Nonclassical light in quantum cryptography

Vladyslav C. Usenko

Department of Optics, Palacký University,
Olomouc, Czech Republic

Bielefeld, 2017

Motivation

What is quantum in QKD?

Motivation

What is quantum in QKD?

- States (single-photon, squeezed, coherent)

Motivation

What is quantum in QKD?

- States (single-photon, squeezed, coherent)
- Measurement (photodetection, homodyning)

Motivation

What is quantum in QKD?

- States (single-photon, squeezed, coherent)
- Measurement (photodetection, homodyning)

When do we really need nonclassicality of the signal?

Motivation

What is quantum in QKD?

- States (single-photon, squeezed, coherent)
- Measurement (photodetection, homodyning)

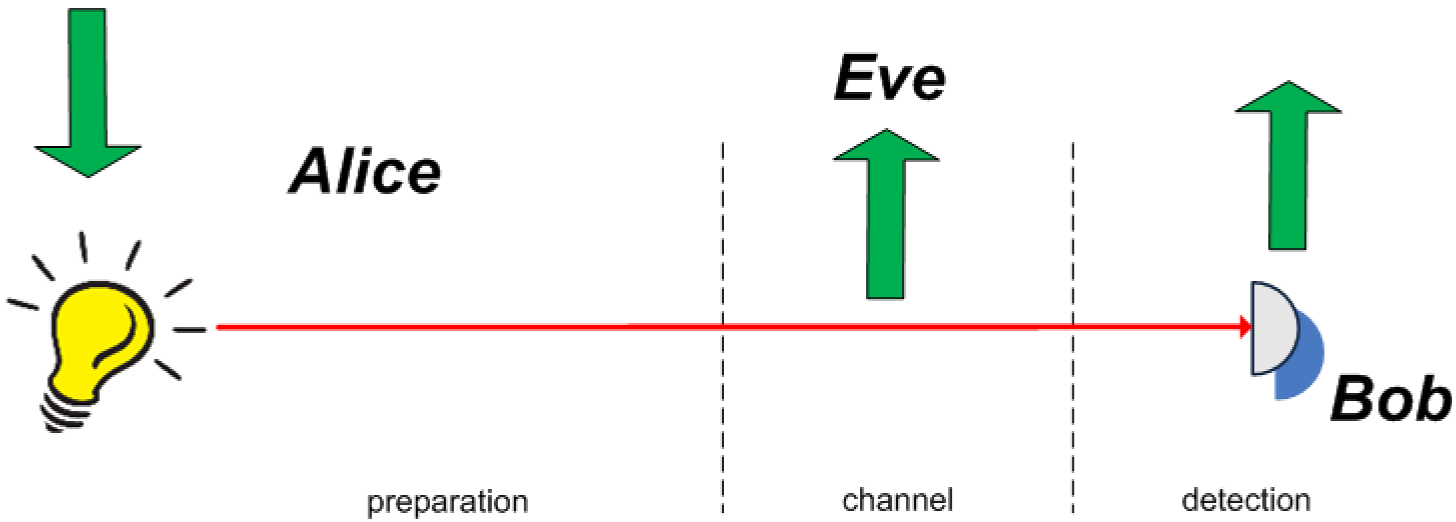
When do we really need nonclassicality of the signal?

How much does it help?

Is it worth the effort?

…is it always good?

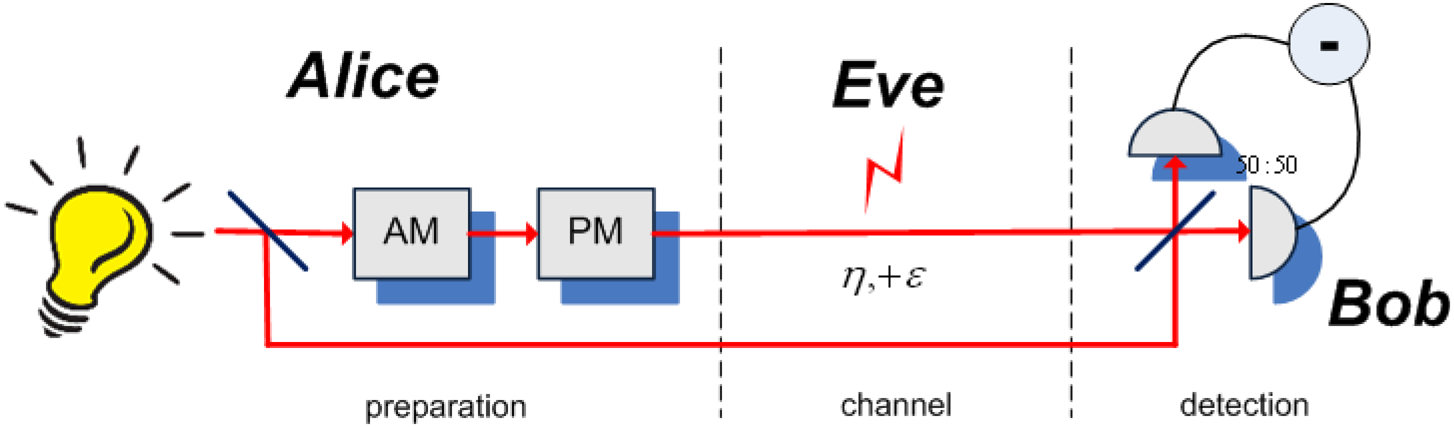
Quantum key distribution

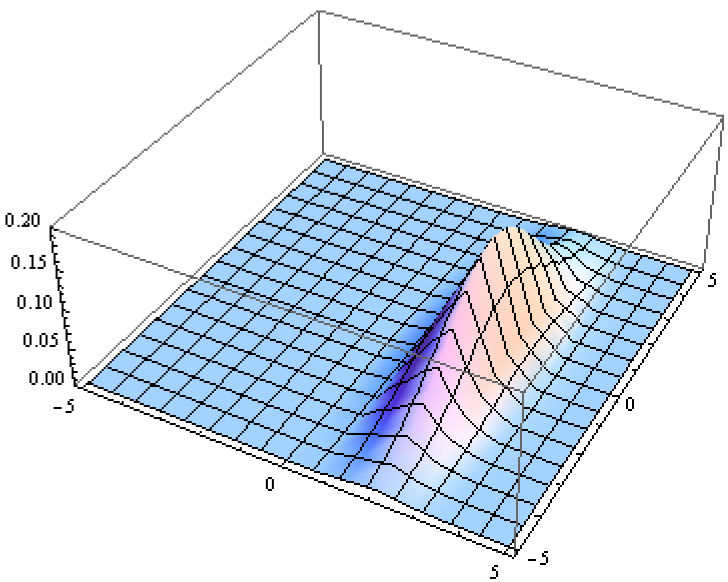


The secure key can be distilled if $I_{AB} > I_{BE}$ or $I_{AB} > I_{AE}$.

Lower bound on secure key: $\boxed{K \geq \max(I_{AB} - I_{BE}, I_{AB} - I_{AE})}$

CV Quantum Key Distribution

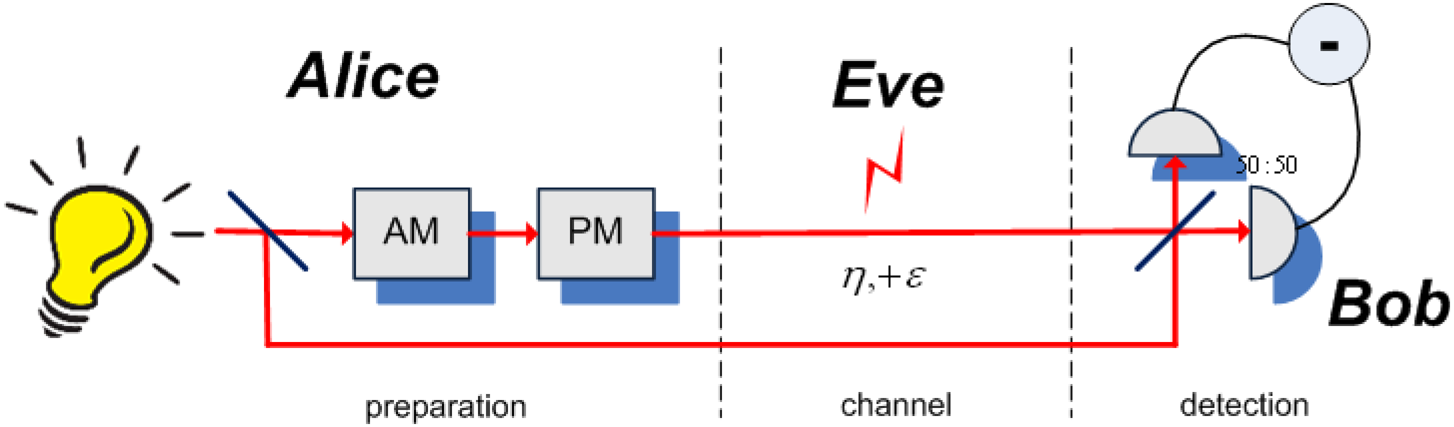


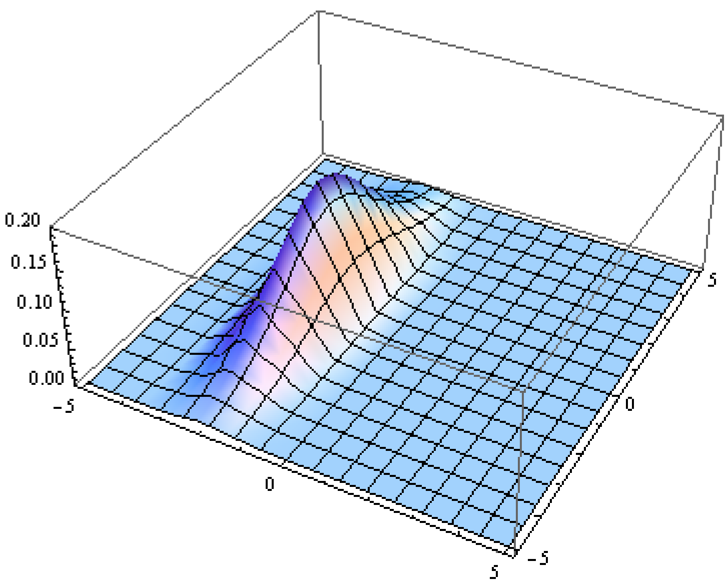


Squeezed states-based protocol:
Squeezed source, quadrature modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

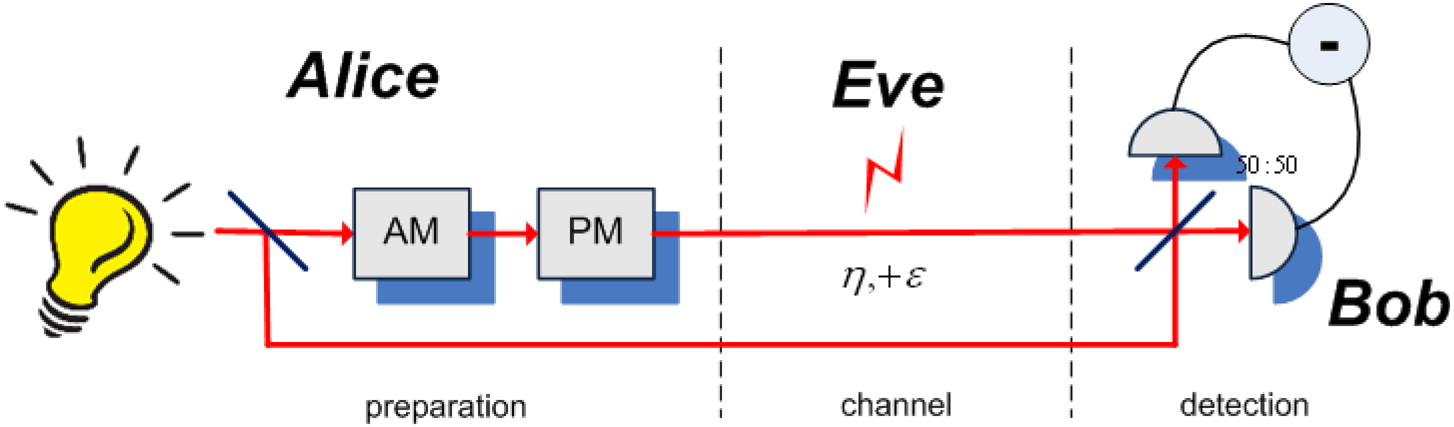


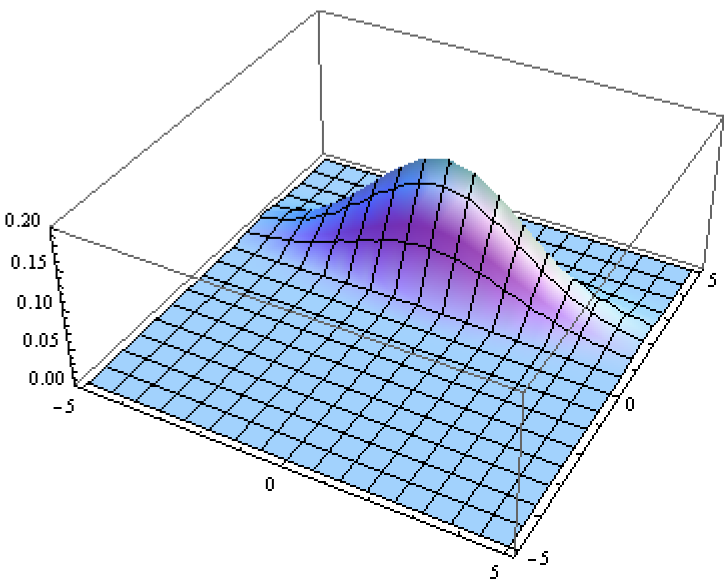


Squeezed states-based protocol:
Squeezed source, quadrature modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

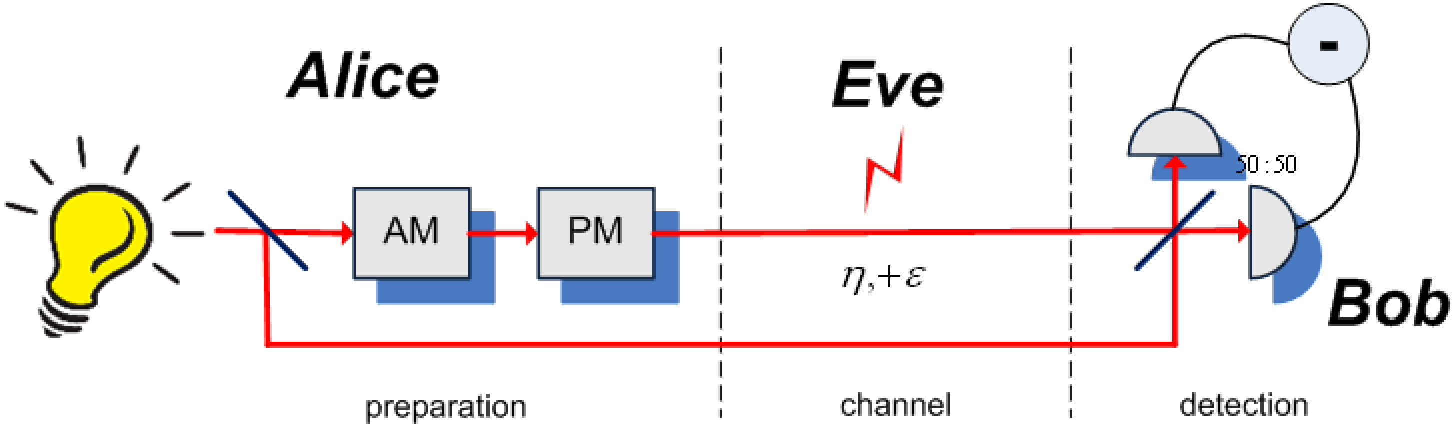


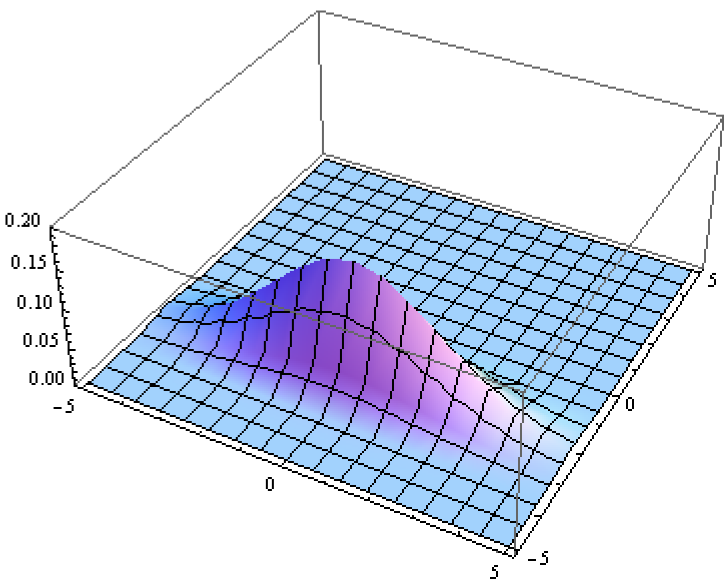


Squeezed states-based protocol:
Squeezed source, quadrature modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

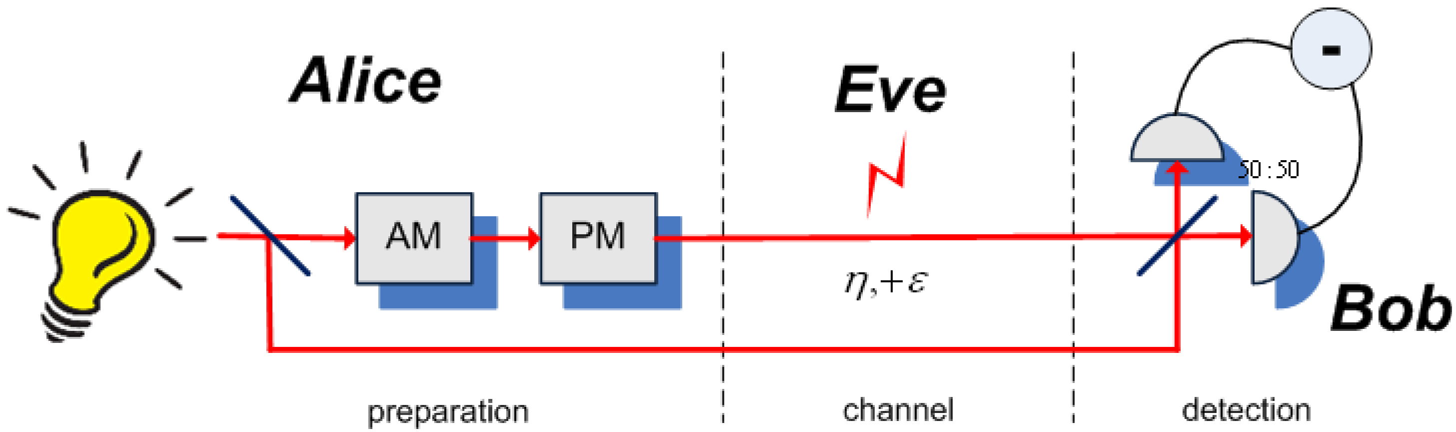


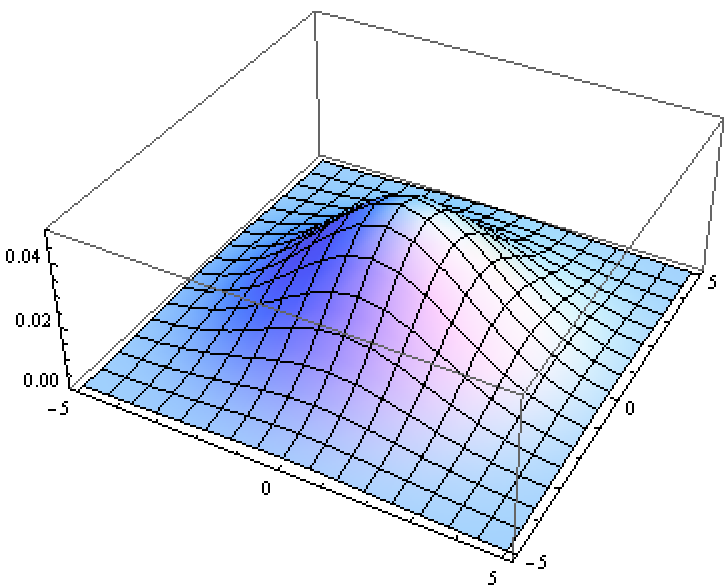


Squeezed states-based protocol:
Squeezed source, quadrature modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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



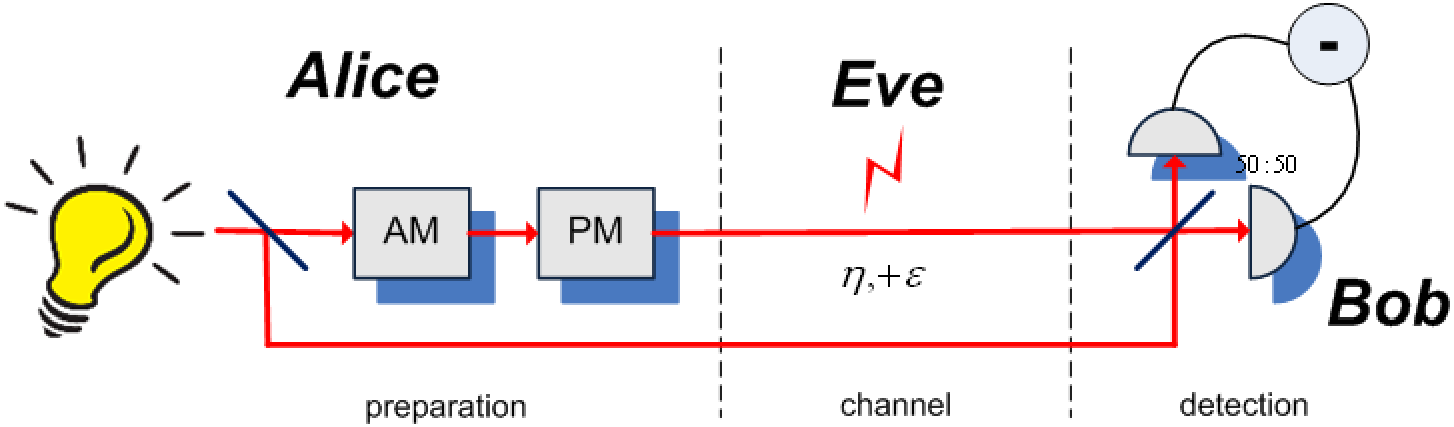


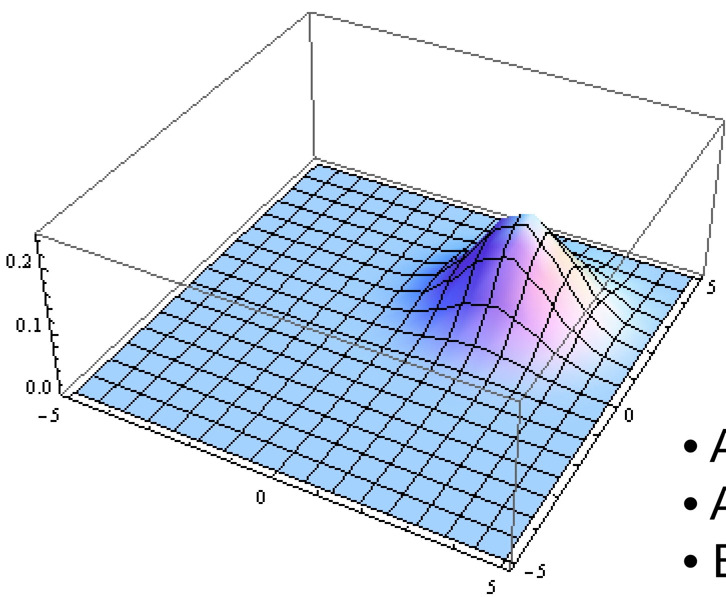
Mixture

Squeezed states-based protocol:
Squeezed source, quadrature 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

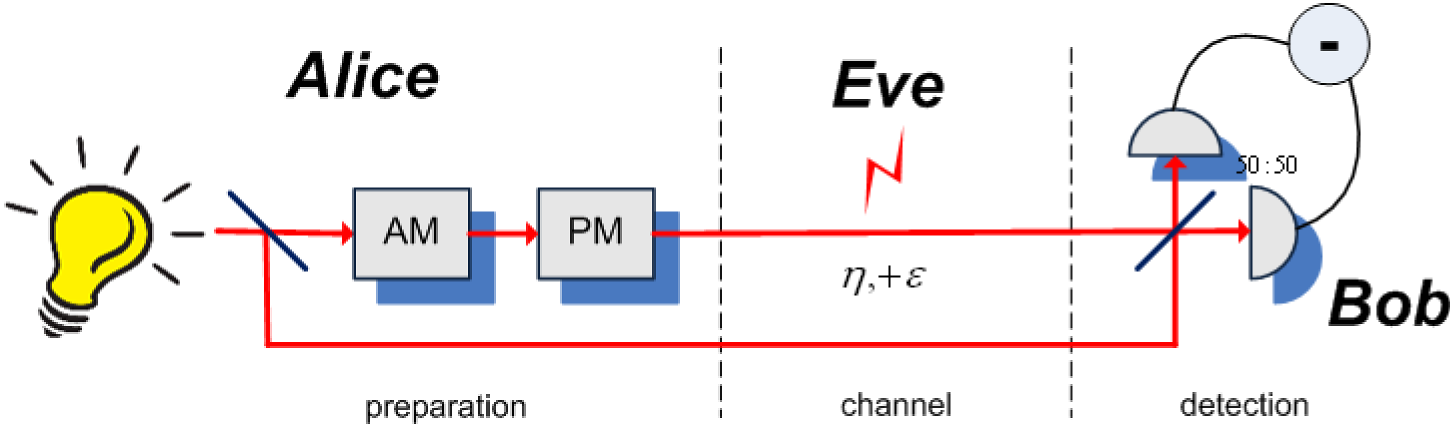


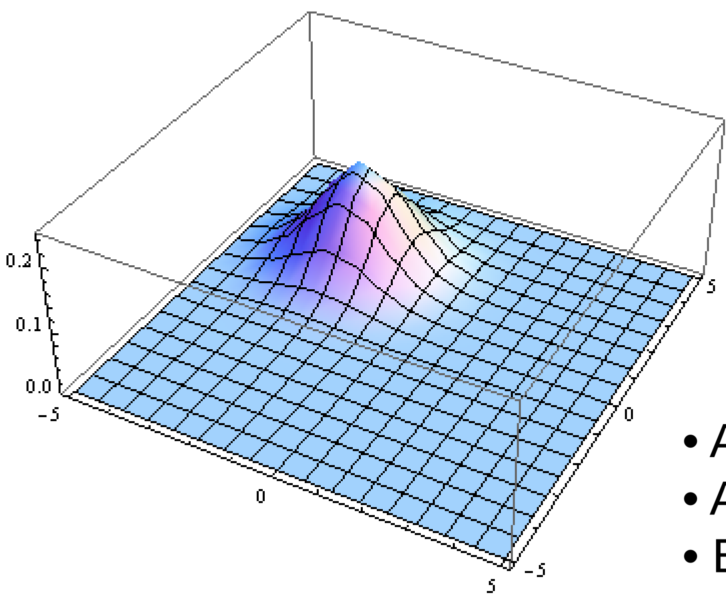


Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

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

CV Quantum Key Distribution

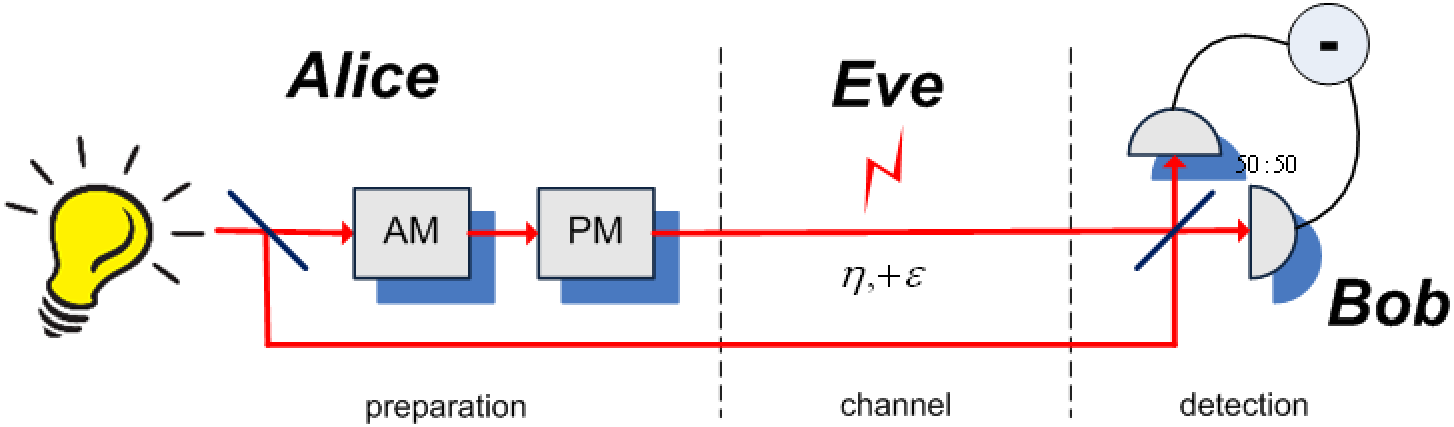


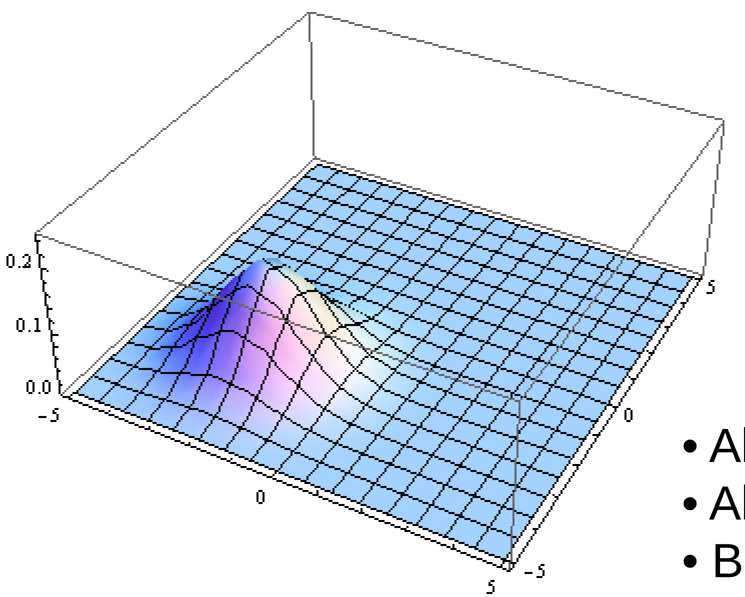


Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

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

CV Quantum Key Distribution

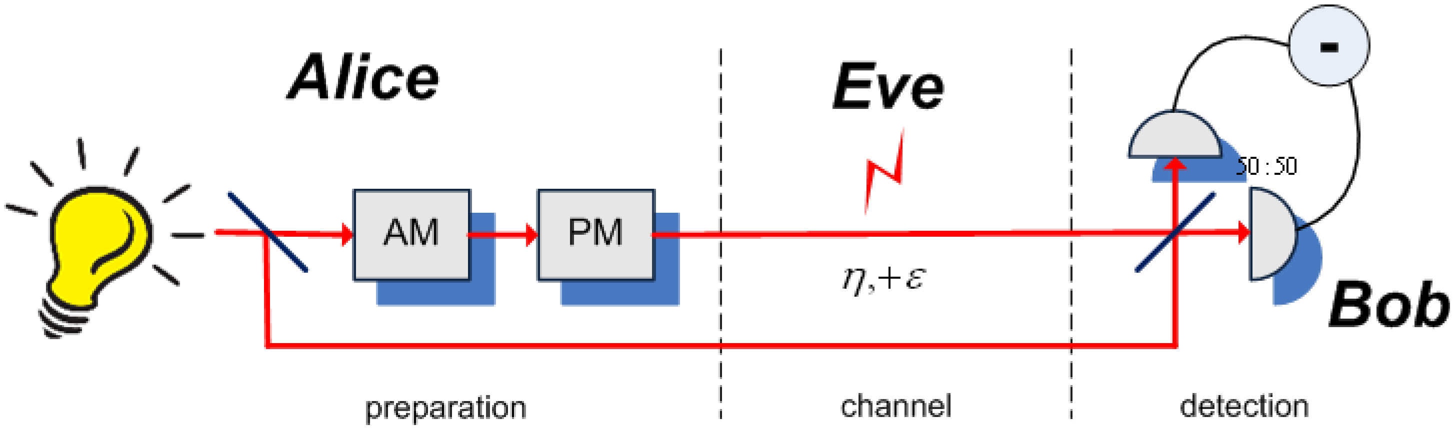


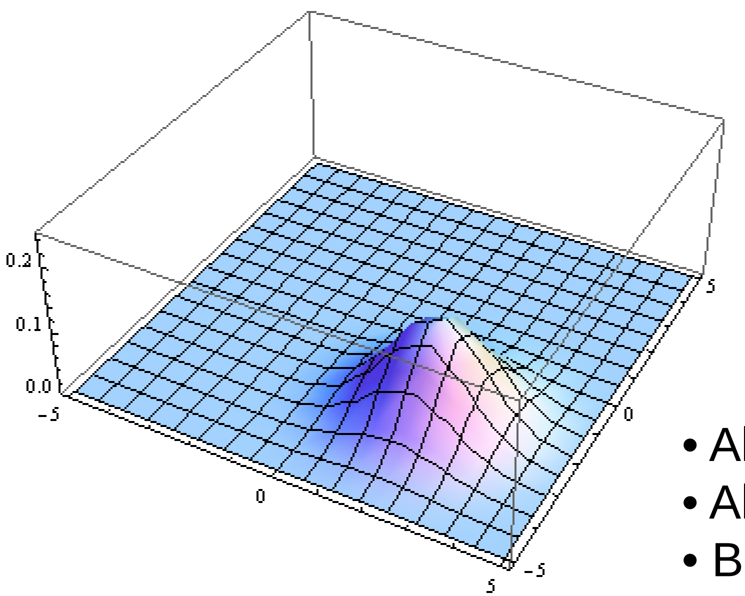


Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

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

CV Quantum Key Distribution

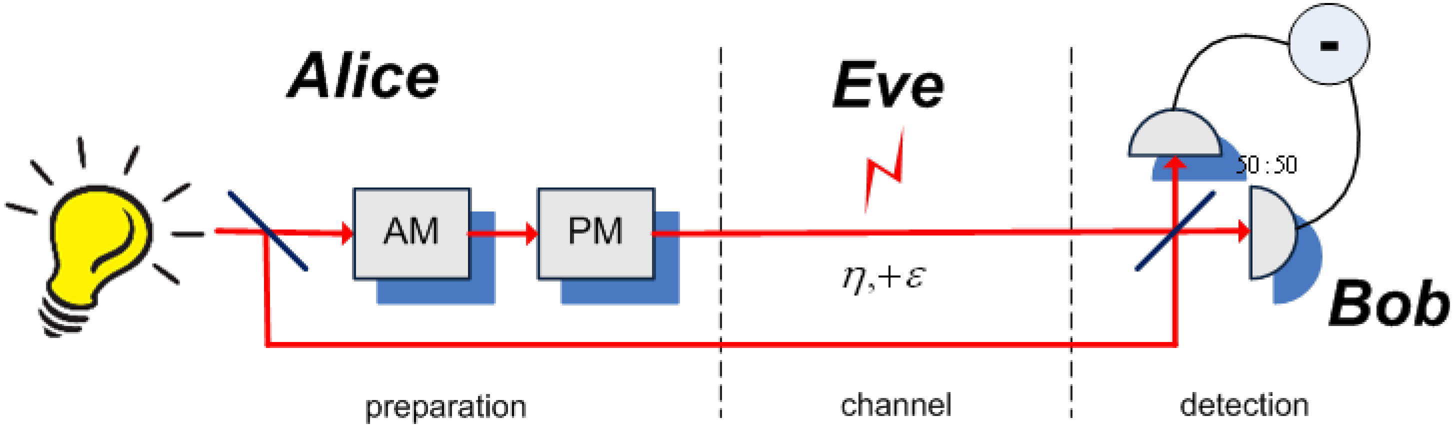


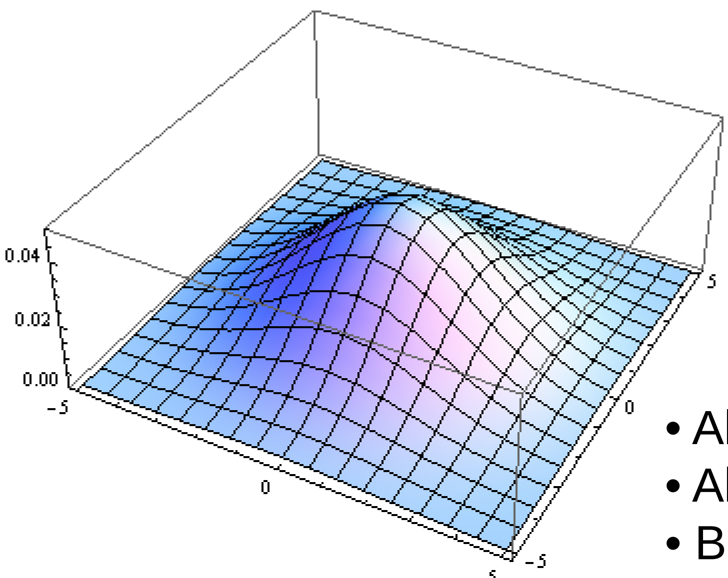


Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

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

CV Quantum Key Distribution



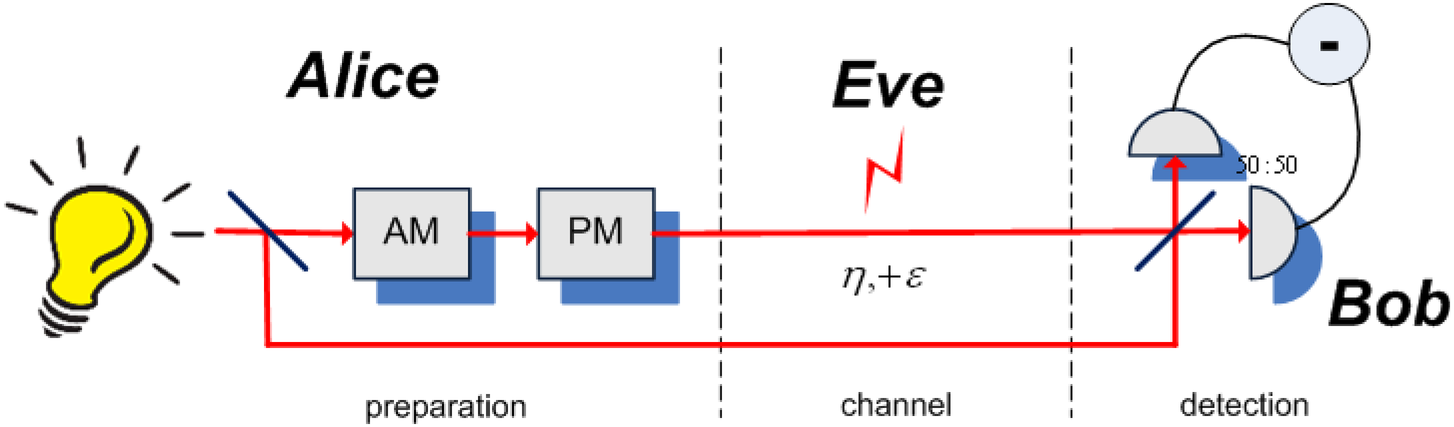


Mixture

Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

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

CV Quantum Key Distribution



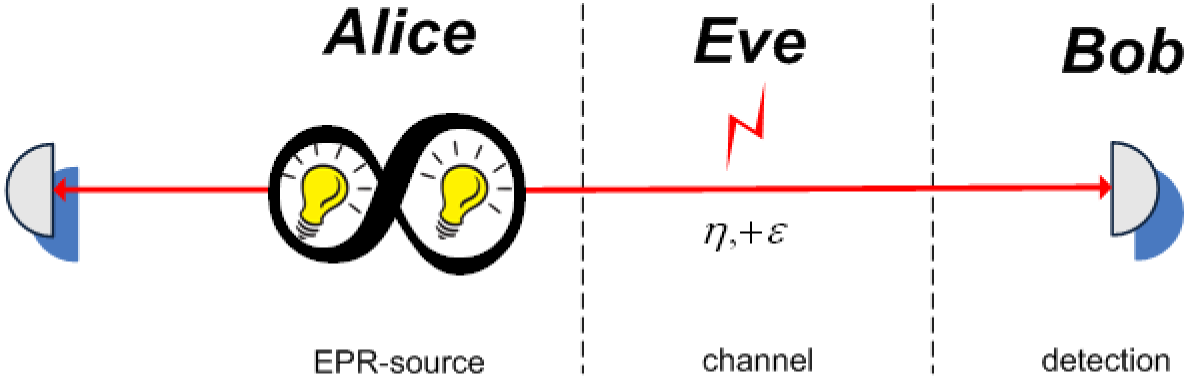
Coherent states-based protocol:
Laser source, quadrature modulation
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

Achievements:

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

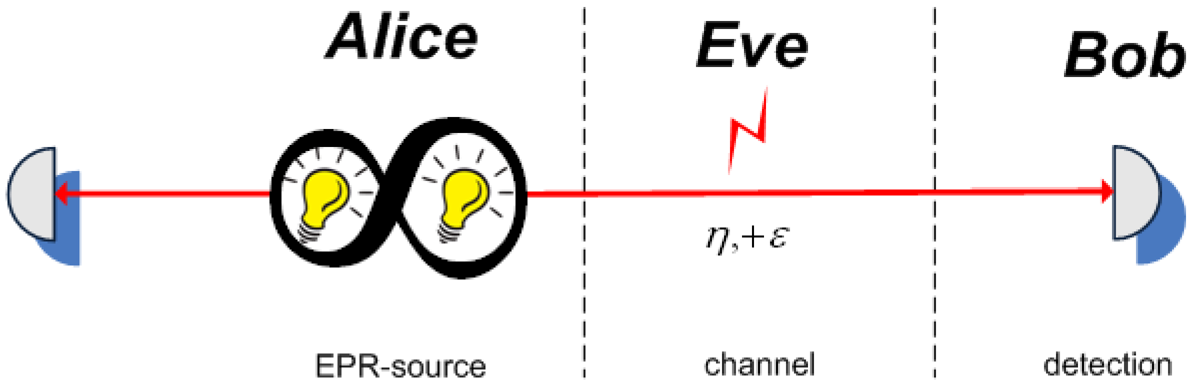
100 km [D. Huang et al., Sci. Rep. 6, 19201 (2016)]

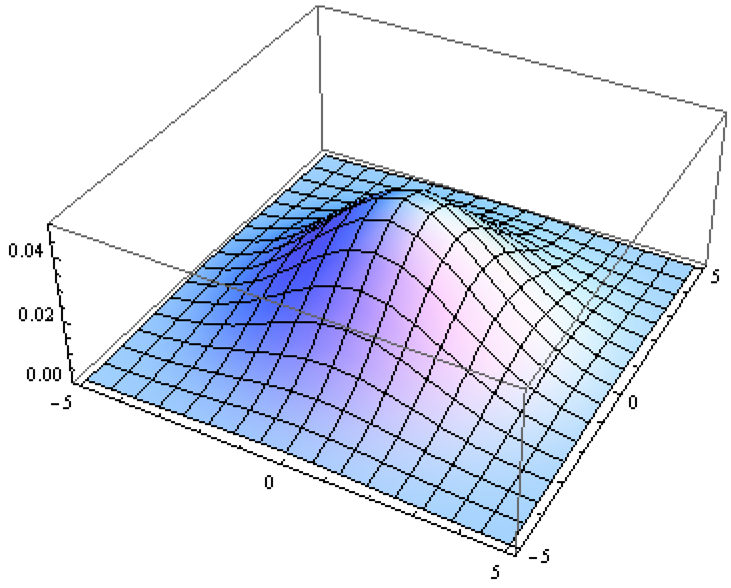
CV QKD: entangled-based

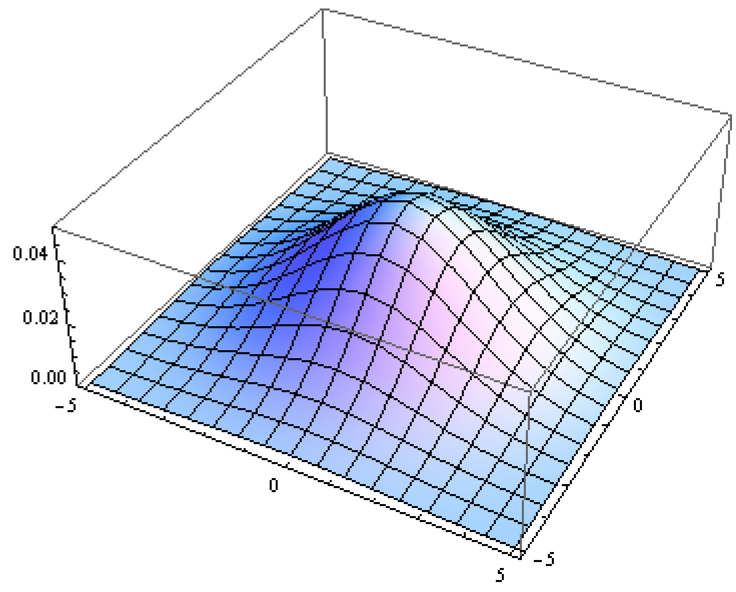


Two-mode squeezed vacuum state shared between the trusted parties

CV QKD: entangled-based

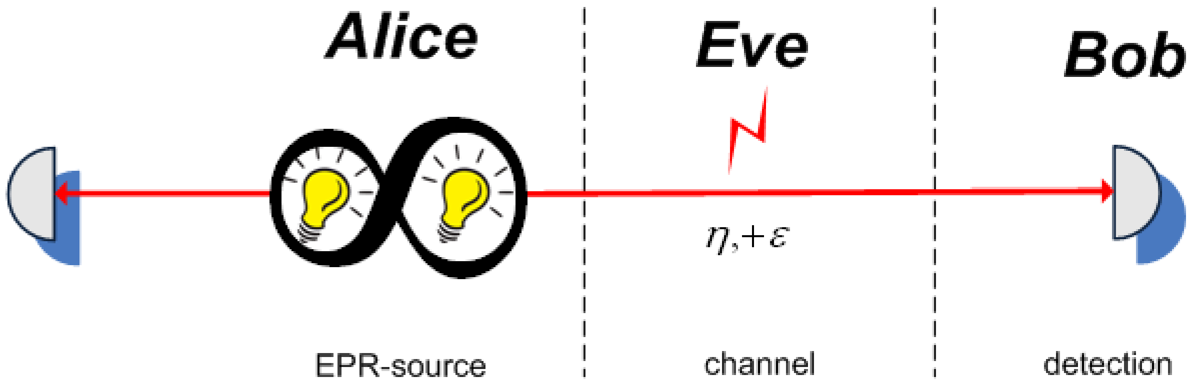




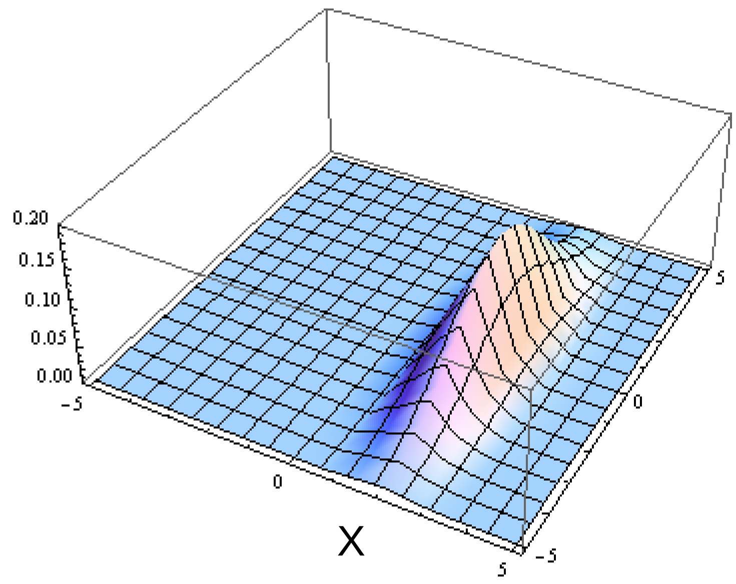


Two-mode squeezed vacuum: before measurement

CV QKD: entangled-based

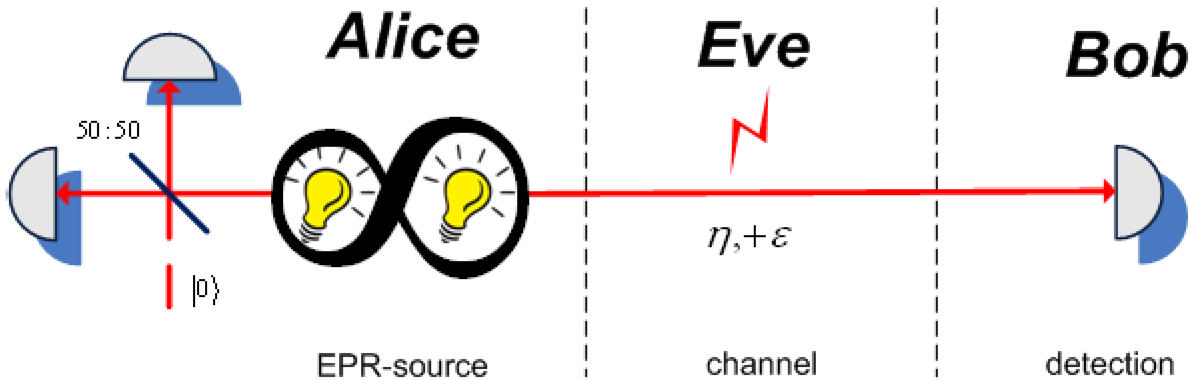


X

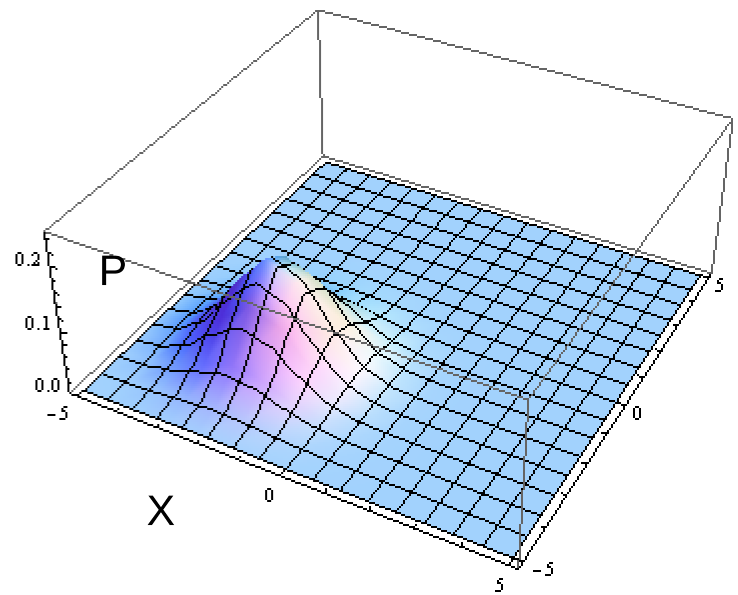


Two-mode squeezed vacuum: after homodyne measurement

CV QKD: entangled-based

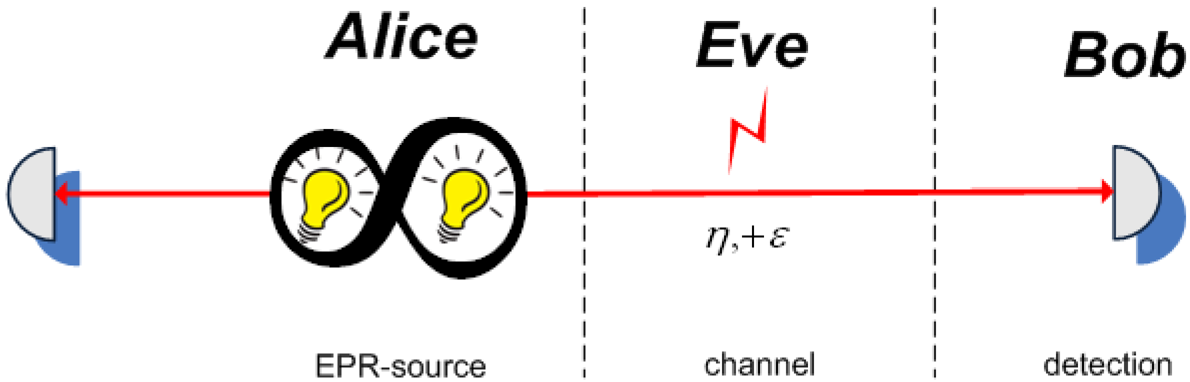


X,P

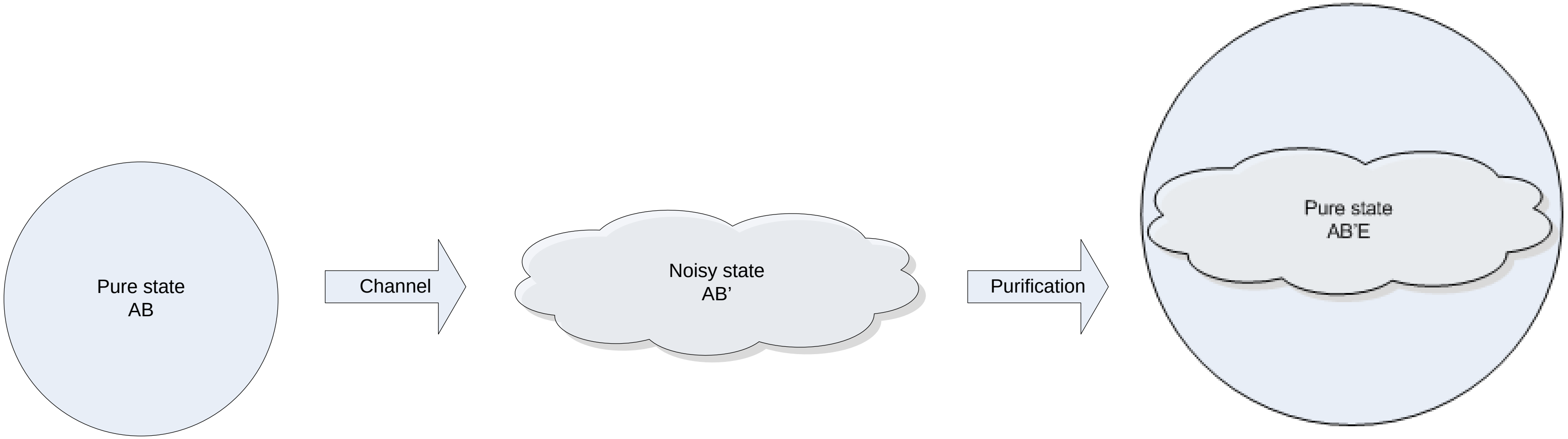


Two-mode squeezed vacuum: after heterodyne measurement

CV QKD: entangled-based



Allows security analysis based on state purification



CV QKD

Features

- Quadrature encoding & homodyne detection
- Mode description of light
- Gaussian security proofs, optimality of Gaussian attacks
- Covariance matrix formalism (symplectic framework)

$$\boxed{K = I_{AB} - \chi_{BE}}$$

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

$$\chi_{BE} = S(\rho_E) - S(\rho_{E|B})$$

Purification: $S(\rho_E) = S(\rho_{AB})$ $\quad S(\rho_{E|B}) = S(\rho_{A|B})$

Von Neumann entropy:

$$S_\gamma = \sum_i G\left(\frac{\lambda_i - 1}{2}\right)$$

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x$$

Conditional states:

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

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

CV QKD

Features

- Quadrature encoding & homodyne detection
- Mode description of light
- Gaussian security proofs, optimality of Gaussian attacks
- Covariance matrix formalism (symplectic framework)

Details of security analysis

- E. Diamanti and A. Leverrier, Entropy 17, 6072 (2015) / arXiv:1506.02888
- VCU and R. Filip, Entropy 18, 20 (2016) / arXiv:1601.03105

CV QKD

Features

- Quadrature encoding & homodyne detection
- Mode description of light
- Gaussian security proofs, optimality of Gaussian attacks
- Covariance matrix formalism (symplectic framework)

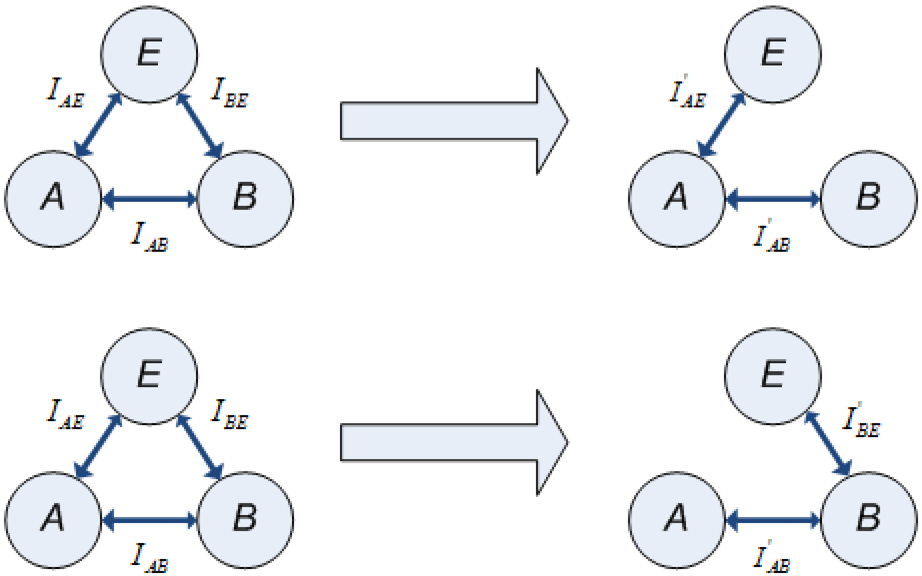
Details of security analysis

- E. Diamanti and A. Leverrier, Entropy 17, 6072 (2015) / arXiv:1506.02888
- VCU and R. Filip, Entropy 18, 20 (2016) / arXiv:1601.03105

Issues

- **Gaussian modulation** (possibly with a single modulator:
  VCU, F. Grosshans, Phys. Rev. A 92, 062337 (2015), but still..)
- **Channel estimation** (can be optimized,
  L. Ruppert, VCU, and R. Filip, Phys. Rev. A 90, 062310 (2014))

Key distillation

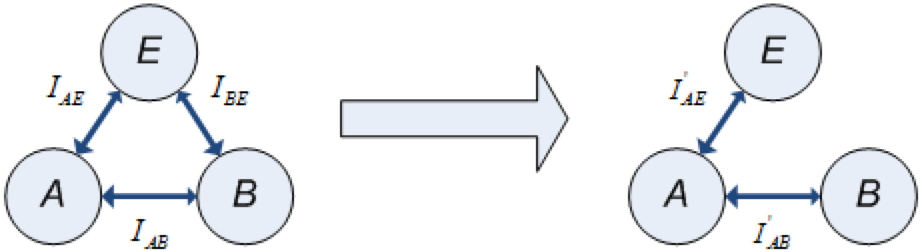


Key distillation: classical algorithms (data manipulation)

• error correction (producing identical data sequences)

• privacy amplification (decoupling Eve form a reference side of the protocol)

Key distillation



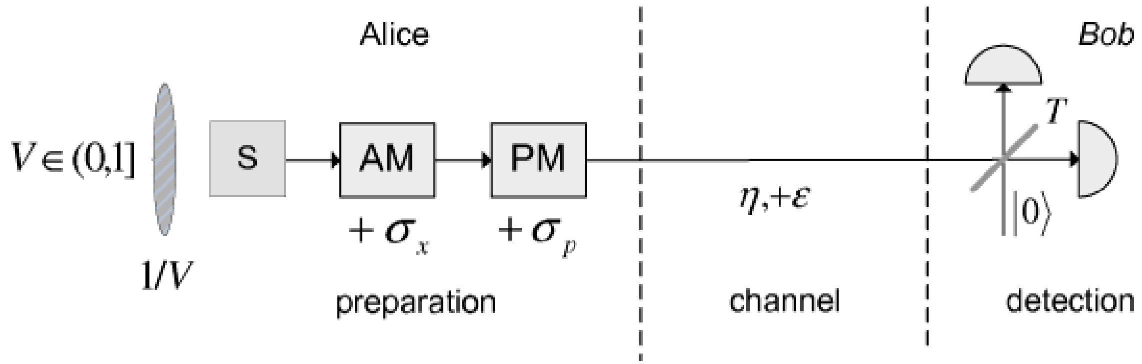
Problem: error correction is costly (reduces the mutual information)

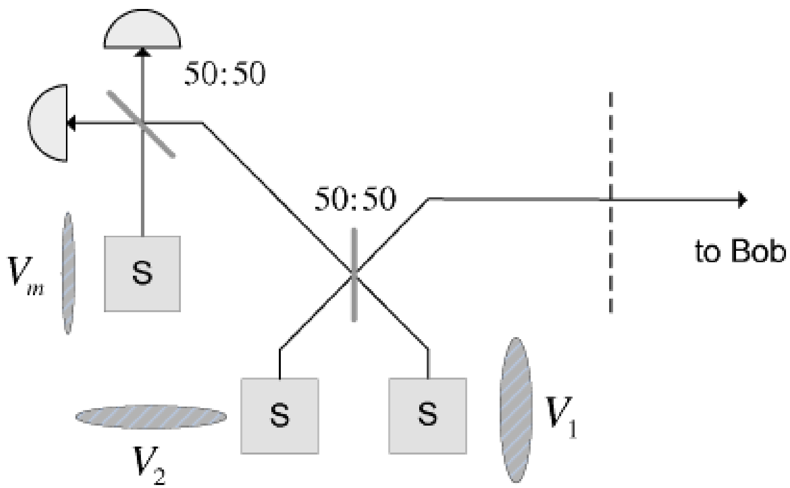
$$\boxed{K = \beta I_{AB} - I_{BE}} \quad \text{where} \quad \beta \in [0,1]$$

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

1. Squeezed-state protocol tolerates lower post-processing efficiencies





$$V_{1,2} = V + \sigma_x \pm \sqrt{\frac{(V+\sigma_x)(\sigma_x + V\sigma_p(V+\sigma_x))}{1+V\sigma_p}}$$

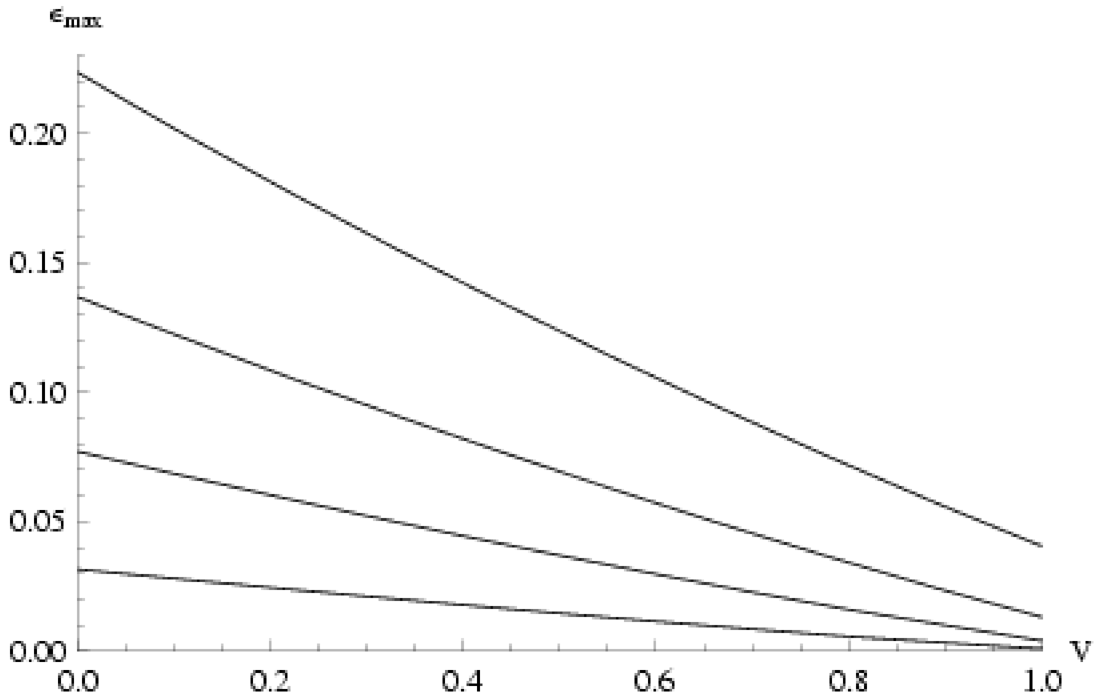
$$V_m = \frac{V^2\sigma_p(V+\sigma_x)}{\sigma_x(1+V\sigma_p)},$$

Generalized entanglement-based CV QKD scheme: arbitrary Gaussian modulation of an arbitrarily squeezed state

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

1. Squeezed-state protocol tolerates lower post-processing efficiencies

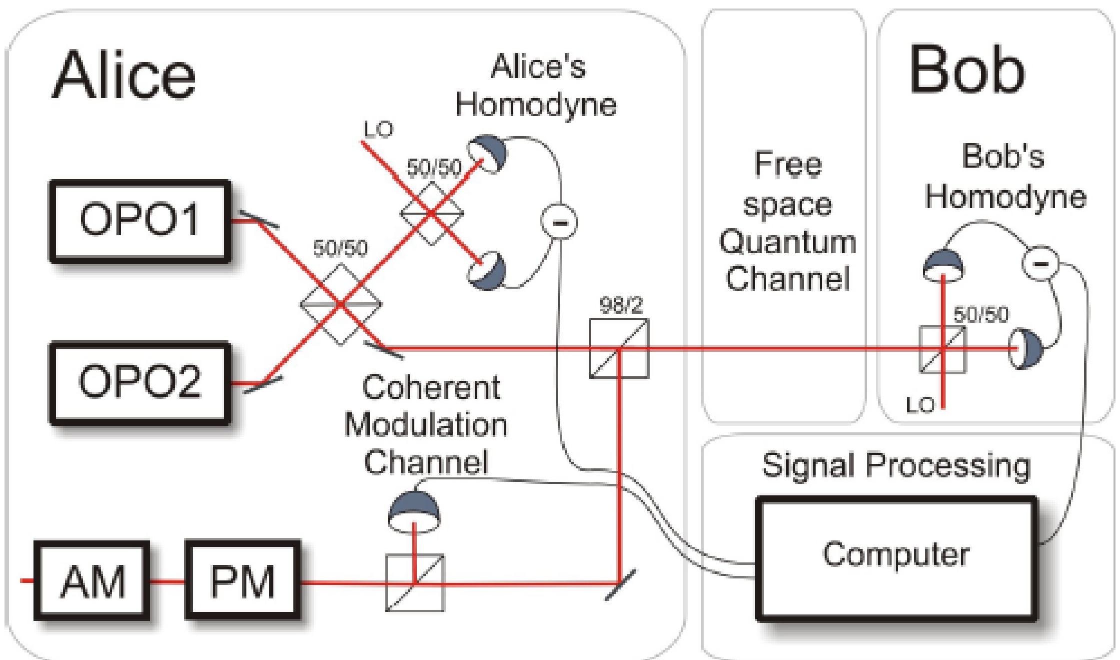


Maximum tolerable versus signal squeezing noise upon limited post-processing efficiency (from top to bottom: $\beta = 0.8, 0.6, 0.4, 0.2$)
[VCU and R. Filip, New J. Phys. 13, 113007 (2011)]

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

2. Squeezed-state protocol can tolerate more noise/loss than any coherent-state CV QKD protocol

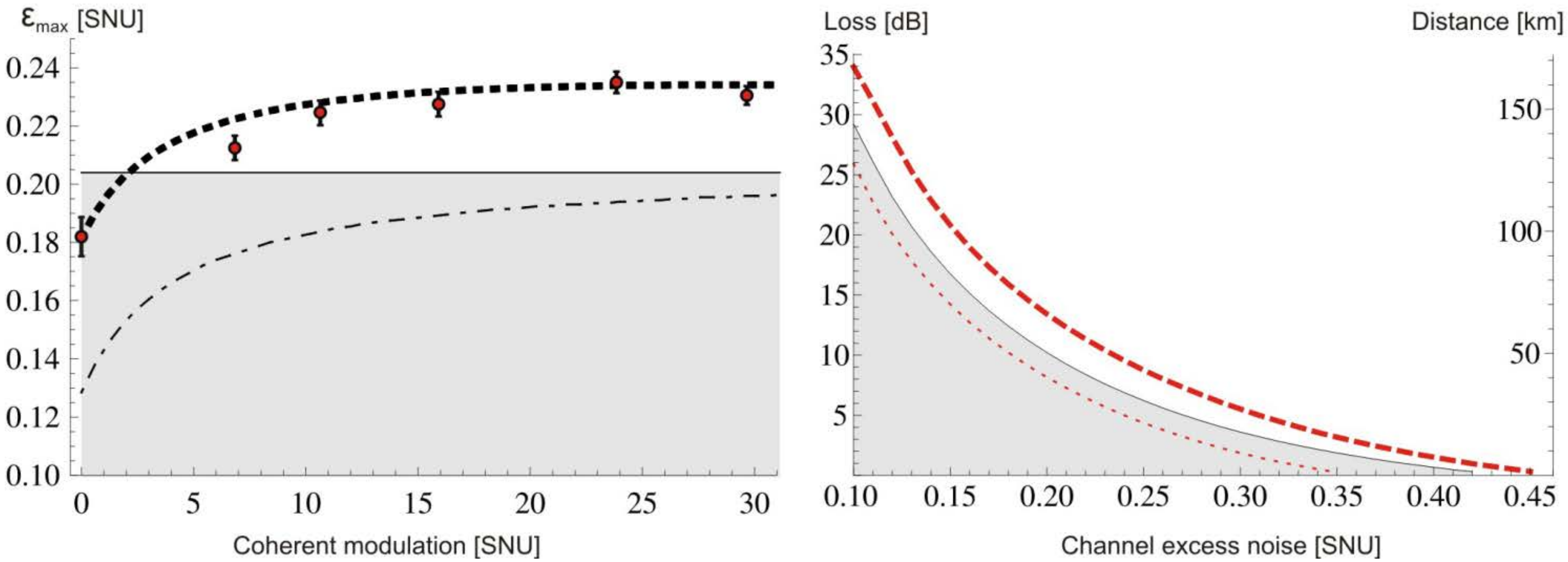


Sketch of the experiment, performed at DTU in Lyngby (group of Ulrik Andersen)

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

2. Squeezed-state protocol can tolerate more noise/loss than any coherent-state CV QKD protocol



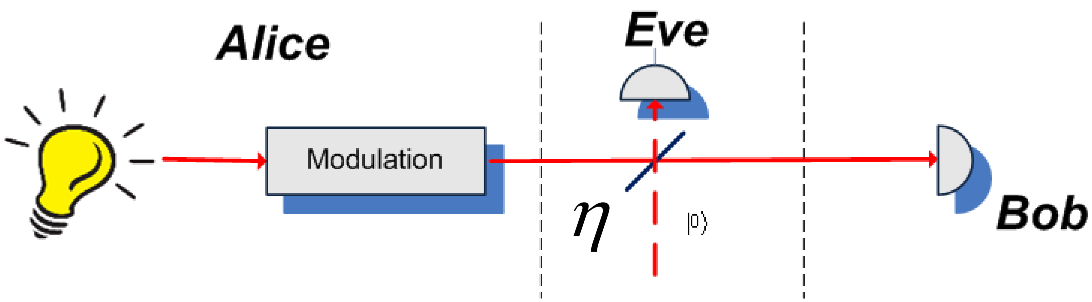
Maximum tolerable channel noise versus modulation (left) and maximum tolerable noise for given channel noise (right) for optimized coherent-state protocol (grey area) and squeezed-state (theory dashed lines + experimental points)

[L. Madsen, VCU, M. Lassen, R. Filip, U. Andersen, Nat. Comm. 3, 1083 (2012)]

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

3. Squeezed-state protocol can decouple an eavesdropper from a lossy channel



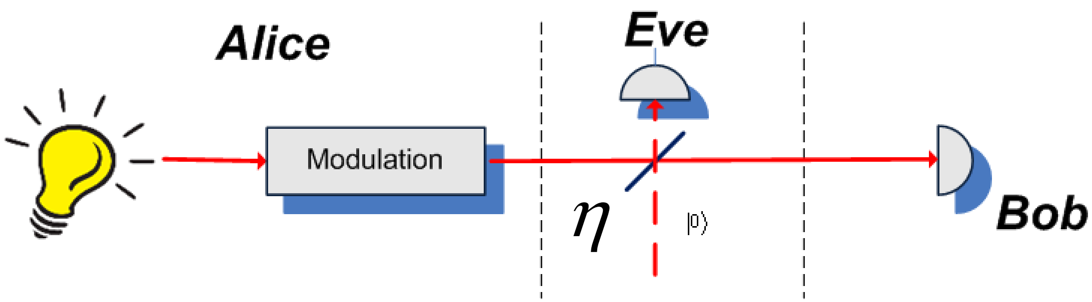
$$\begin{pmatrix} a \\ b \end{pmatrix}_{out} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}_{in}$$

$$\begin{pmatrix} V_S & 0 & 0 & 0 \\ 0 & V_S^{(p)} & 0 & 0 \\ 0 & 0 & V_E & 0 \\ 0 & 0 & 0 & V_E^{(p)} \end{pmatrix} \rightarrow \begin{pmatrix} \eta V_S + (1-\eta)V_E & 0 & \sqrt{\eta(1-\eta)}(V_E - V_S) & 0 \\ 0 & \eta V_S^{(p)} + (1-\eta)V_E^{(p)} & 0 & \sqrt{\eta(1-\eta)}(V_E^{(p)} - V_S^{(p)}) \\ \sqrt{\eta(1-\eta)}(V_E - V_S) & 0 & \eta V_E + (1-\eta)V_S & 0 \\ 0 & \sqrt{\eta(1-\eta)}(V_E^{(p)} - V_S^{(p)}) & 0 & \eta V_E^{(p)} + (1-\eta)V_S^{(p)} \end{pmatrix}$$

Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

3. Squeezed-state protocol can decouple an eavesdropper from a lossy channel



Correlation of the outputs of a beamsplitter: $C_{BE} \propto V_S - V_E = (V+\sigma) - 1 = 0$

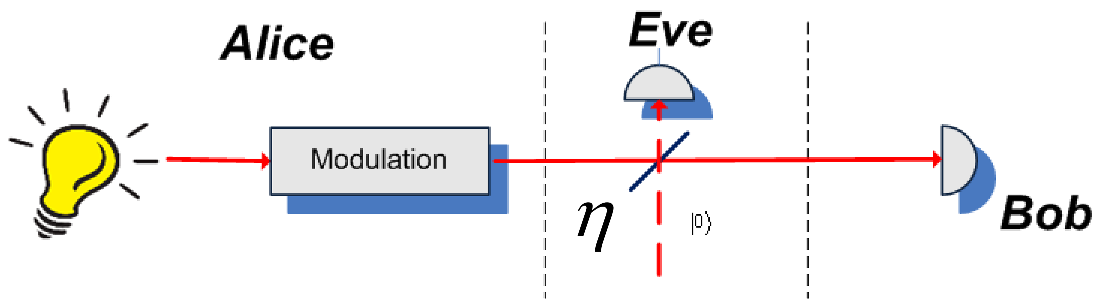
Condition for vanishing of Holevo bound: $\boxed{\sigma = 1 - V}$

$$\begin{pmatrix} V_S & 0 & 0 & 0 \\ 0 & V_S^{(p)} & 0 & 0 \\ 0 & 0 & V_E & 0 \\ 0 & 0 & 0 & V_E^{(p)} \end{pmatrix} \to \begin{pmatrix} \eta V_S + (1-\eta)V_E & 0 & \sqrt{\eta(1-\eta)}(V_E - V_S) & 0 \\ 0 & \eta V_S^{(p)} + (1-\eta)V_E^{(p)} & 0 & \sqrt{\eta(1-\eta)}(V_E^{(p)} - V_S^{(p)}) \\ \sqrt{\eta(1-\eta)}(V_E - V_S) & 0 & \eta V_E + (1-\eta)V_S & 0 \\ 0 & \sqrt{\eta(1-\eta)}(V_E^{(p)} - V_S^{(p)}) & 0 & \eta V_E^{(p)} + (1-\eta)V_S^{(p)} \end{pmatrix}$$

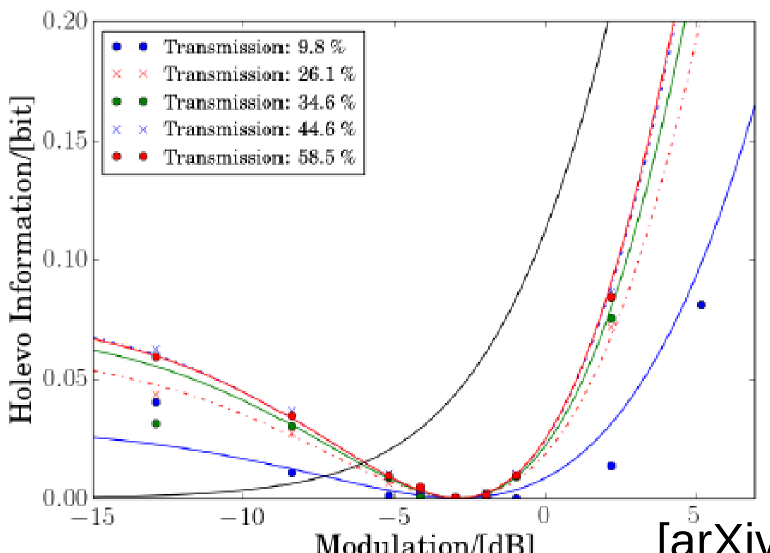
Role of squeezing in CV QKD

If we apply modulation independently on the amount of squeezing and optimize it…

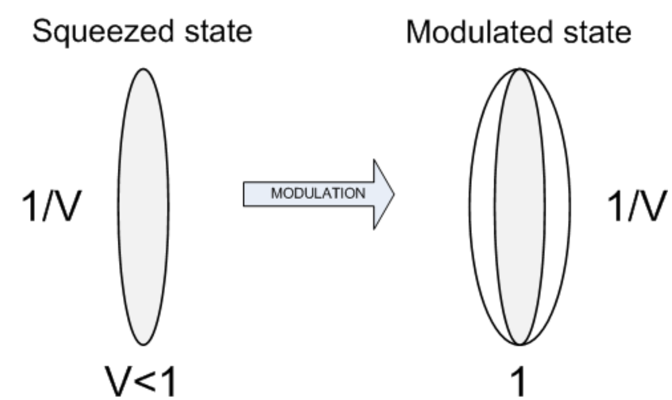
3. Squeezed-state protocol can decouple an eavesdropper from a lossy channel



Condition for vanishing of Holevo bound: $\boxed{\sigma = 1 - V}$



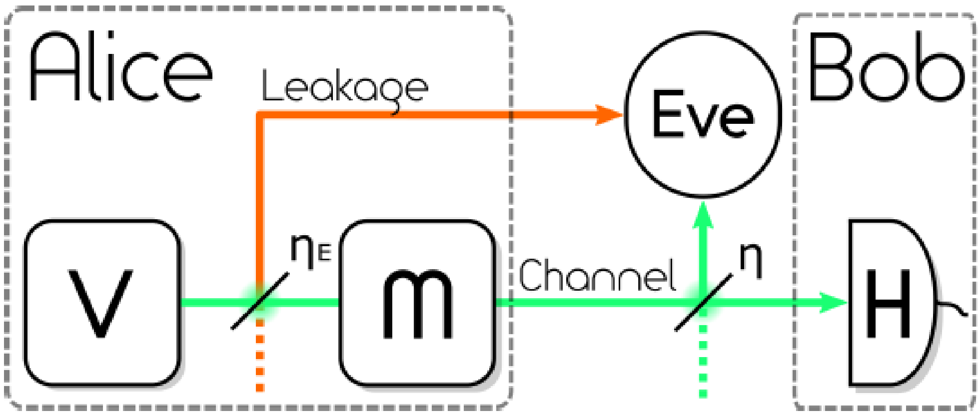
[arXiv:1408.4566]



Role of squeezing in CV QKD

…but if a pre-modulation lossy side channel on the sender side is present…

Squeezed-state protocol is more sensitive to the side-channel loss

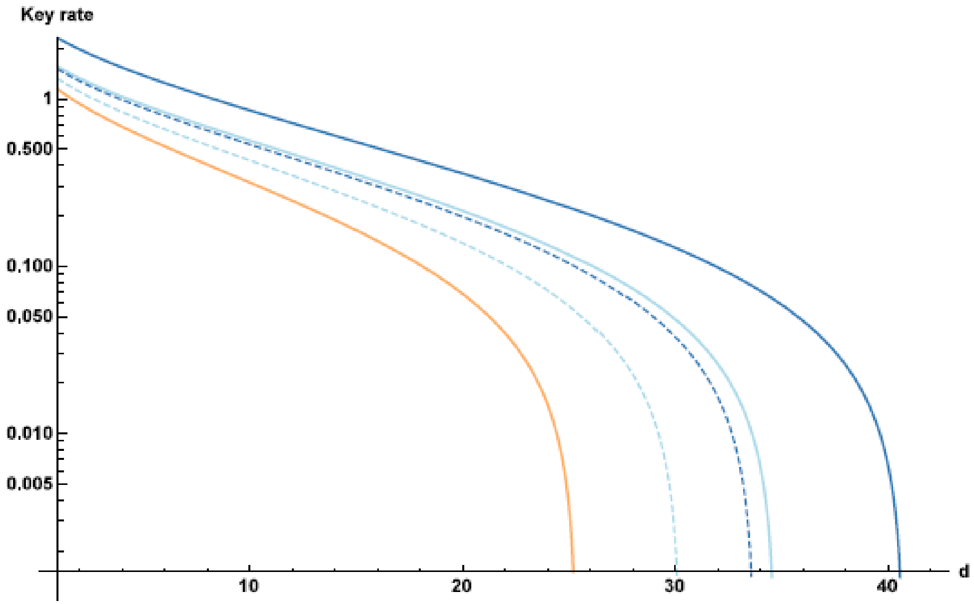


Lossy side channel prior to state modulation

Role of squeezing in CV QKD

…but if a pre-modulation lossy side channel on the sender side is present…

Squeezed-state protocol is more sensitive to the side-channel loss

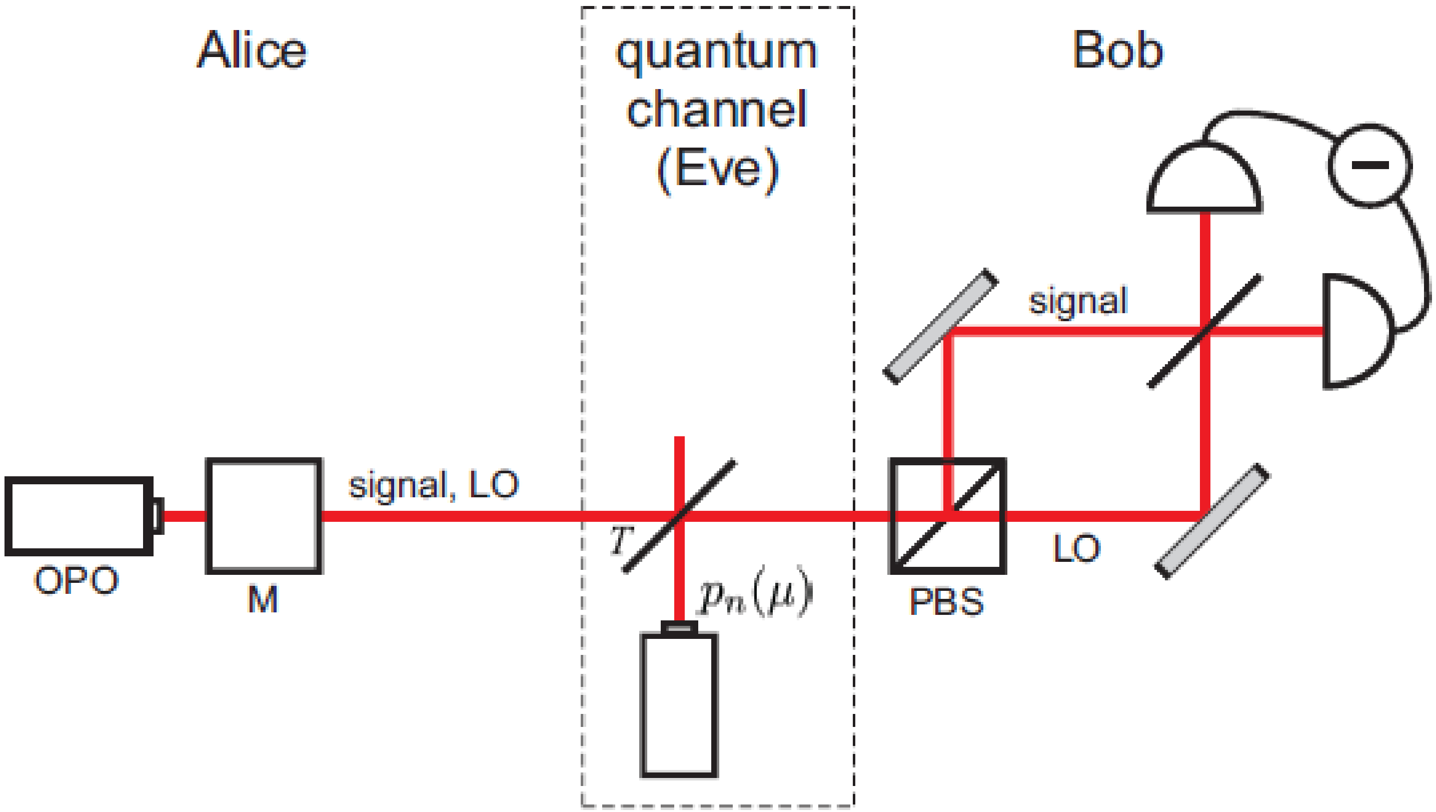


Key rate vs distance without (solid lines) and with a 50% pre-modulation side channel.

Blue: squeezed states (0.1, 0.5 SNU), orange: coherent-state protocol (no effect).

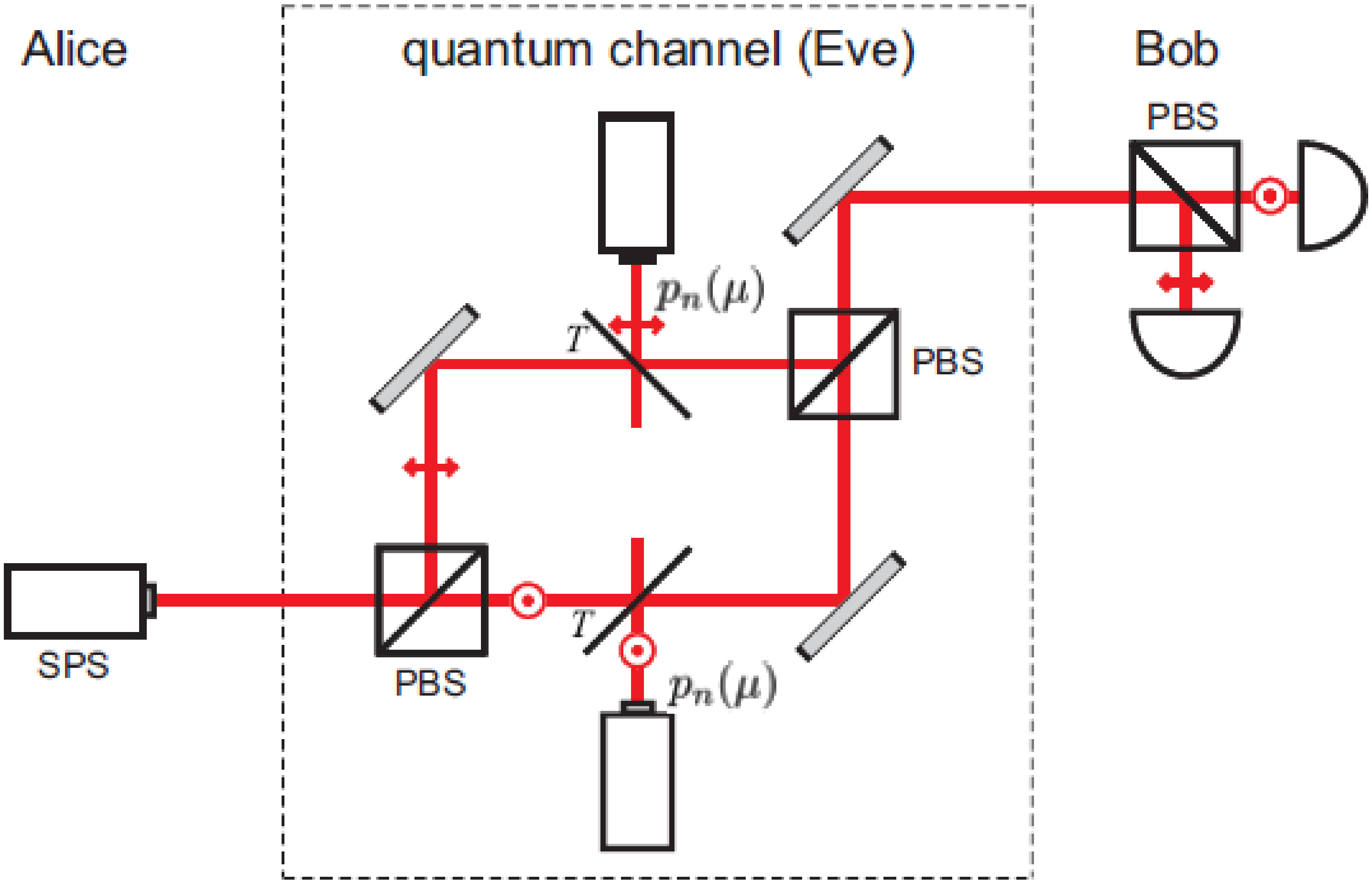
[I. Derkach, VCU, and R. Filip, PRA 93, 032309 (2016) + in preparation]

CV vs DV



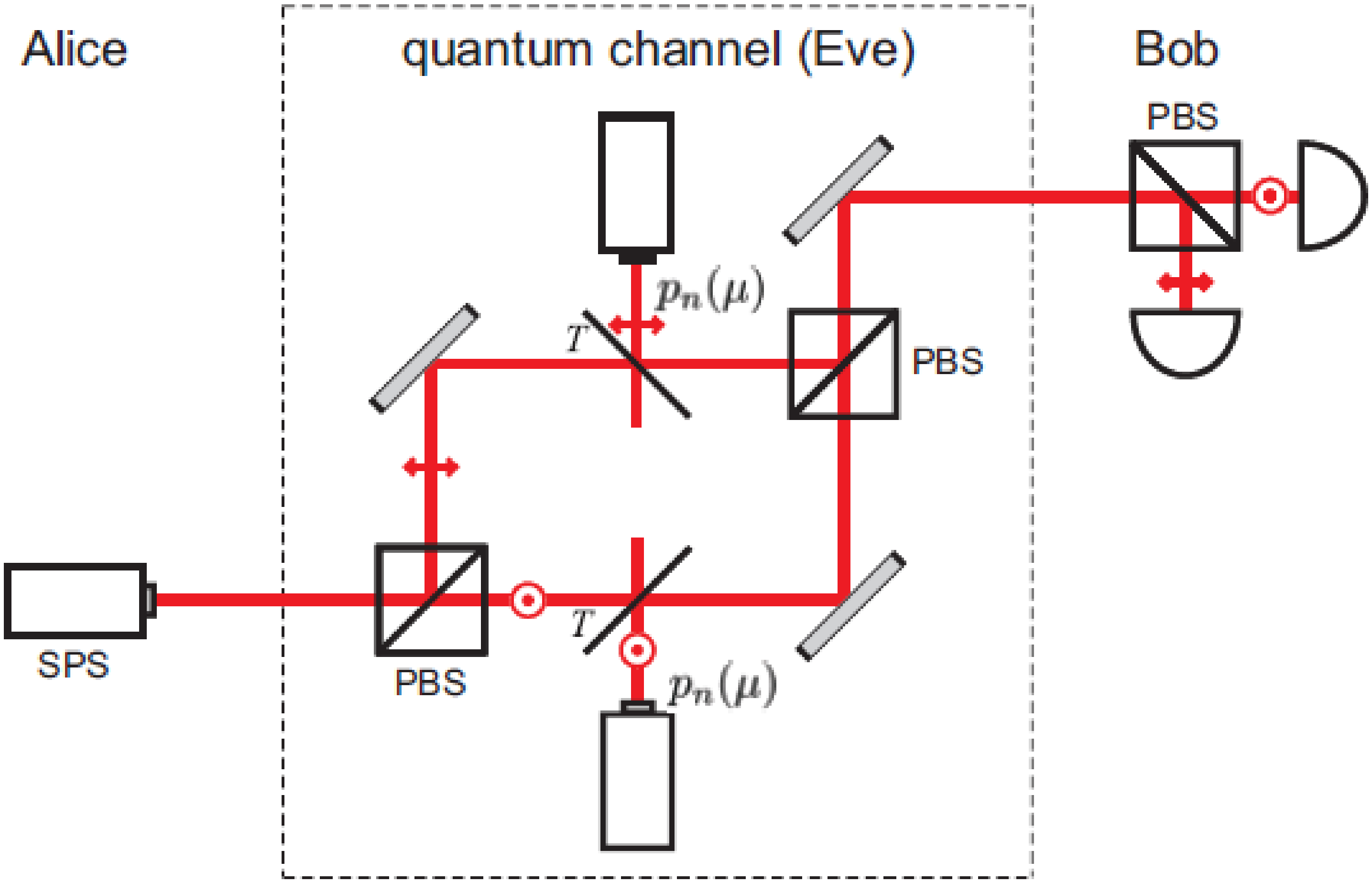
Typical noise model used in CV QKD and parametrized by a mean photon number

CV vs DV



The same noise model applied to DV QKD protocol

CV vs DV



Photonic noise:

$$p_n(\mu) = \frac{\mu^n}{(\mu+1)^{n+1}}$$

Quadrature noise:

$$W = 2\mu + 1$$

CV vs DV

DV security analysis

$$K^{(BB84)} = p_{exp} \max[0, 1 - 2H(Q)]$$

$$K^{(6state)} = p_{exp} \max\left[0, 1 - F(Q)\right]$$

$$F(Q) = -\left(1 - \frac{3Q}{2}\right) \log_2 \left(1 - \frac{3Q}{2}\right) - \frac{3Q}{2} \log_2 \frac{Q}{2}$$

[B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005);
R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005)]

CV vs DV

Evaluation of QBER

Click on a “right” detector along with ***k*** noise photons on the “right” and ***l*** noise photons on the “wrong” detector:

$$p_+(k,l) = T\pi_k(T)\pi_l(T)$$

Click on a “wrong” detector: $p_-(k,l) = (1-T)\pi_k(T)\pi_l(T)$

Where $\pi_k(T) = \sum_{n=k}^{\infty} p_n(\mu)\binom{n}{k}(1-T)^k T^{n-k}$

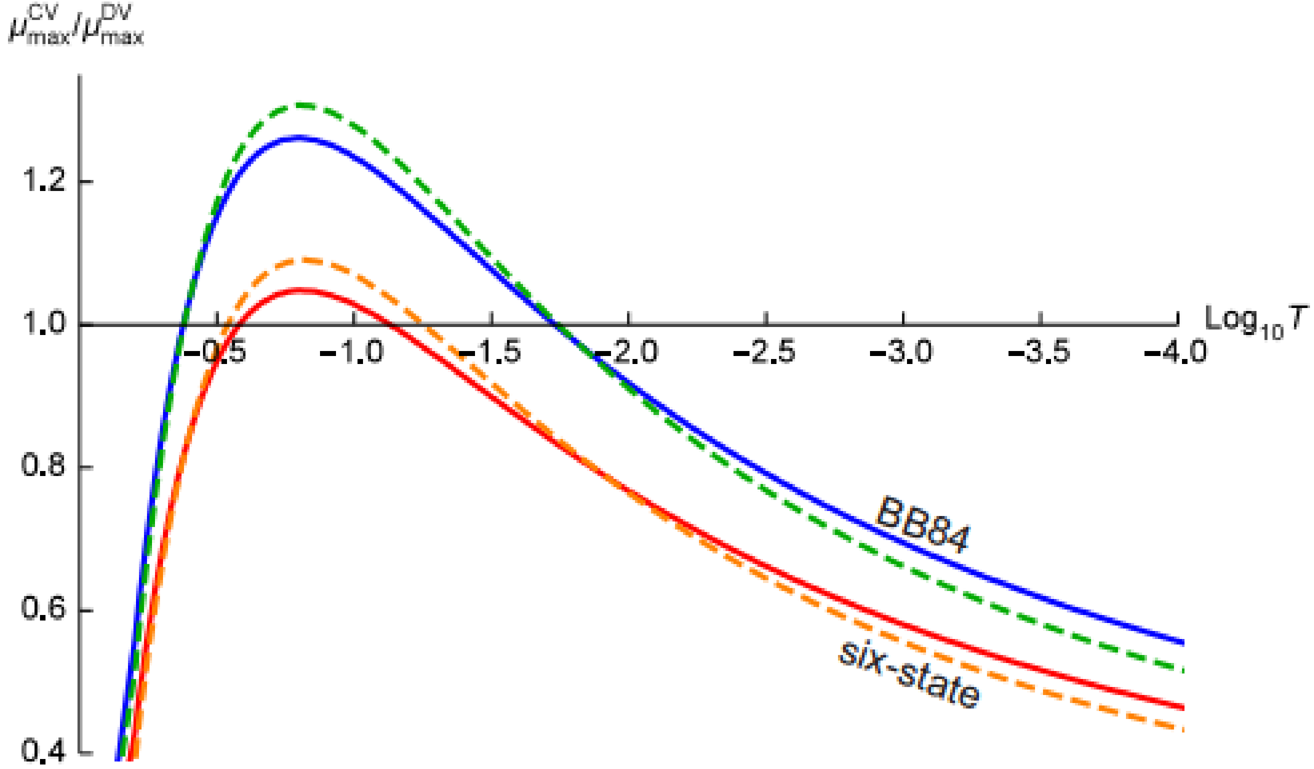
[VCU, M. G. A. Paris, Phys. Lett. A 374, 1342 (2010)]

Expected probability of accepting a given event:

$$p_{exp} = \sum_{k=0}^{\infty} p_+(k,0) + \sum_{k=1}^{\infty} p_-(k,0) + \sum_{l=1}^{\infty} p_-(0,l)$$

then $Q = \dfrac{\sum_{l=1}^{\infty} p_-(0,l)}{p_{exp}}$

CV vs DV



Comparison between robustness to noise in DV and CV

CV vs DV

Analytical result for CV:

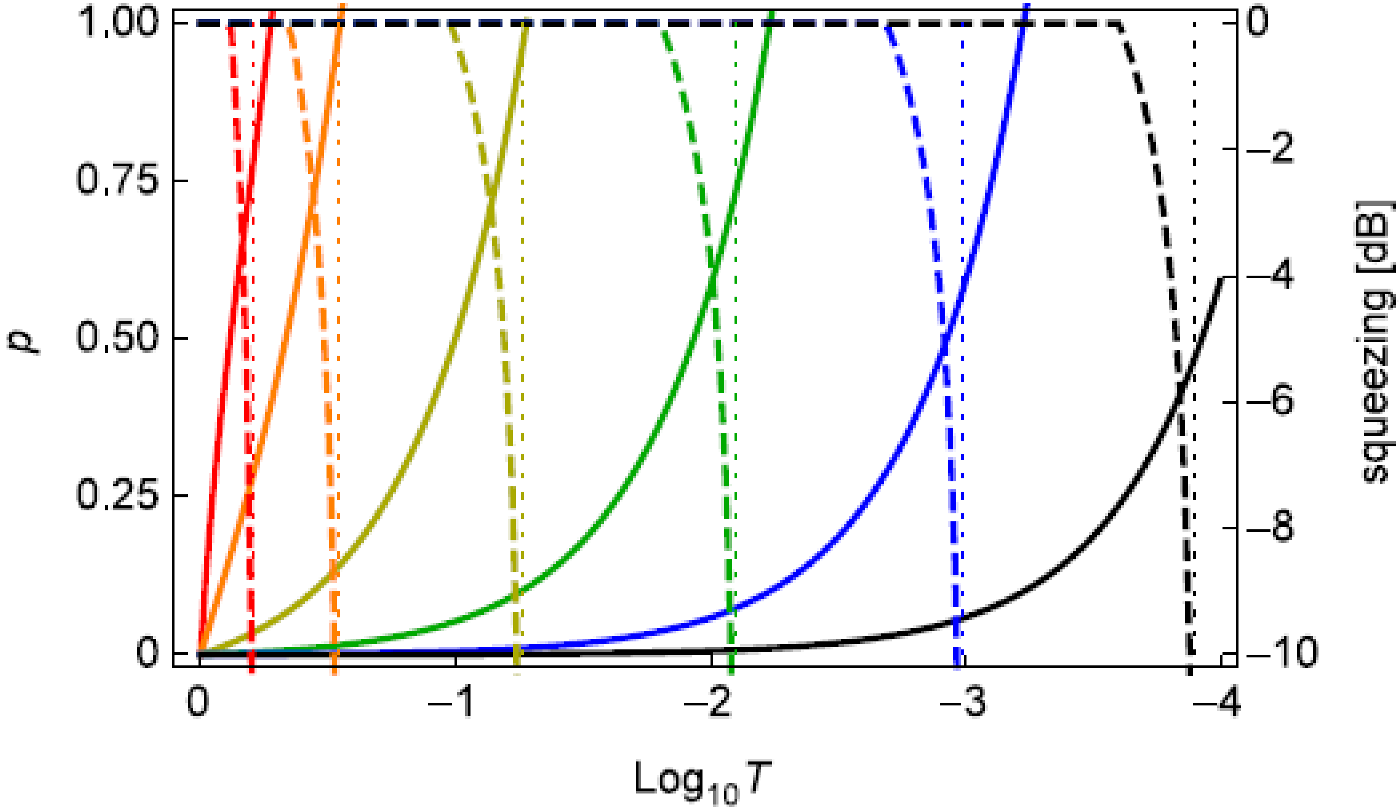
$$\mu_{max}(T) = \exp[1 + W_{-1}(-T/e)]$$

Analytical result for DV:

$$\mu_{max}^{DV}(T) = \frac{TQ_{\mathrm{th}}}{1 - 2Q_{\mathrm{th}}}$$

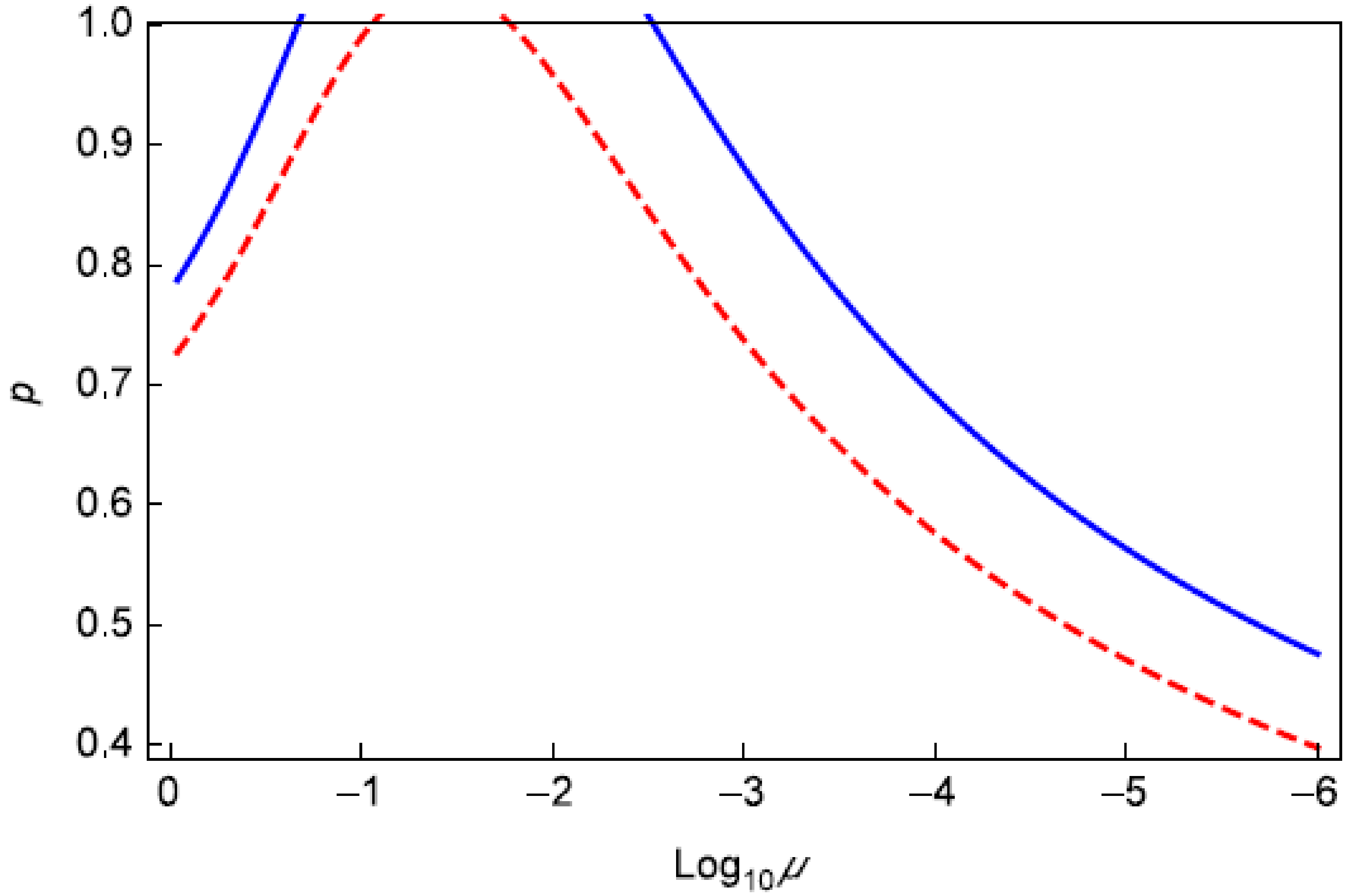
($Q_{th} \approx 12.6\%$ for BB84)

CV vs DV



Requirements on nonclassicality of the sources for CV and DV in noisy channels

CV vs DV



How good shall be the single-photon DV source to beat any CV protocol

[M. Lasota, R. Filip, VCU, arXiv:1602.03122]

…and much more:

- For CV squeezing is also helpful in fluctuating channels (test in progress)

- Squeezed states improve channel estimation [L. Ruppert, VCU, and R. Filip, Phys. Rev. A 90, 062310 (2014)]

- For DV in noisy channels non-Gaussianity can indicate the suitability of a channel to QKD (nonclassicality is not sufficient) [arXiv:1603.06620]

…and much more:

- For CV squeezing is also helpful in fluctuating channels (test in progress)
- Squeezed states improve channel estimation [L. Ruppert, VCU, and R. Filip, Phys. Rev. A 90, 062310 (2014)]
- For DV in noisy channels non-Gaussianity can indicate the suitability of a channel to QKD (nonclassicality is not sufficient) [arXiv:1603.06620]

What next?

- Incorporate decoy-state DV QKD
- Entanglement-based schemes
- Better witnesses for channel verification

To sum up:

- In CV QKD nonclassicality and optimal use of resources is helpful, unless side-channel loss on the sender side is present (and channel noise is low).

- Single-photon DV QKD can be more robust to channel noise than any squeezed-state CV QKD.

Acknowledgements

- Radim Filip, Laszlo Ruppert, Ivan Derkach (Olomouc)
- Ulrik Andersen, Mikael Lassen, Lars Madsen, Christian Scheffmann (Lyngby)
- Christoph Marquardt, Bettina Heim, Christian Peuntinger (Erlangen)
- Mikolaj Lasota (Torun)

Thank you for attention!

usenko@optics.upol.cz