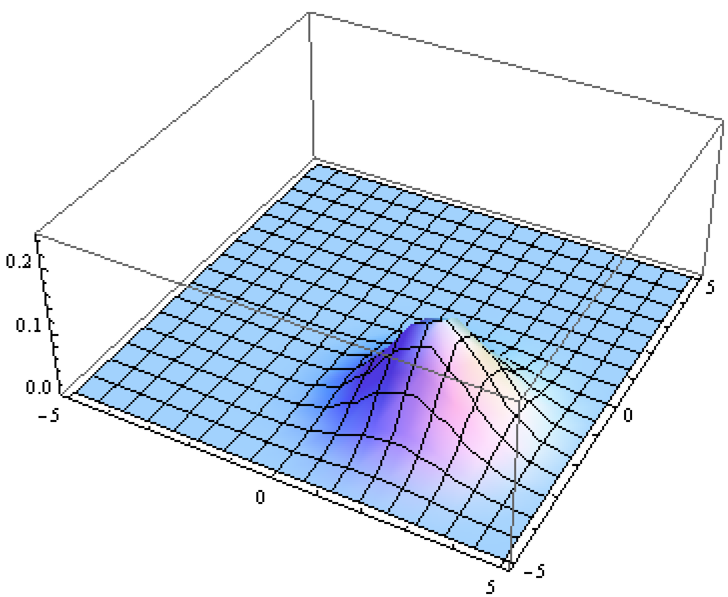


Coherent states-based protocol:

- 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

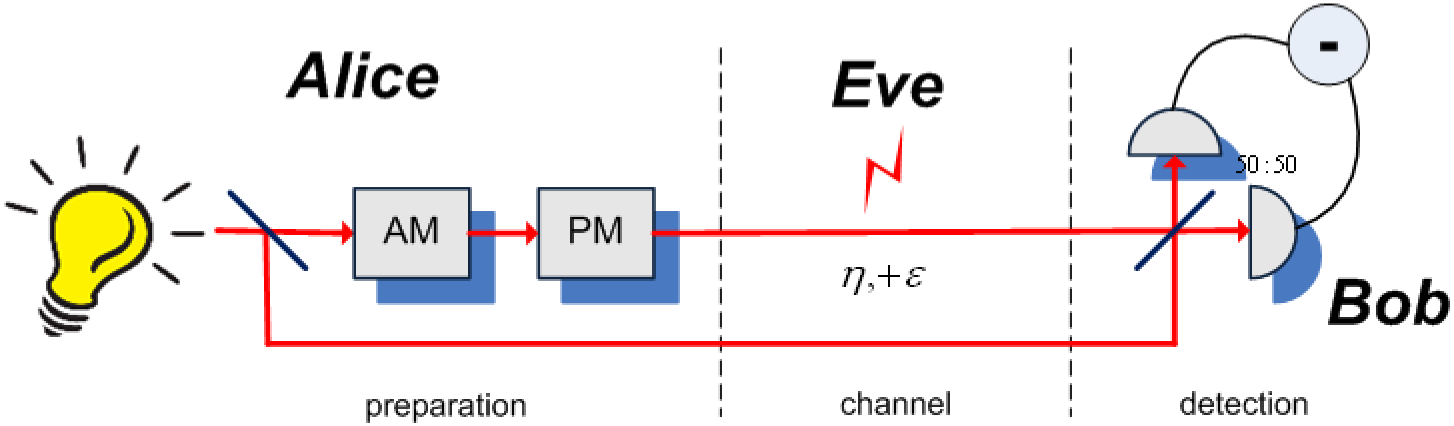


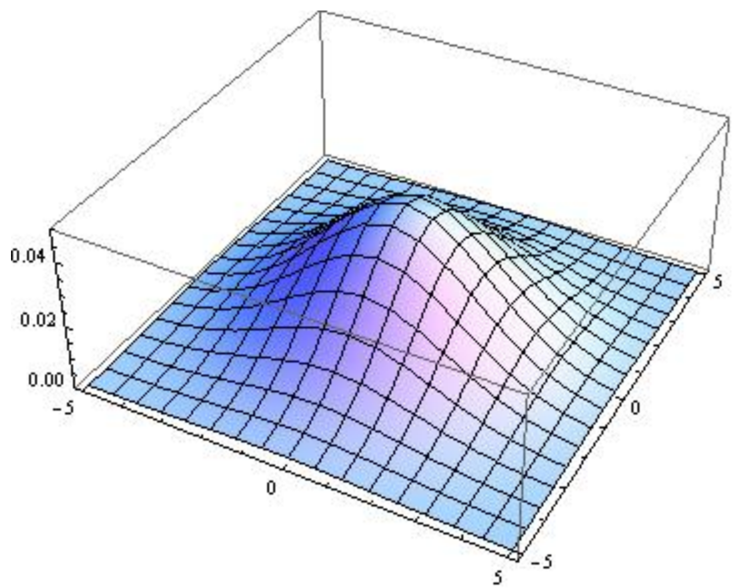


Coherent states-based protocol:

- 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



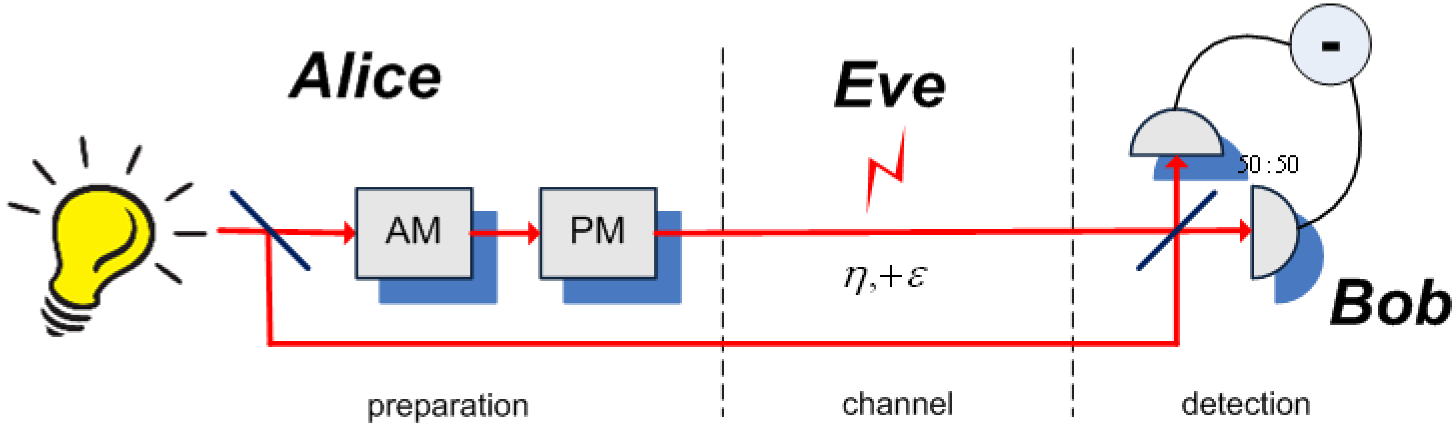


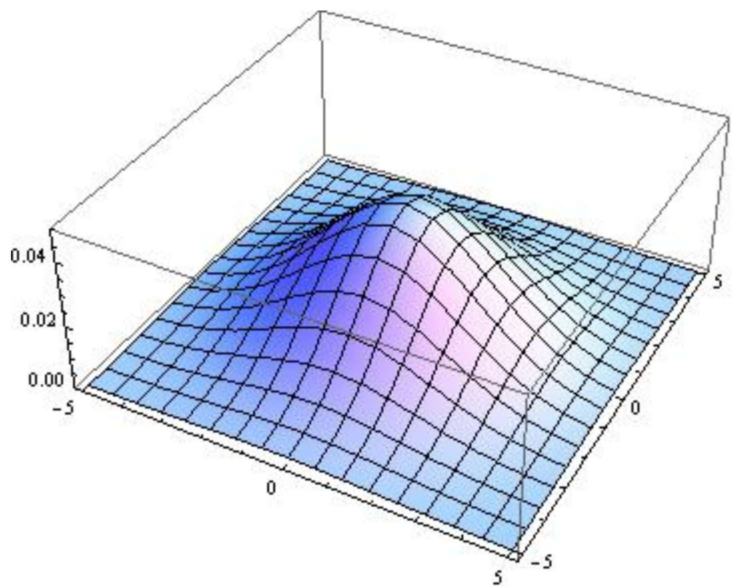
Mixture

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





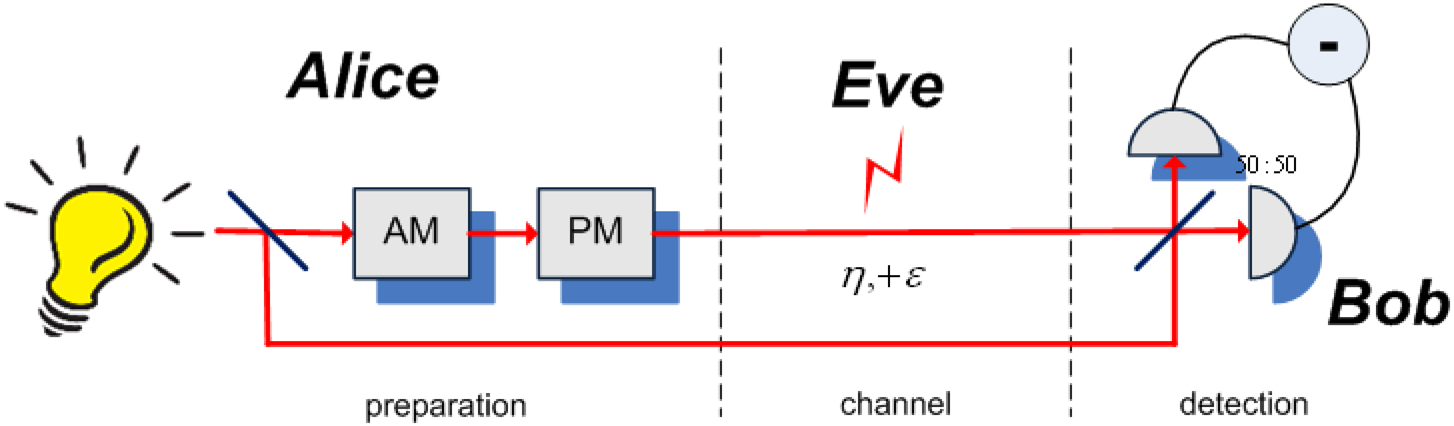
Mixture

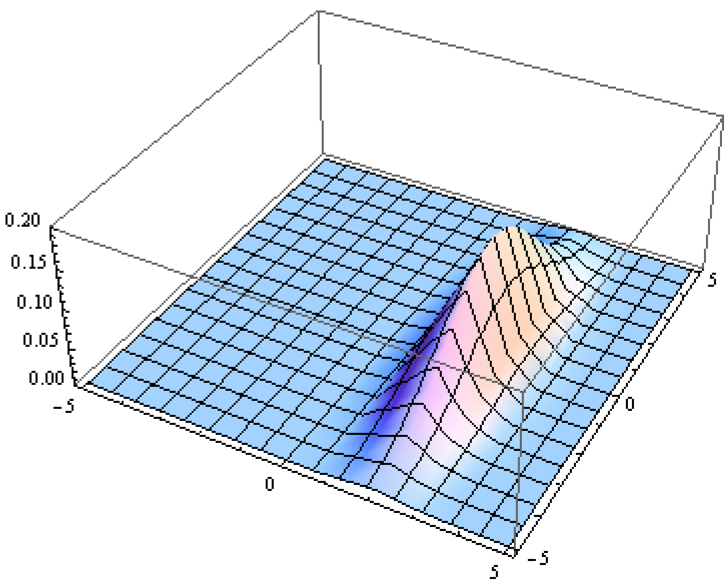
Coherent states-based protocol:

Achievements: 25 km, 2 kbps
J. Lodewyck et al., PRA 76, 042305 (2007)

Recent: 80 km
P.Jouguet et al., arXiv:1210.6216 (Nature Photonics 2013)

CV Quantum Key Distribution

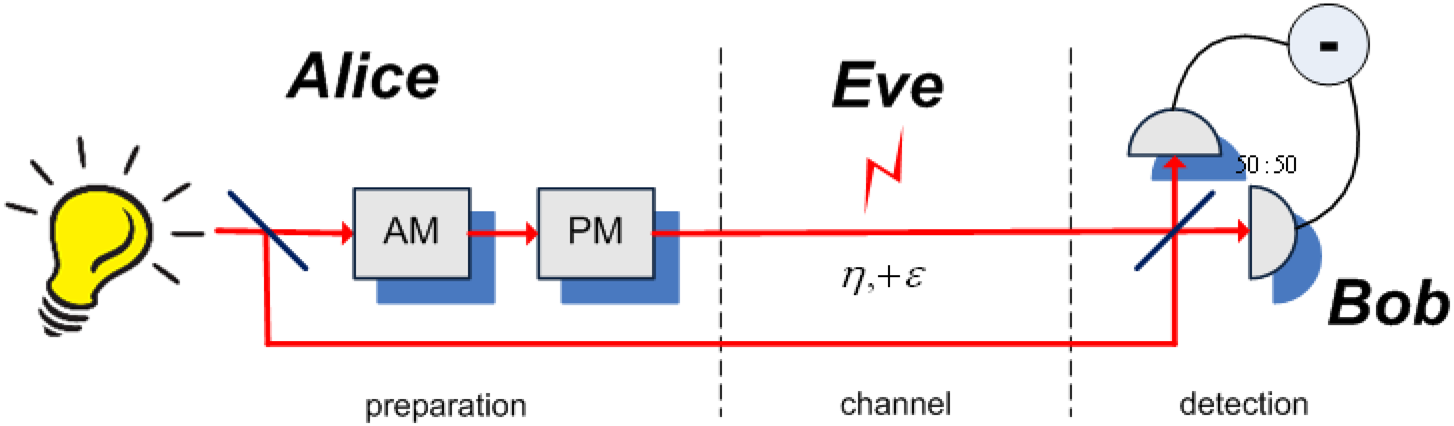


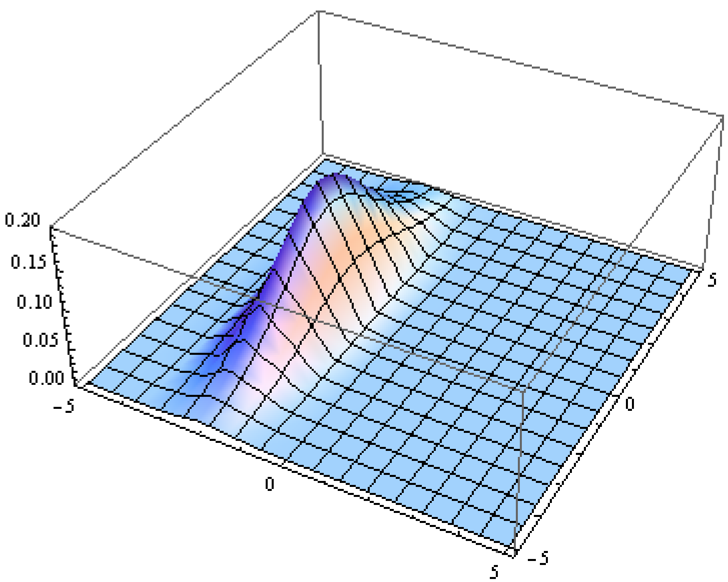


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- Alice generates a Gaussian random variable **a**
- Alice prepares a squeezed state, displaced by **a**
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

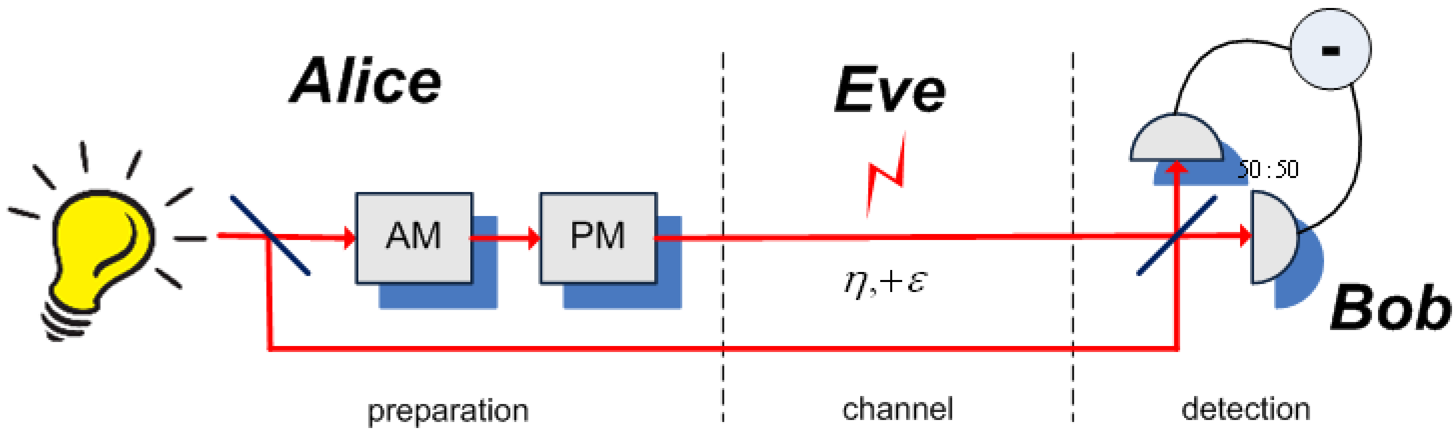


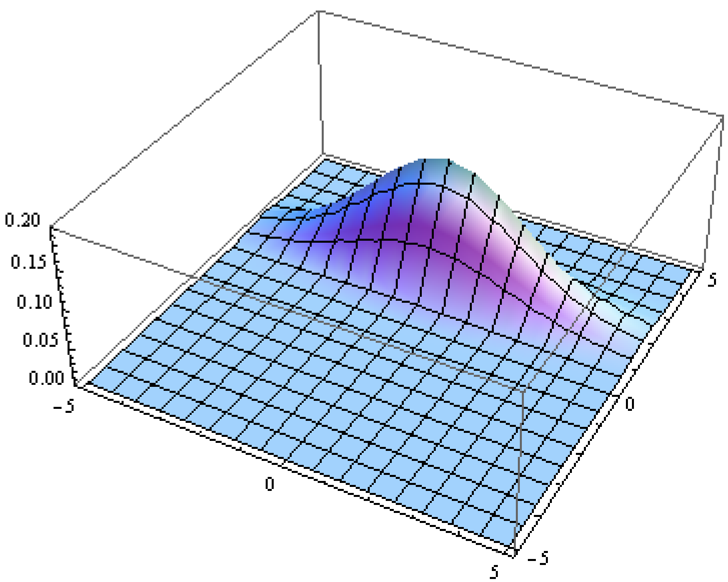


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- Alice generates a Gaussian random variable **a**
- Alice prepares a squeezed state, displaced by **a**
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

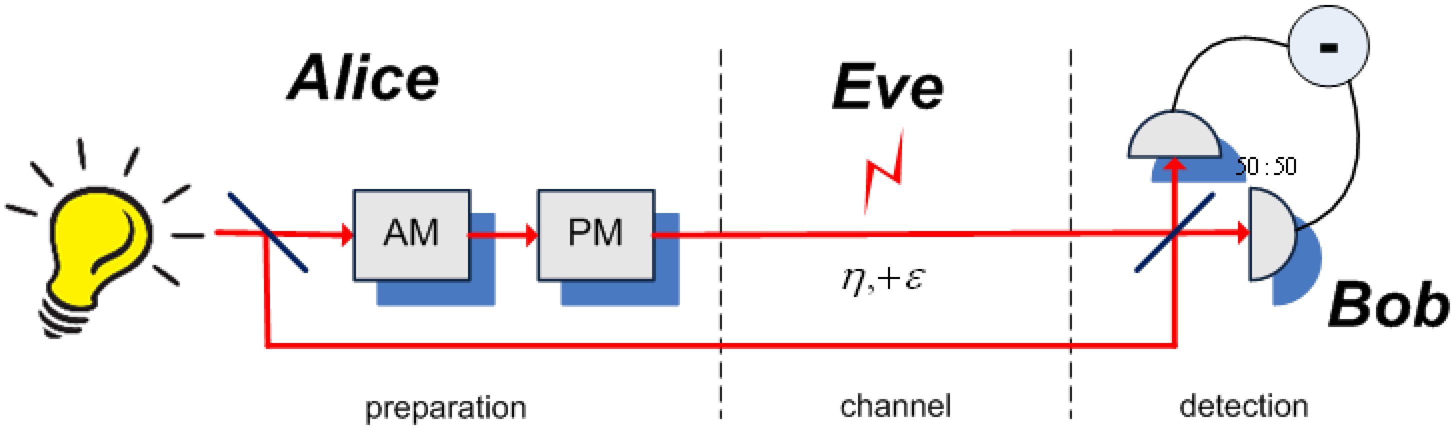


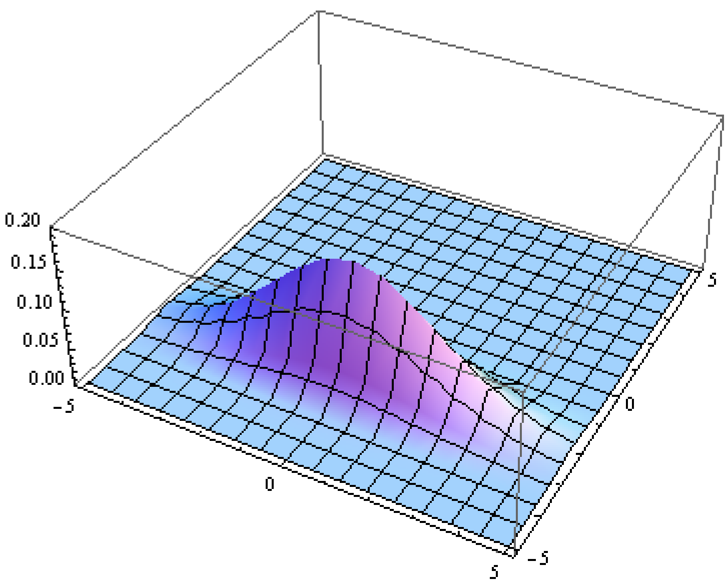


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- Alice generates a Gaussian random variable **a**
- Alice prepares a squeezed state, displaced by **a**
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

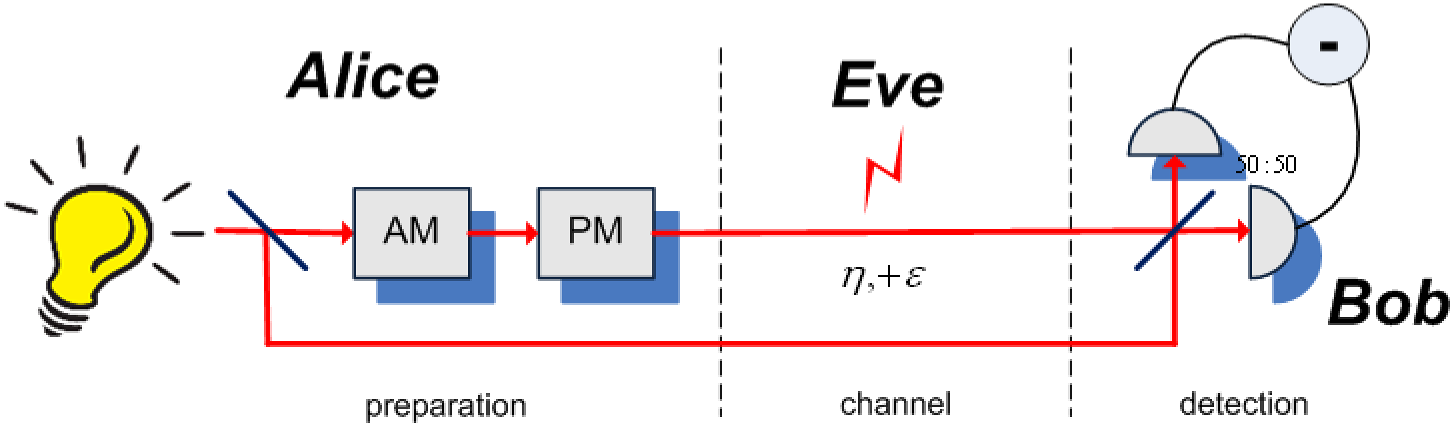


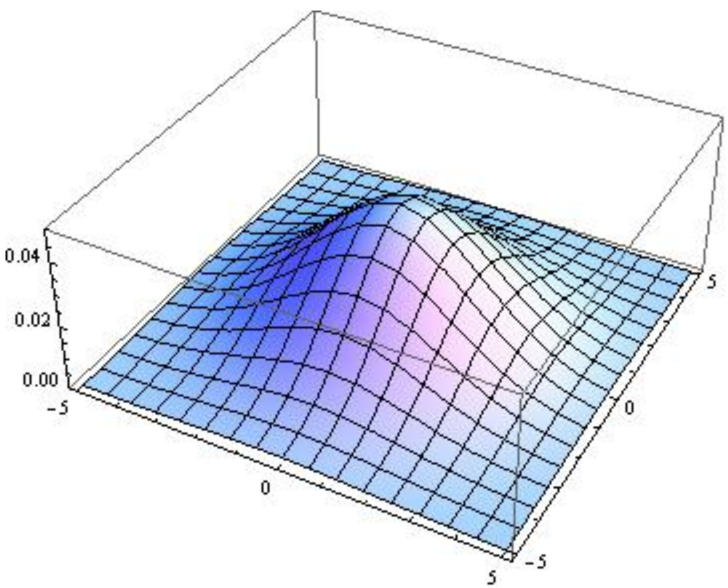


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- Alice generates a Gaussian random variable **a**
- Alice prepares a squeezed state, displaced by **a**
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution



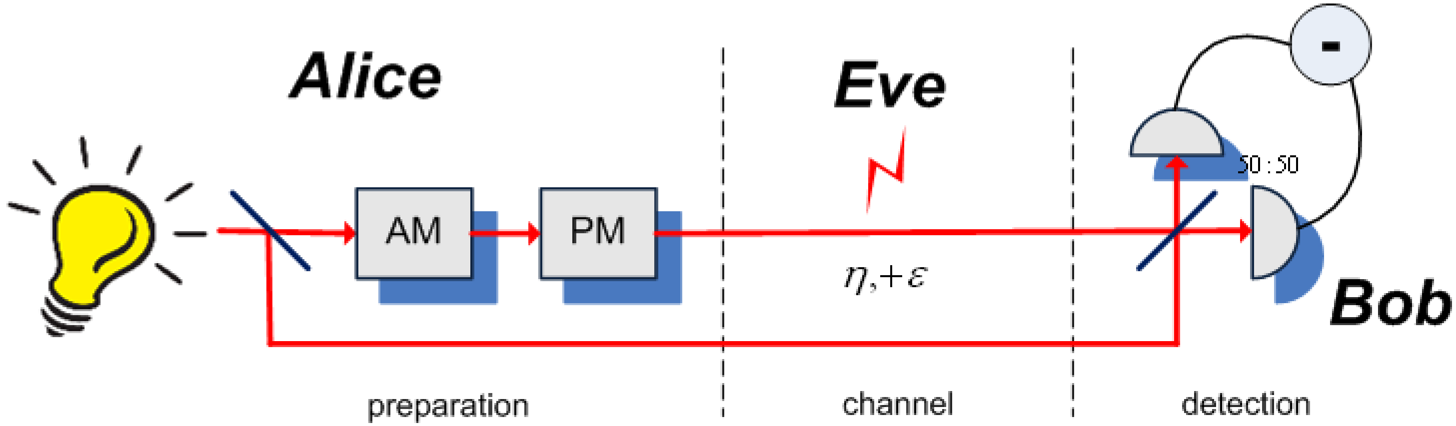


Mixture

Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- Alice generates a Gaussian random variable **a**
- Alice prepares a squeezed state, displaced by **a**
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution



Is unsecure for > 50% channel loss

Classical Information →

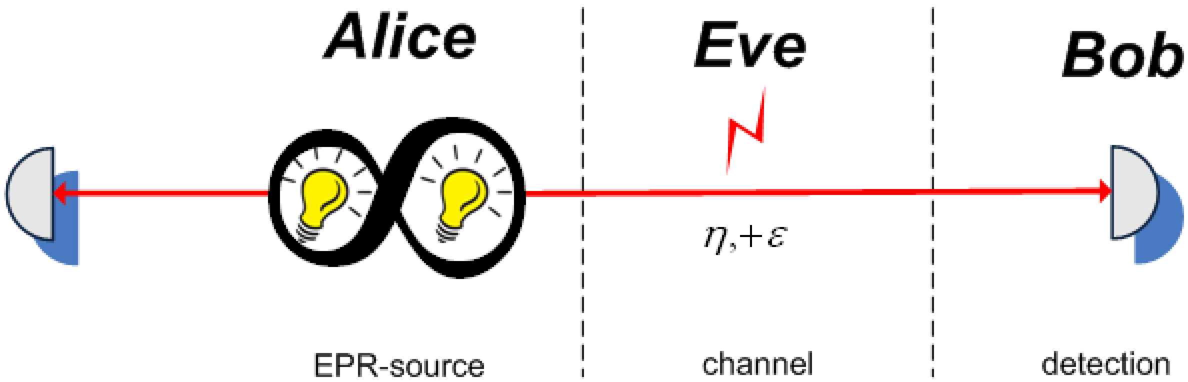
Direct reconciliation

Tolerates any pure loss

← Classical Information

Reverse reconciliation

CV QKD: entangled-based

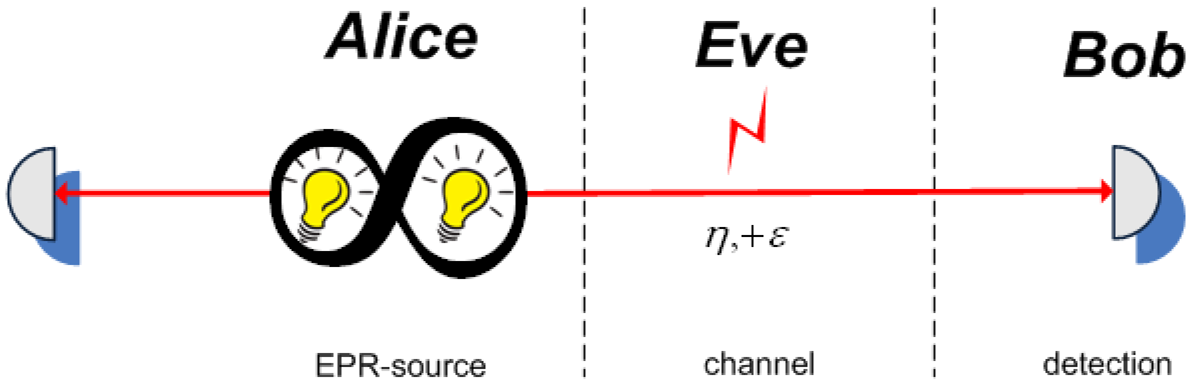


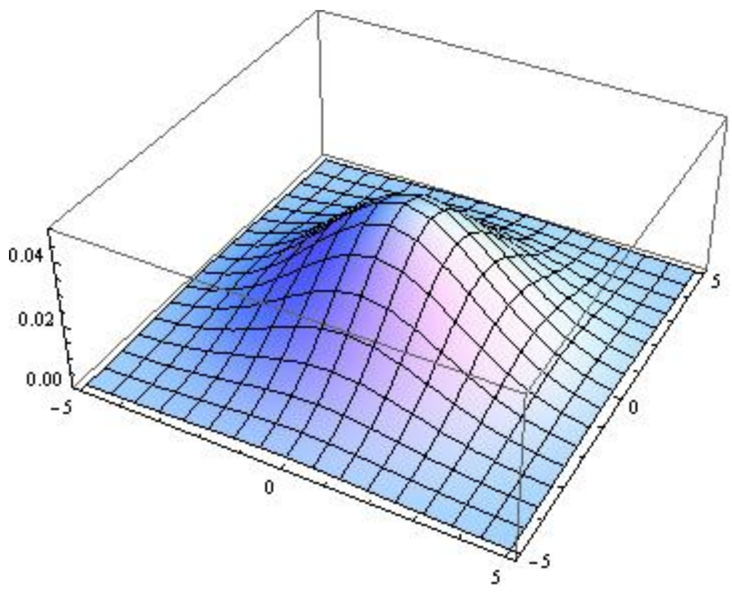
Two-mode squeezed vacuum state:

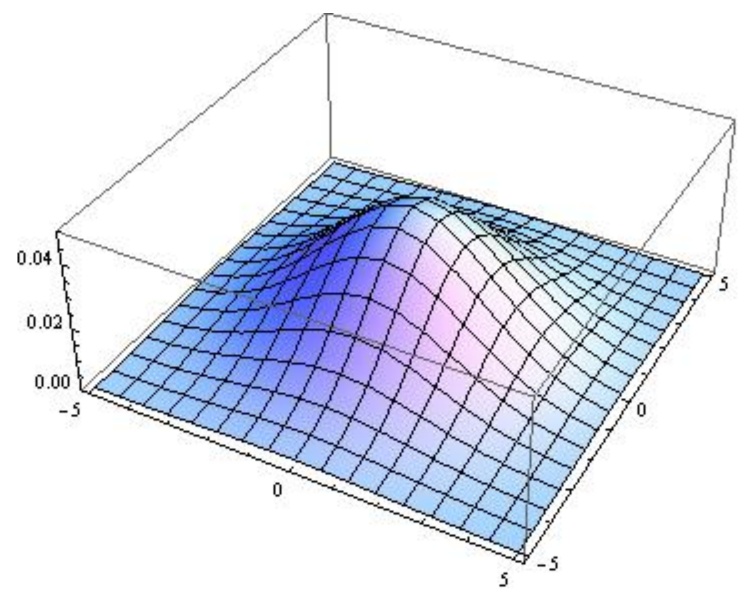
$$|x\rangle\rangle = \sqrt{(1-x^2)}\sum_n x^n \, |n,n\rangle\rangle$$

$$x \in \mathbb{C} \text{ and } 0 \leq |x| \leq 1$$

CV QKD: entangled-based

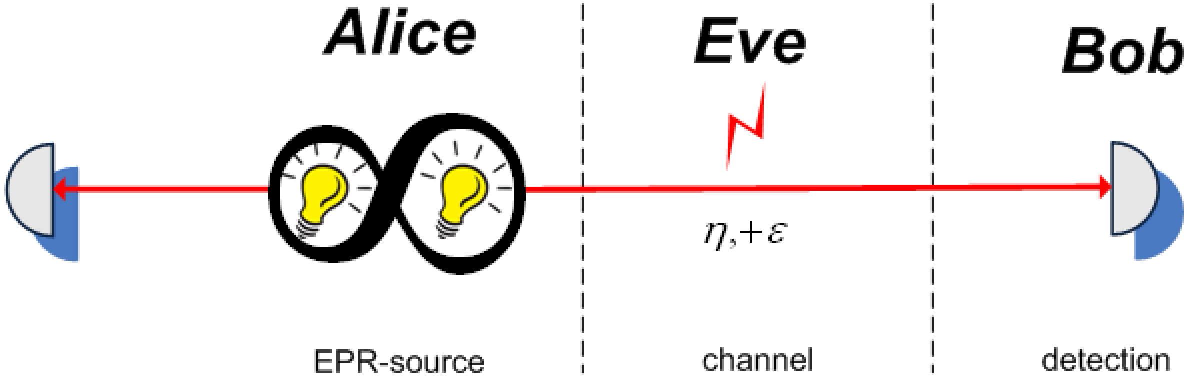




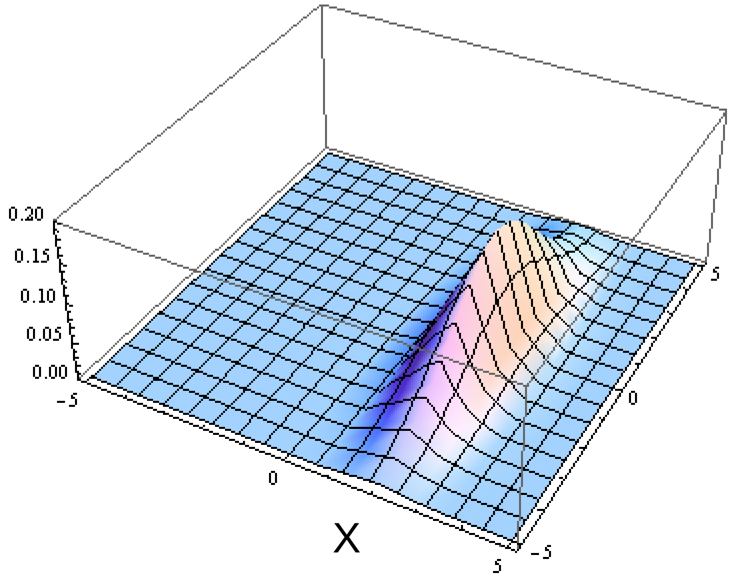


Before homodyne measurement

CV QKD: entangled-based

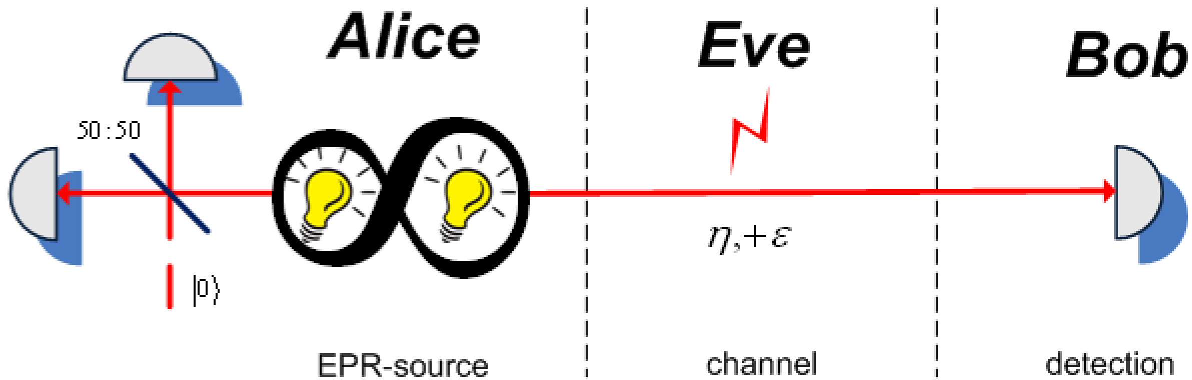


X

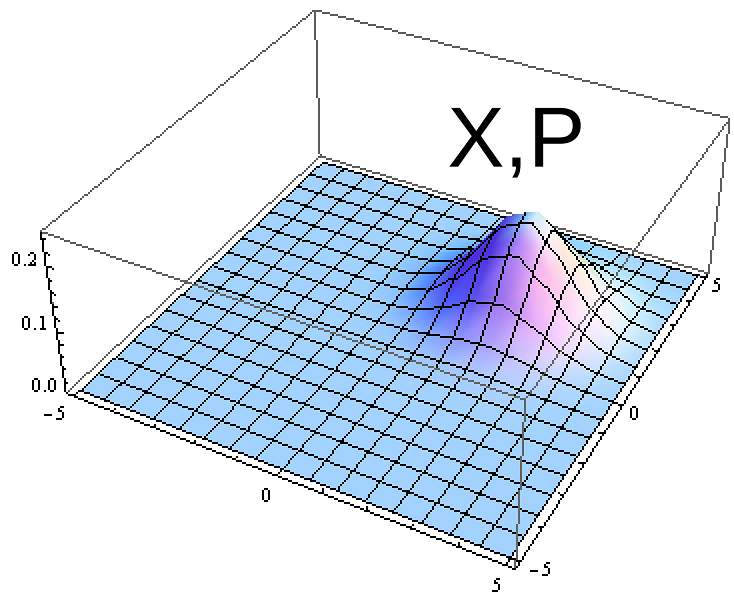


After homodyne measurement

CV QKD: entangled-based

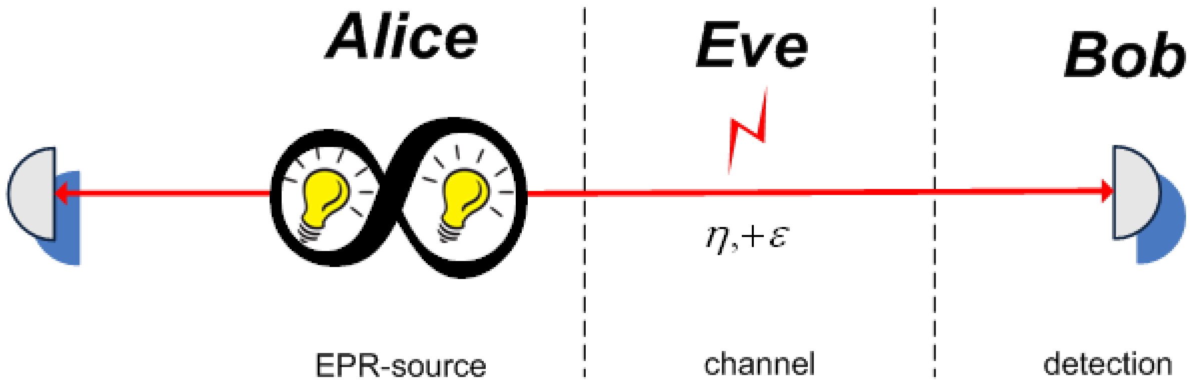


X,P



After heterodyne measurement

CV QKD: entangled-based



Advantages:

• Complete theoretical description of coherent/squeezed protocol

• Potential scalability

CV Quantum key distribution: security

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

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

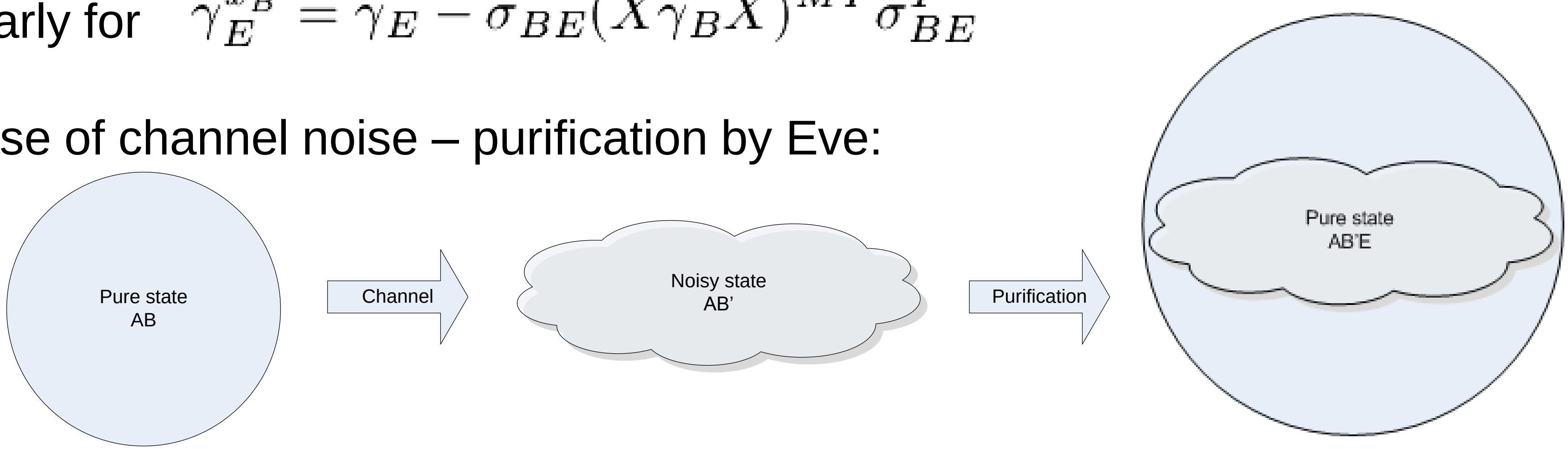
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

computation: $S_E = \sum_i G\left(\frac{\lambda_i - 1}{2}\right)$, $G(x) = (x+1)\log_2(x+1) - x\log_2 x$

λ_i - symplectic eigenvalues of the covariance matrix γ_E ,

similarly for $\gamma_E^{x_B} = \gamma_E - \sigma_{BE}(X\gamma_B X)^{MP}\sigma_{BE}^T$

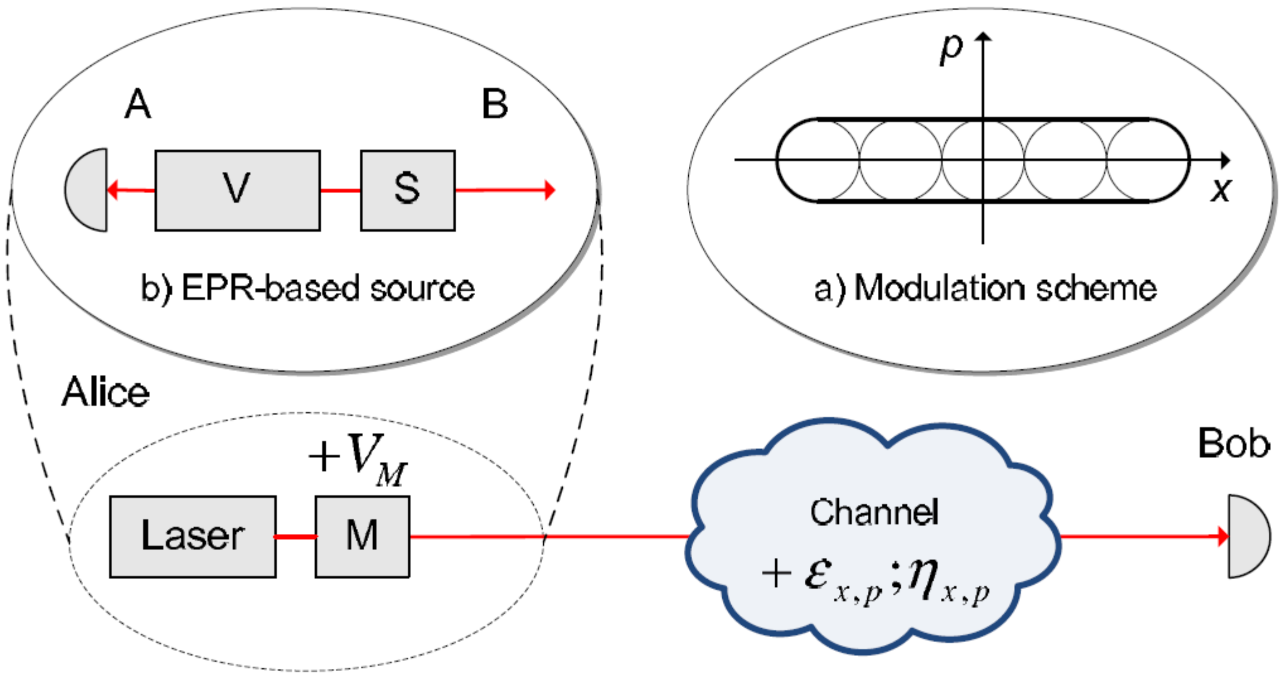
In case of channel noise – purification by Eve:



Single-quadrature protocol

Project accomplished during the visits to ENS Cachan and Univ. Paris-Sud. (group of Dr. Grosshans)

The scheme



Scheme of the single-quadrature modulation protocol

Theory of the protocol

$$\gamma_{AB} = \begin{bmatrix} V & 0 & \sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\frac{V^2-1}{V}} \\ \sqrt{V(V^2-1)} & 0 & V^2 & 0 \\ 0 & -\sqrt{\frac{V^2-1}{V}} & 0 & 1 \end{bmatrix}$$

$$\gamma'_{AB} = \begin{bmatrix} \sqrt{1+V_M} & 0 & \sqrt{\eta_x V_M}(1+V_M)^{\frac{1}{4}} & 0 \\ 0 & \sqrt{1+V_M} & 0 & C_p \\ \sqrt{\eta V_M}(1+V_M)^{\frac{1}{4}} & 0 & 1+\eta_x(V_M+\epsilon_x) & 0 \\ 0 & C_p & 0 & V_p^B \end{bmatrix}$$

Effective covariance matrices prior to and after the channel

$$\gamma_{A|x_B} = \begin{bmatrix} \frac{\sqrt{V_M+1}(1+\eta_x\epsilon_x)}{1+\eta_x(V_M+\epsilon_x)} & 0 \\ 0 & \sqrt{1+V_M} \end{bmatrix}$$

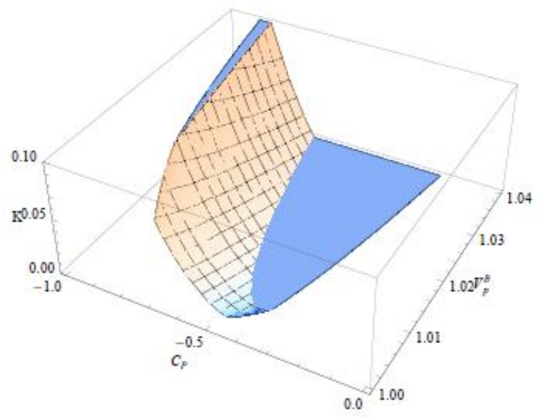
Conditional covariance matrix

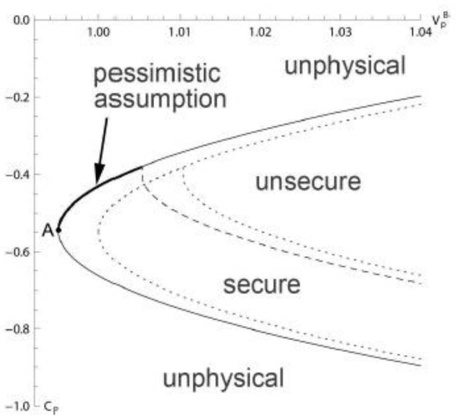
Theory of the protocol

$$(C_p - C_0)^2 \leq \frac{V_M}{(1+V_M)^{\frac{1}{2}}}(1-\eta_x V_0^B)(V_p^B - V_0^B)$$

$$V_0^B = \frac{1}{1+\eta_x \epsilon_x} \qquad\qquad C_0 = -\frac{V_0^B \sqrt{\eta_x V_M}}{(1+V_M)^{\frac{1}{4}}}.$$

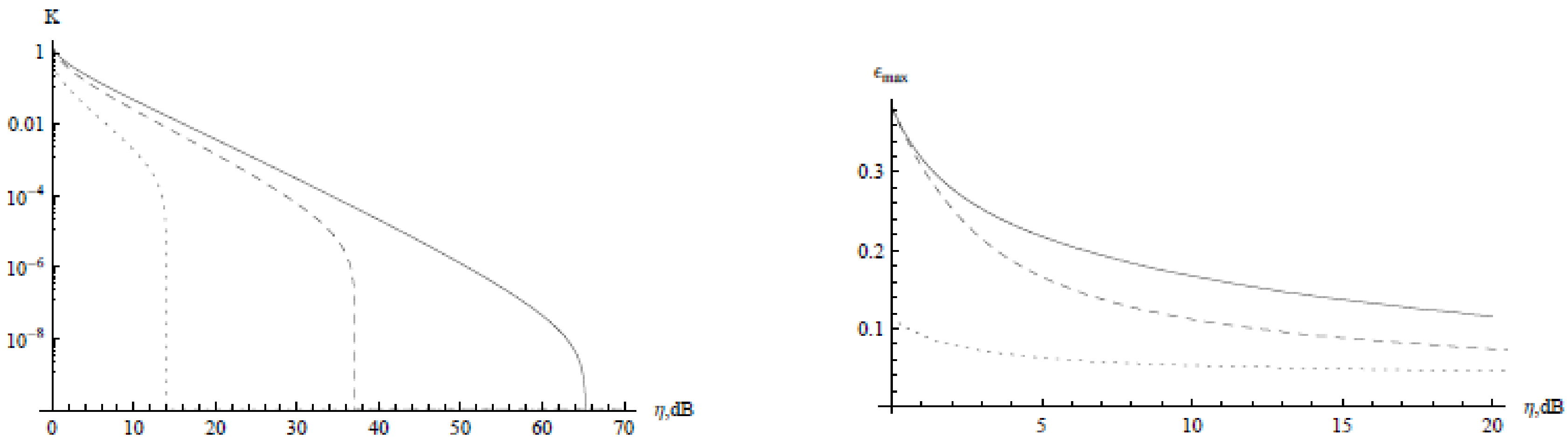
Physicality constraint in terms of the unknown parameters





Key rate (left) and security region (right) versus correlation and variance of the non-modulated quadrature.

Symmetrical quantum channels



Key rate versus distance (left) and maximum tolerable channel noise (right) of the single-quadrature protocol (dotted line), protocol with single-quadrature mutual information, but full channel estimation (dashed line) and standard coherent-state protocol (solid line)

Summary

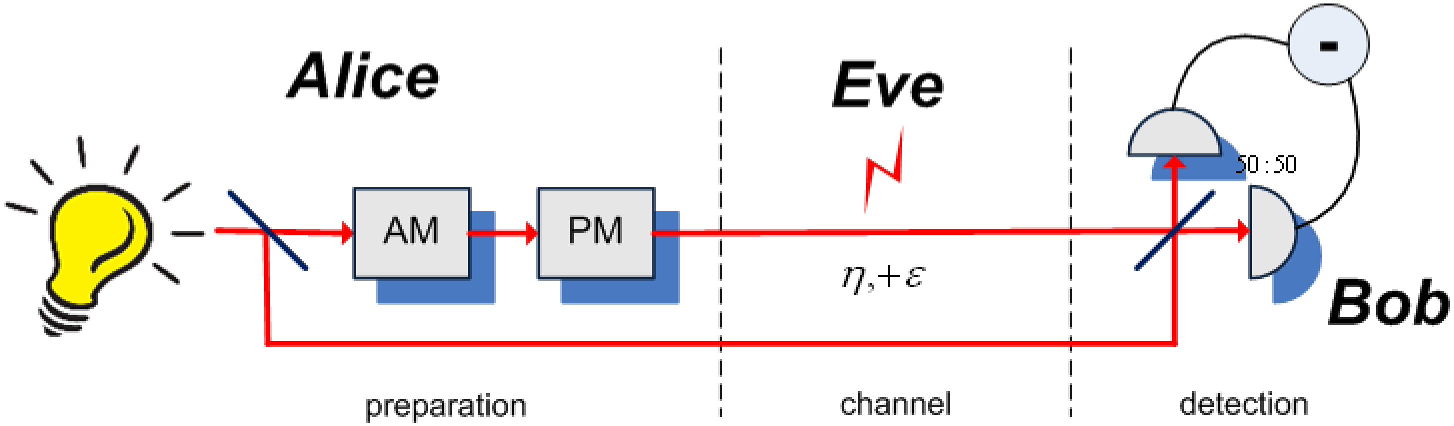
• Single-quadrature protocol potentially enables CV QKD with simplified technical implementation at the cost of key rate and security region

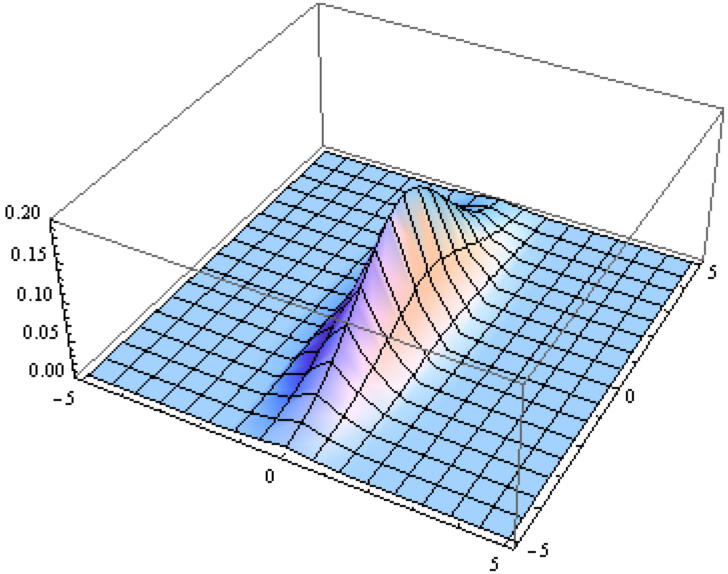
• Despite the fact that channel is not estimated in one of the quadratures, the physicality bounds on the covariance matrices allow to establish security of the protocol.

Weakly modulated squeezed states

Project in progress at DTU, Lyngby

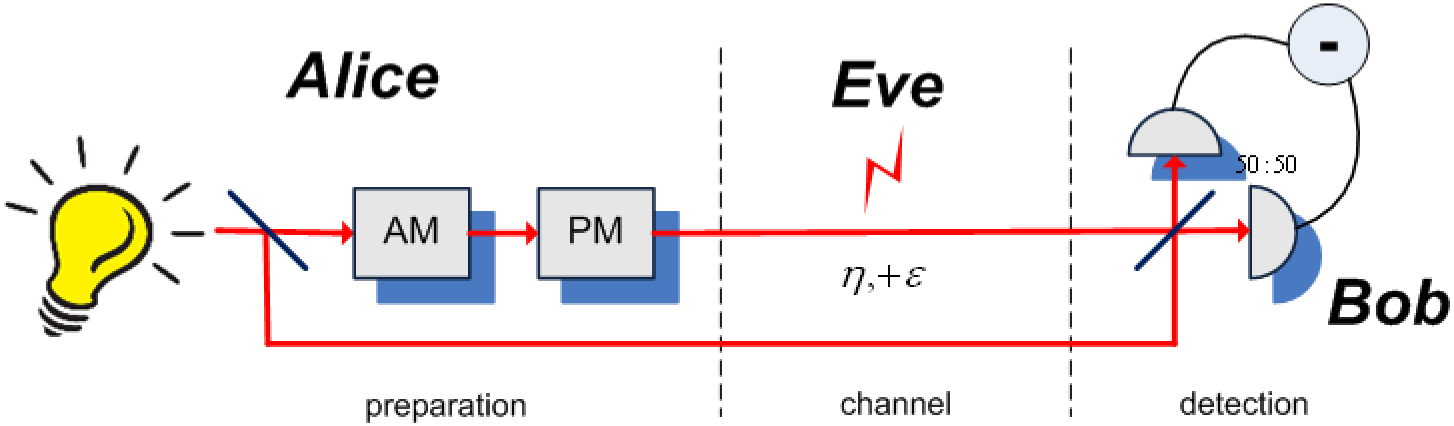
Generalized preparation

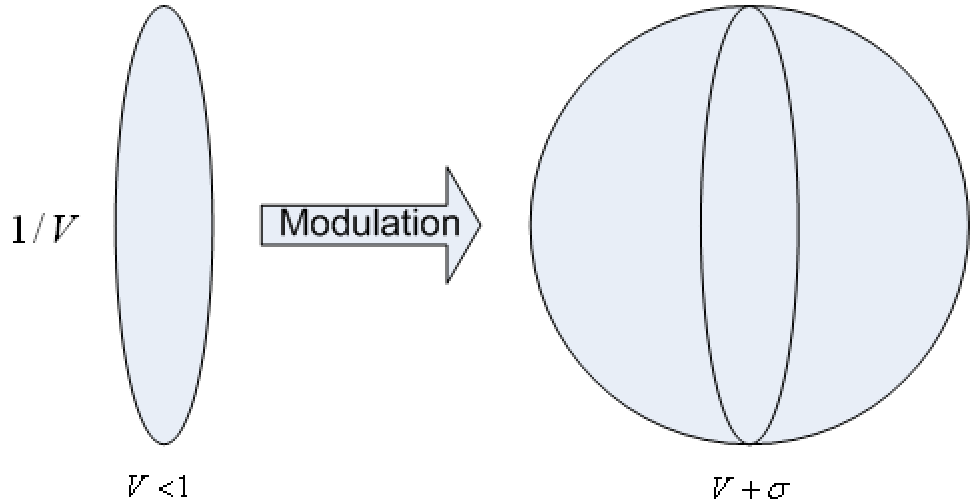




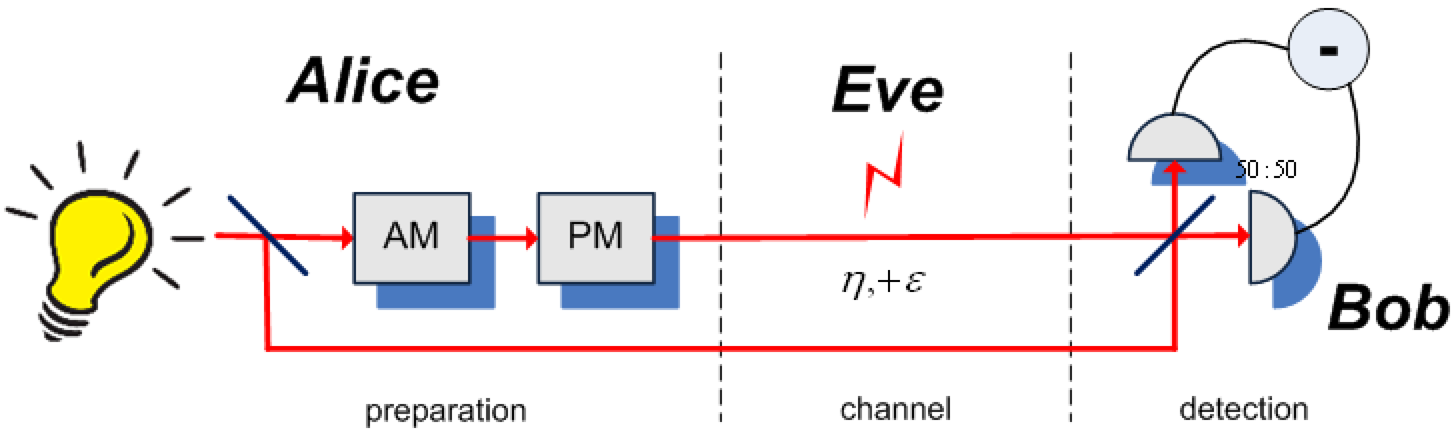
Source state

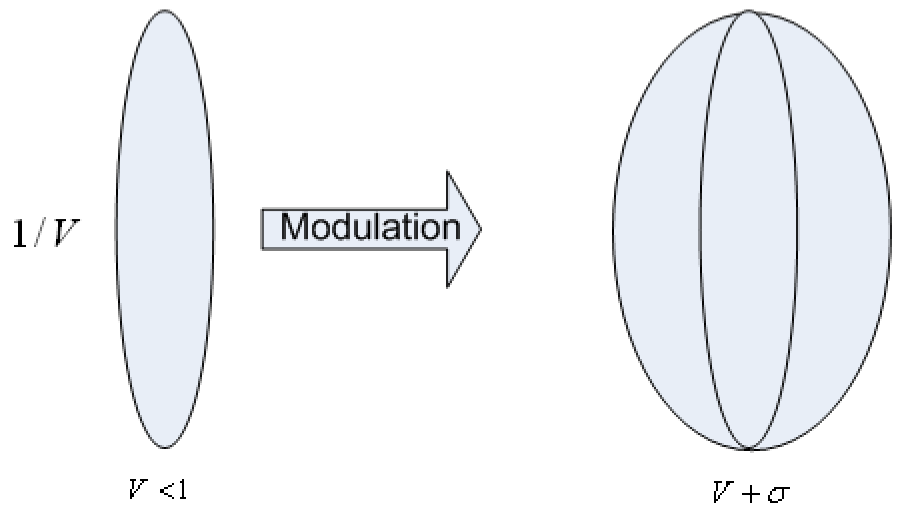
Generalized preparation



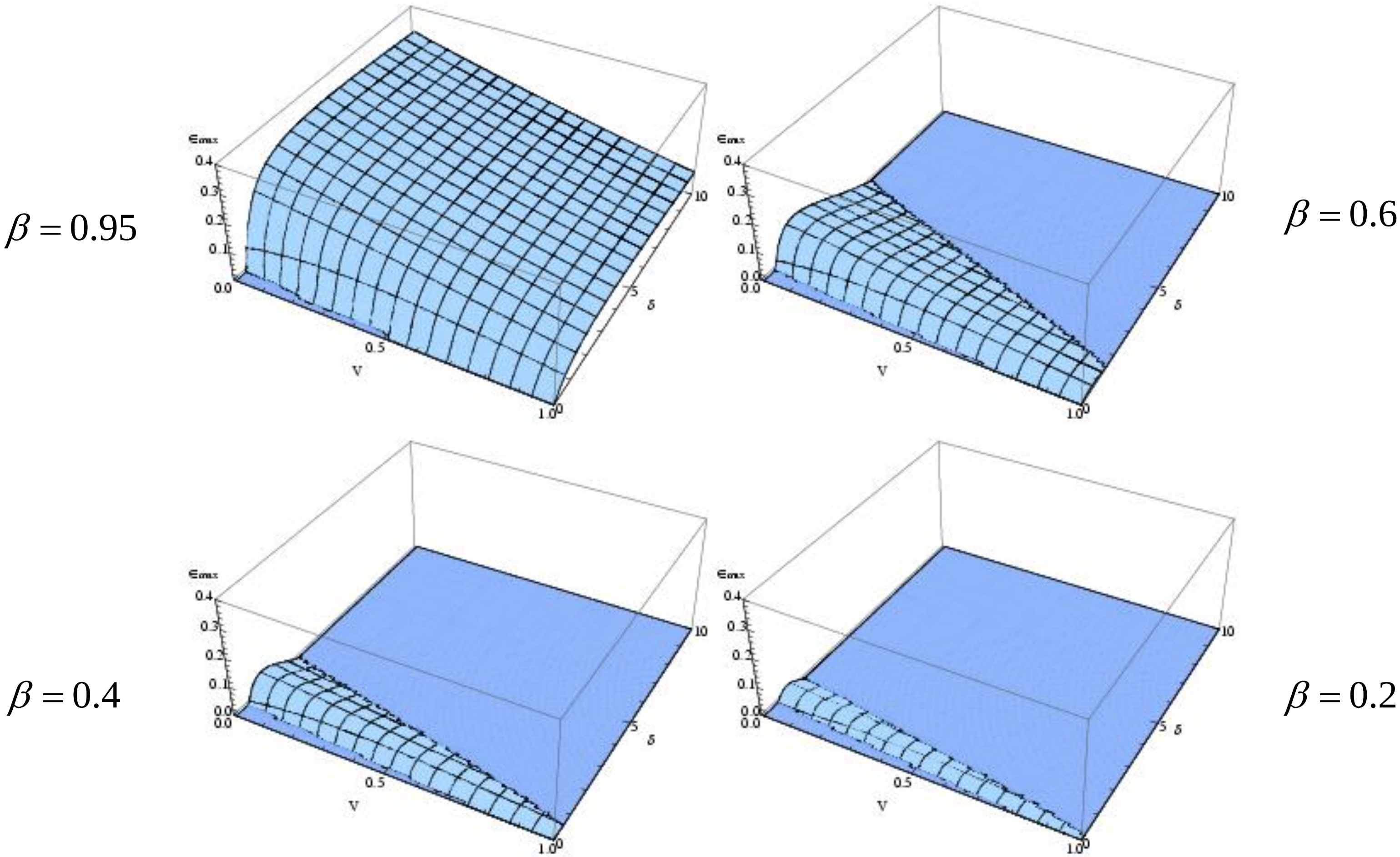


Generalized preparation



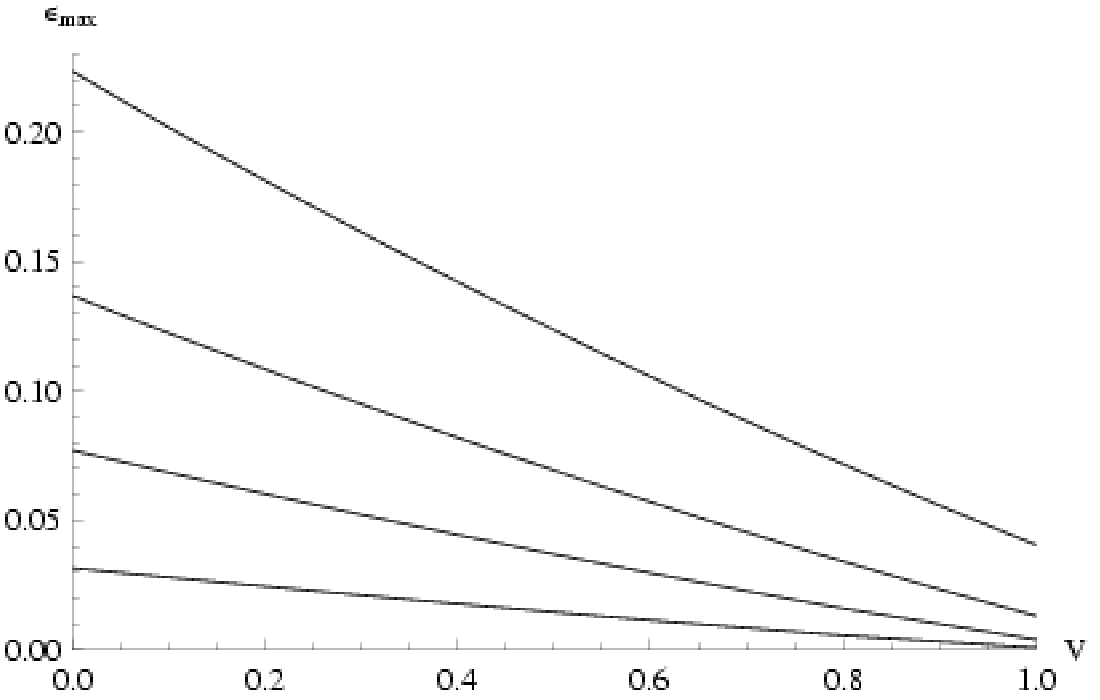


Limited post-processing



Security region (in terms of maximum tolerable excess noise) versus nonclassical resource (squeezing) and classical resource (modulation)

Limited post-processing



Noise threshold profile upon optimized modulation

Ineffective post-processing (long-distance channels)

$$\beta \ll 1$$

$\eta \ll 1$ $\quad I_{AB} = \sigma\eta/\log 4 + O[\eta]^2$ - independent of squeezing

Ineffective post-processing (long-distance channels)

$$\beta \ll 1$$

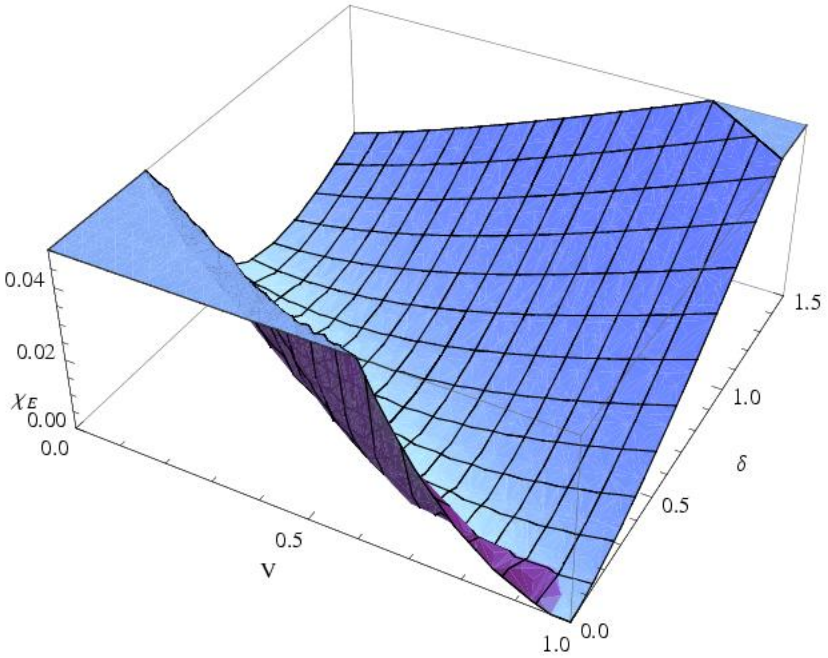
$\eta \ll 1$ $\qquad I_{AB} = \sigma\eta/\log 4 + O[\eta]^2$ - independent of squeezing

$$\boxed{I = \beta I_{AB} - \chi_{BE}}$$

Ineffective post-processing

$$\beta \ll 1$$

$\eta \ll 1$ $$I_{AB} = \sigma\eta/\log 4 + O[\eta]^2$$

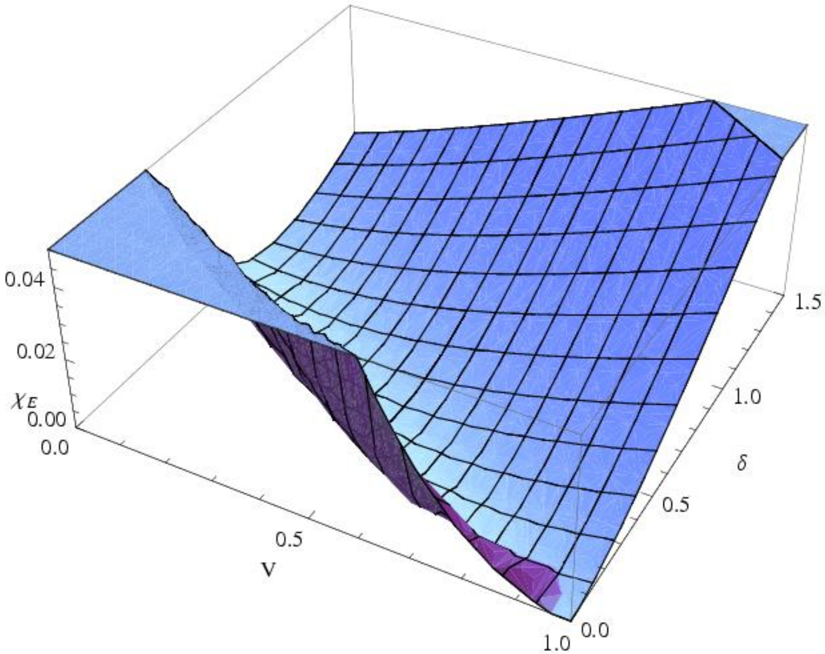


Upper bound on Eve’s information (Holevo quantity)

Ineffective post-processing

$$\beta \ll 1$$

$\eta \ll 1$ $\qquad$ $I_{AB} = \sigma\eta/\log 4 + O[\eta]^2$



Holevo quantity turns to 0 upon pure channel loss when

$$V + \sigma = 1$$

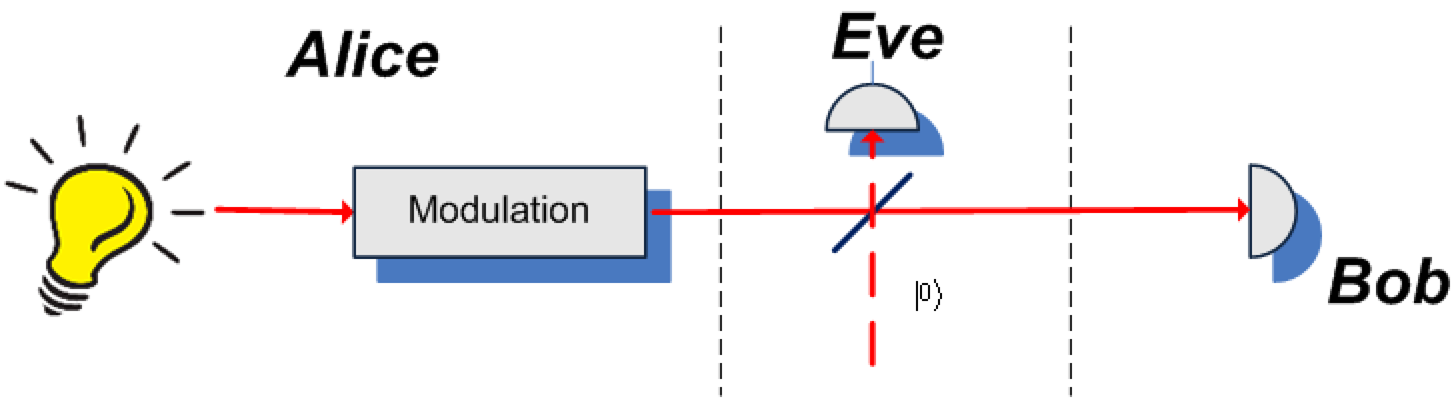
i.e. modulation must be

$$\boxed{\sigma = 1 - V}$$

Canceling information leakage

$$\boxed{\sigma = 1 - V}$$

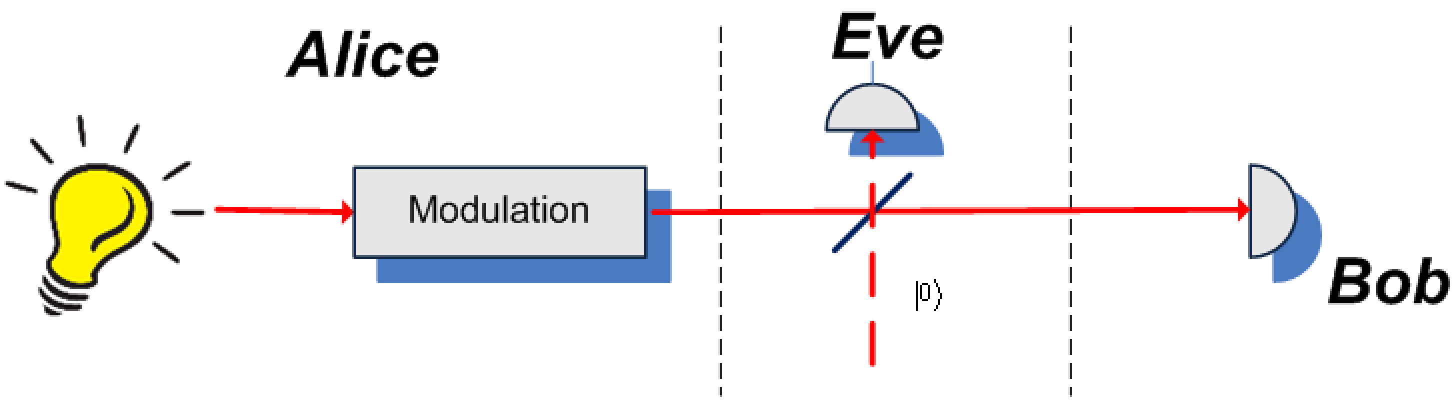
Pure channel loss:



Canceling information leakage

$$\boxed{\sigma = 1 - V}$$

Pure channel loss:

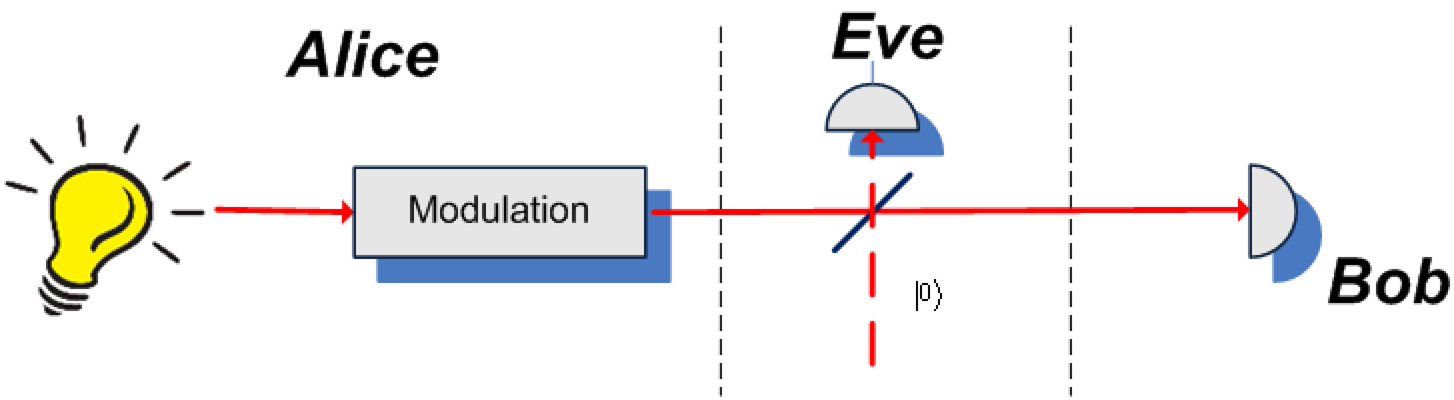


Correlation $C_{BE} \propto V_S - V_E = (V + \sigma) - 1 = 0$

Canceling information leakage

$$\boxed{\sigma = 1 - V}$$

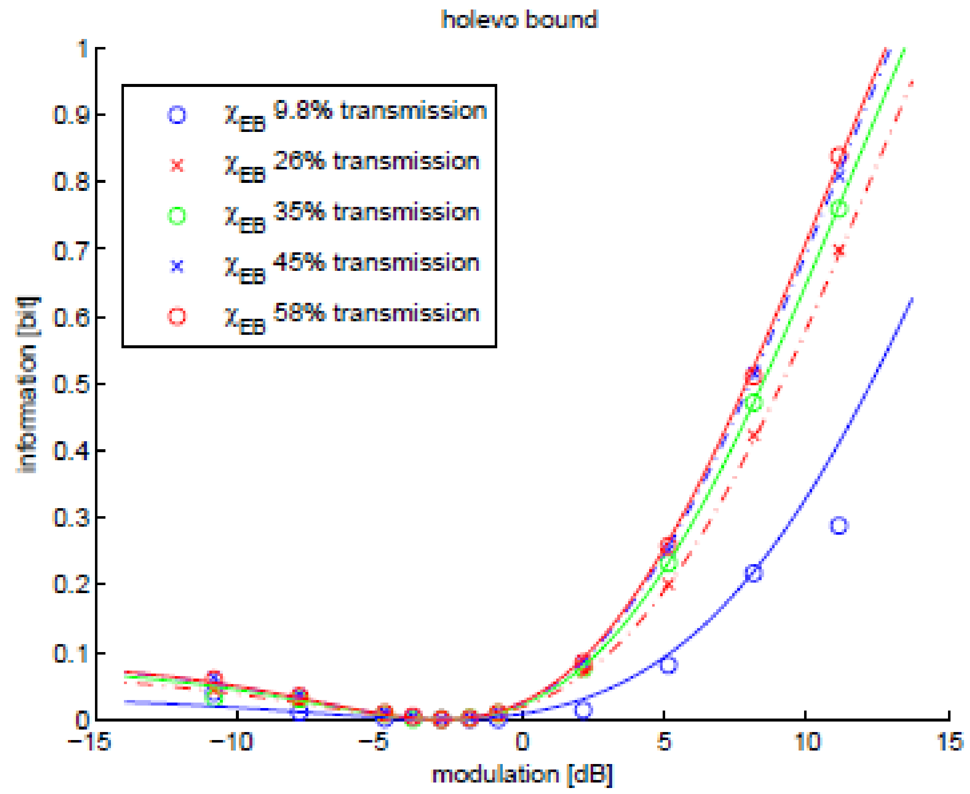
Pure channel loss:



Correlation $\quad C_{BE} \propto V_S - V_E = (V+\sigma) - 1 = 0$

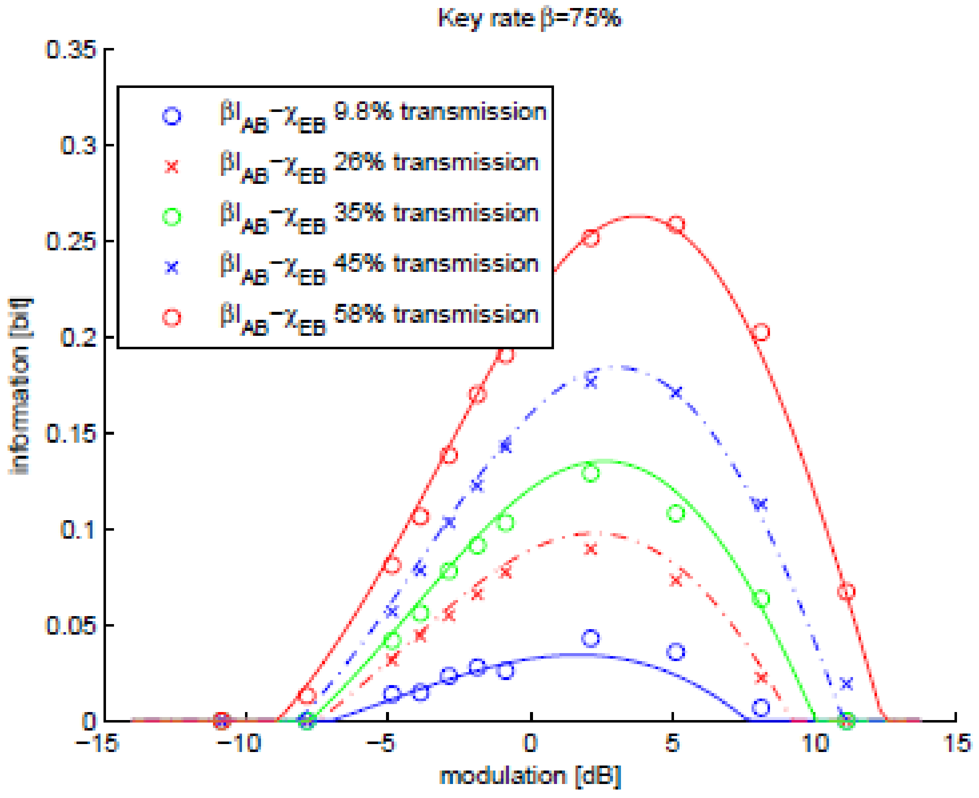
Holevo quantity $\quad \chi_{BE} = 0 \quad$ since $\quad S(E) - S(E \mid B) = 0$

Canceling information leakage



Experimental results, confirming canceling of information leakage at proper modulation at the different values of channel transmittance. Eve's information is directly measured at the output of the channel.

Canceling information leakage



Key rate upon 75% of post-processing efficiency

Work in progress

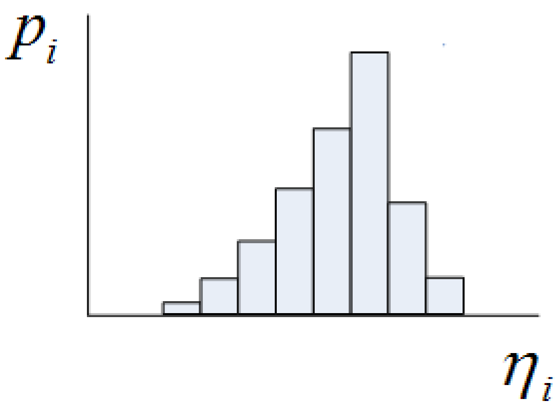
The protocol is now tested for stronger channel losses and at the more precise modulation.

CV QKD over fading channels

Project is progress at MPI, Erlangen
group of prof. Gerd Leuchs

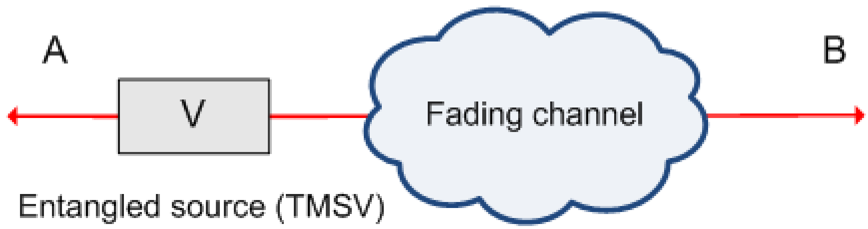
Fading channels

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.

Fading channels: effect on entanglement



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:

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

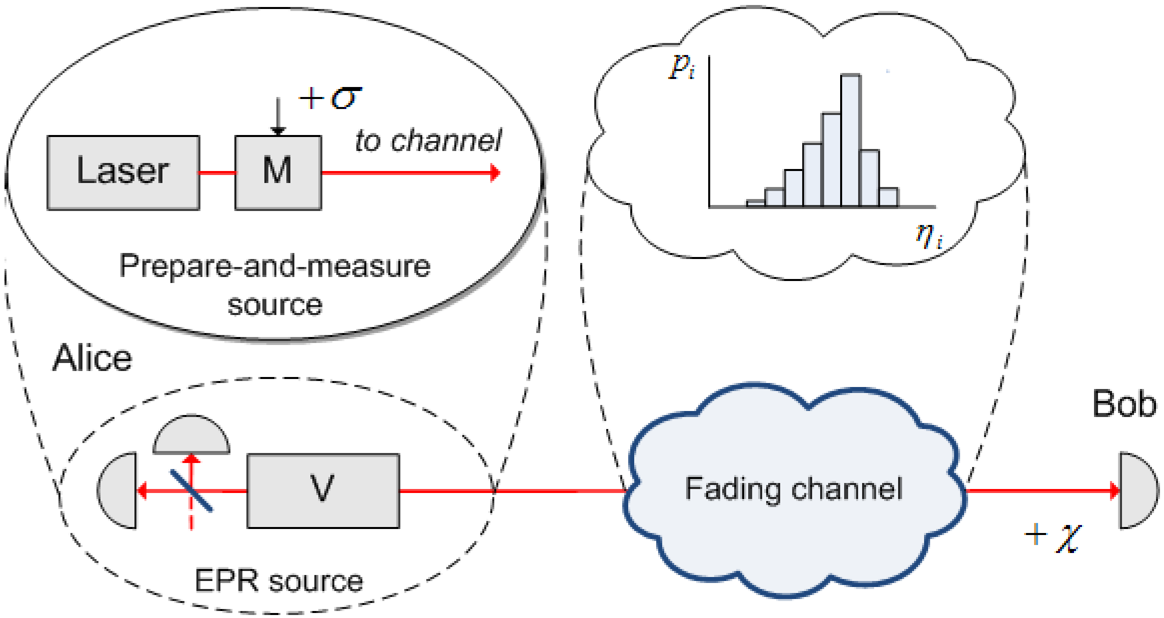
Is equivalent to a fixed channel with variance-dependent excess noise:

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

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

Fading channels: effect on QKD

Equivalent entanglement-based scheme:



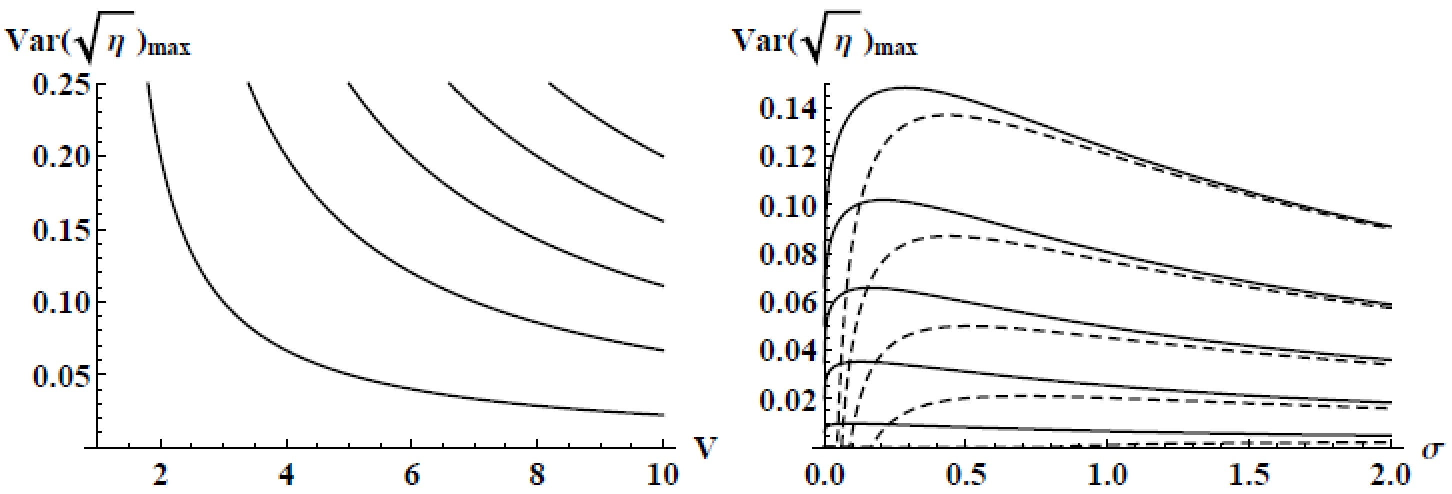
Effect of a fading channel upon individual attacks:

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

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

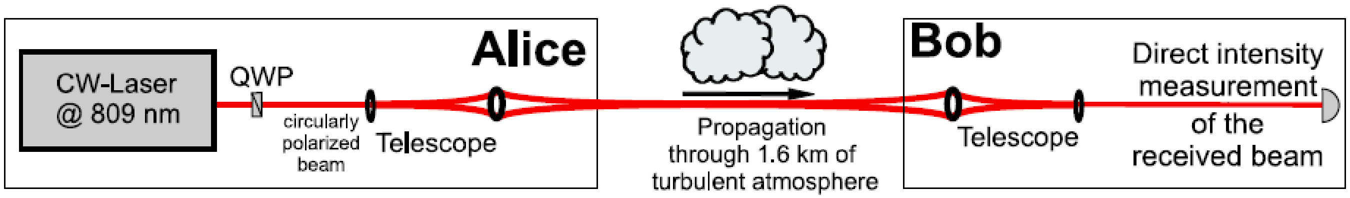
Fading channels: effect on QKD

Entanglement (left) and security against the collective attacks (right):

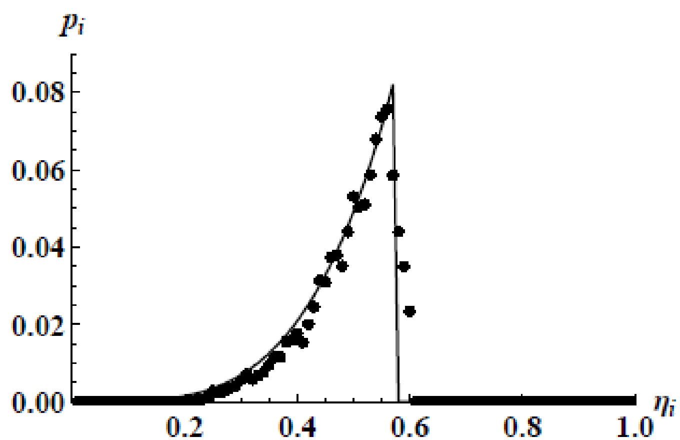


solid lines: no excess noise
dashed lines: excess noise $\chi = 1.2 \cdot 10^{-2}$

Real fading channel



Transmittance distribution obtained from a 1.6 km atmospheric link in Erlangen

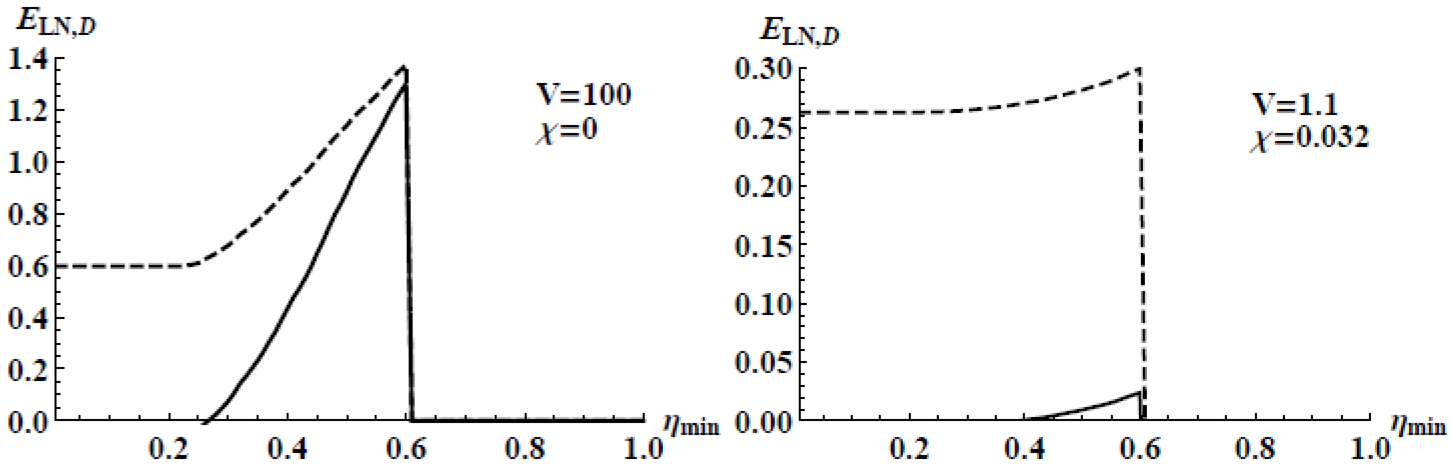


Sampling rate 150 kHz, bin size $\Delta\eta = 0.01$

Experimental distribution is well fitted by the log-normal one with $\sigma_b = 0.6$,$W/a = 1.5$ and additional attenuation of 25%.

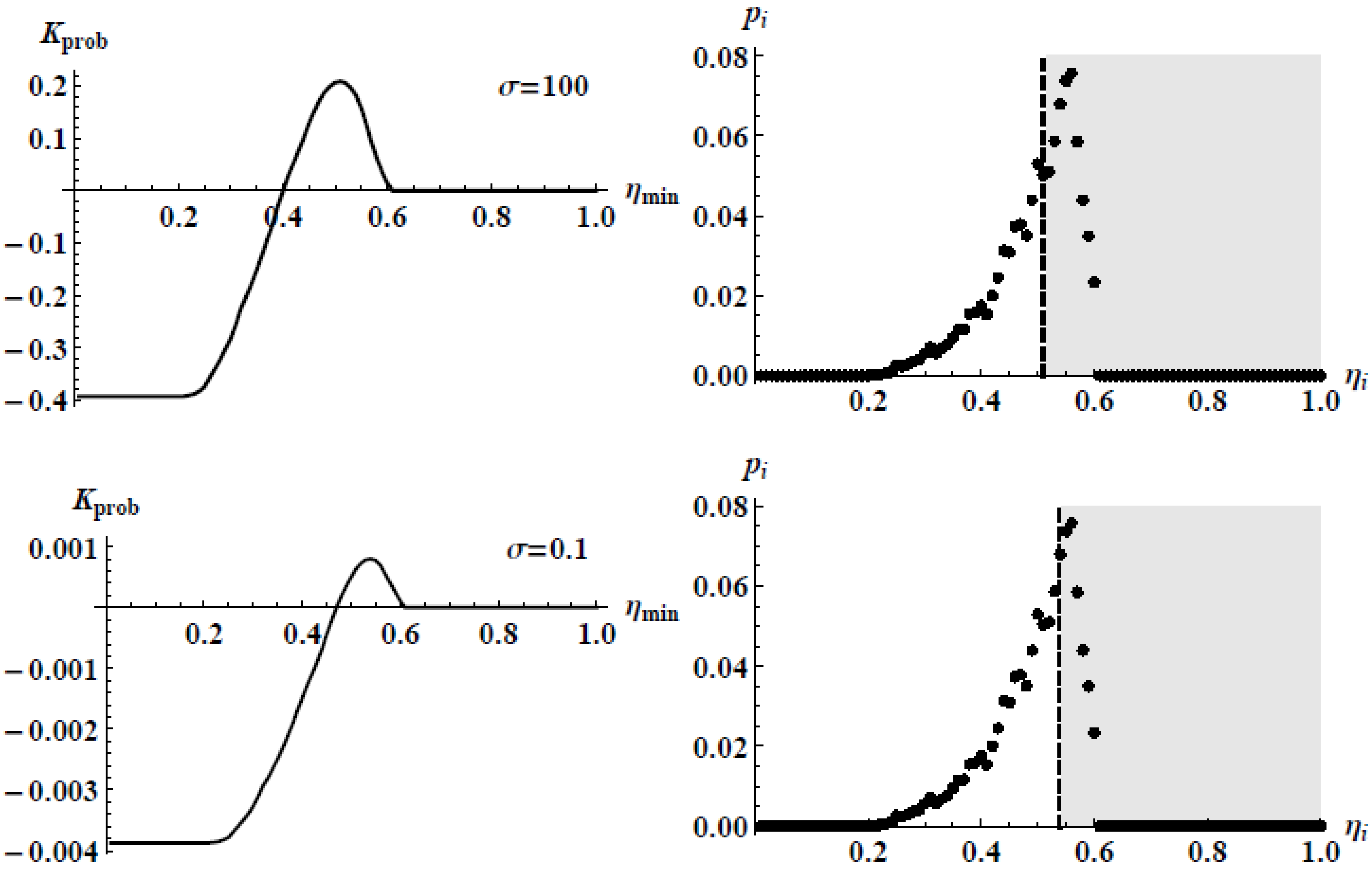
Channel is characterized by $\langle\sqrt{\eta}\rangle^2 \approx 0.492$ and $Var(\sqrt{\eta}) \approx 3 \cdot 10^-3$

Real fading channel



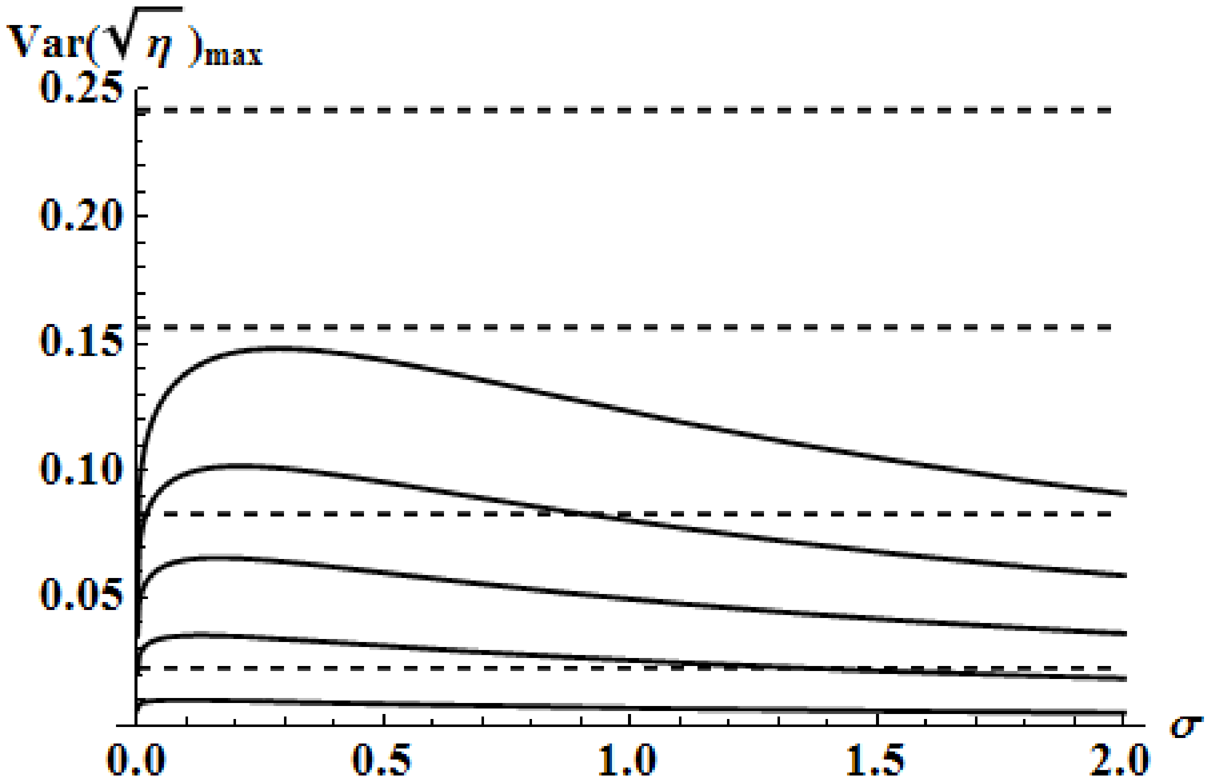
Effect of post-selection after the real fading channel on the entanglement in terms of logarithmic negativity (dashed)
and conditional entropy (solid line) for high (left) and low
state variance (right).

Real fading channel



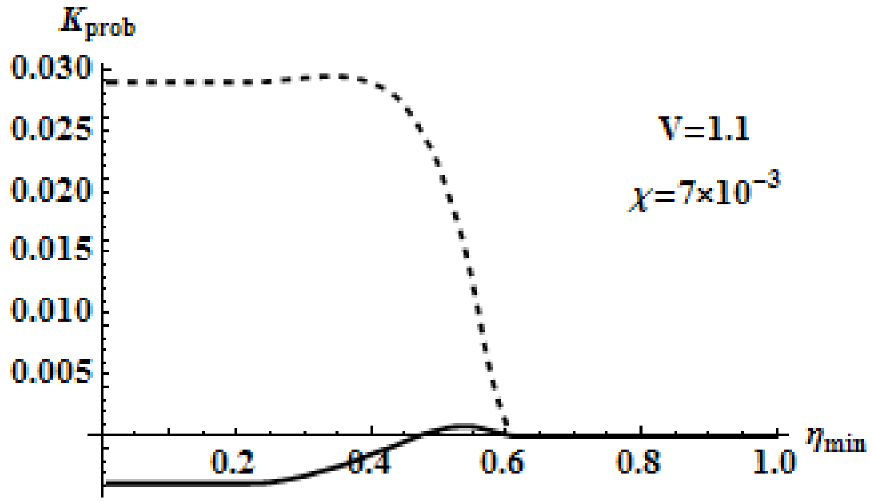
Effect of post-selection after the real fading channel on the security of the coherent-state protocol in terms of the weighted key rate (left). Corresponding optimal PS region is given at the right. Noise $\chi = 3.2 \cdot 10^{-2}$

Alternative: squeezed-state protocol



Sensitivity of the squeezed-state protocol with low squeezing (-0.8 dB of squeezing) and fixed modulation (dashed lines) to fading, compared to the coherent-state based protocol (solid lines) for a general channel.

Alternative: squeezed-state protocol



Effect of post-selection of sub-channels on the squeezed-state protocol (dashed line) and coherent-state protocol (solid line) in the real atmospheric channel.

Post-selection is not needed, if squeezed states are used!

Work in progress

• Measurements were taken on the modulated coherent states after the fading channel, the data analysis is in process;

• Squeezed-state CV QKD will be further tested as a feasible alternative to the coherent-state protocols, not requiring post-selection.

Acknowledgements

Collaborators:

Radim Filip;

Frederic Grosshans (ENS Cachan, University Paris-Sud)

Ulrik Andersen and Lars Madsen (DTU, Copenhagen);

Bettina Heim and Christoph Marquardt (MPI Erlangen)

european social fund in the czech republic

EUROPEAN UNION

MINISTRY OF EDUCATION, YOUTH AND SPORTS

OP Education for Competitiveness

INVESTMENTS IN EDUCATION DEVELOPMENT

Thank you for attention!

usenko@optics.upol.cz