Continuous- and Discrete-Variable Quantum Key Distribution with Nonclassical Light Over Noisy Channels

Vladyslav Usenko, Mikolaj Lasota, Radim Filip

Department of Optics, Palacký University, Olomouc, Czech Republic

Outline

- Motivation: why QKD?
- Discrete vs Continuous variables of light
- Model of channel noise
- Comparison of Discrete & Continuous variables

Motivation

Alice and Bob would like to communicate securely

Motivation

Alice and Bob would like to communicate securely

Asymmetrical cryptosystems are potentially vulnerable

Motivation

Alice and Bob would like to communicate securely

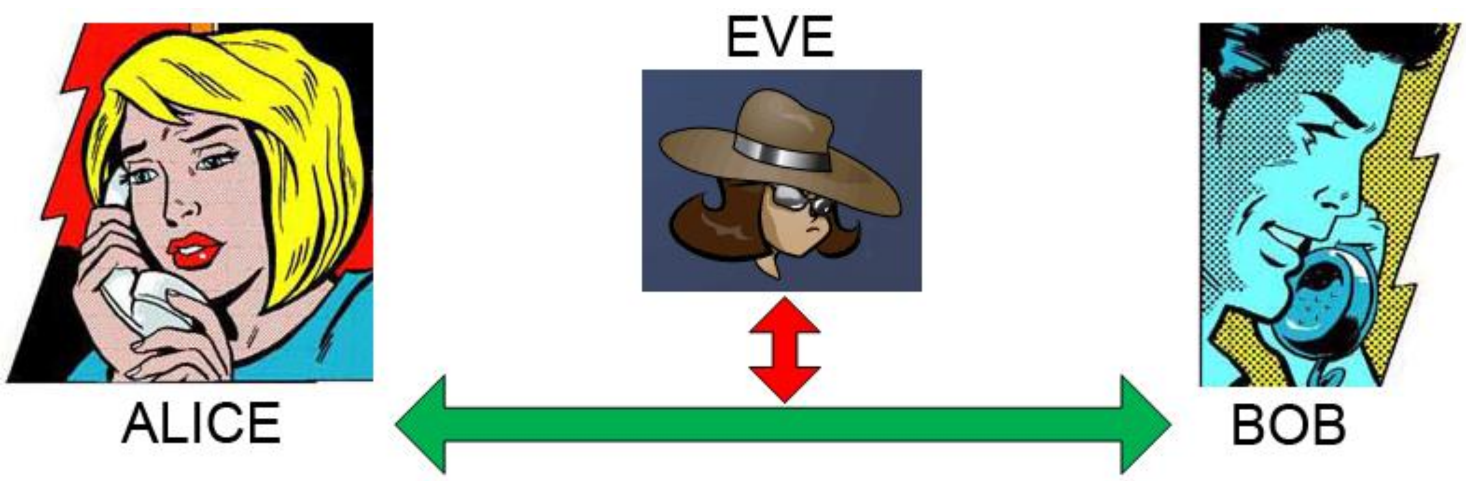
One-time pad (Vernam, 1919) is secure (Shannon, 1949), but needs secret keys

Motivation

Alice and Bob would like to communicate securely

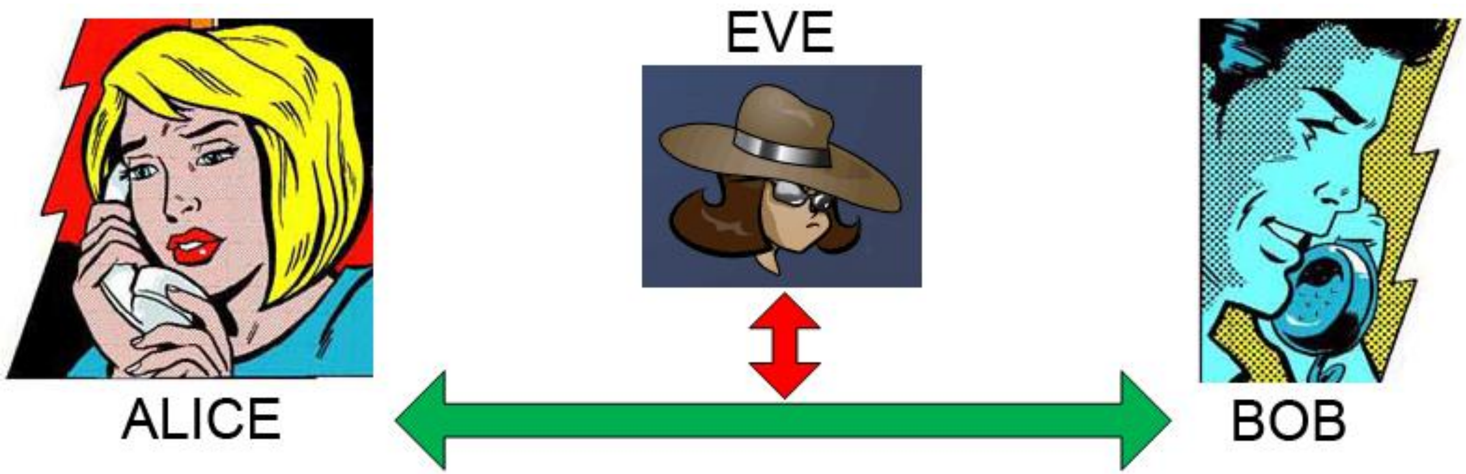
Key distribution: can be solved by mathematical methods
or by involving laws of physics -> **quantum key distribution**

Quantum key distribution



The idea of QKD: detect eavesdropping attempts and estimate security of the key.

Quantum key distribution

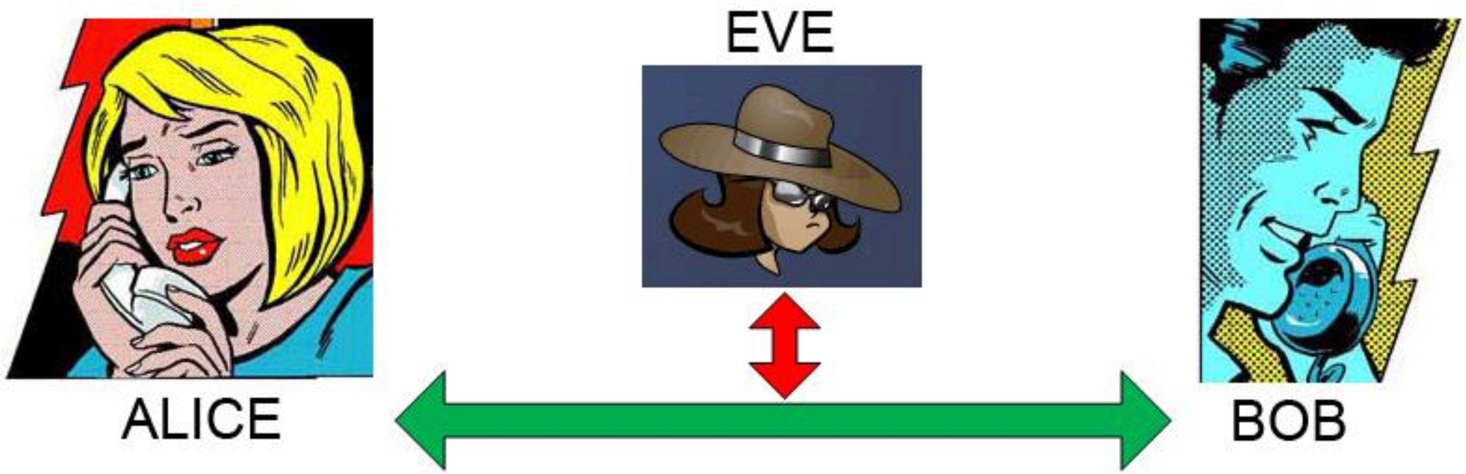


The idea of QKD: detect eavesdropping attempts and estimate security of the key.

Two main families of QKD protocols:

- **Discrete-variable, DV**
- **Continuous-variable, CV**

Quantum key distribution

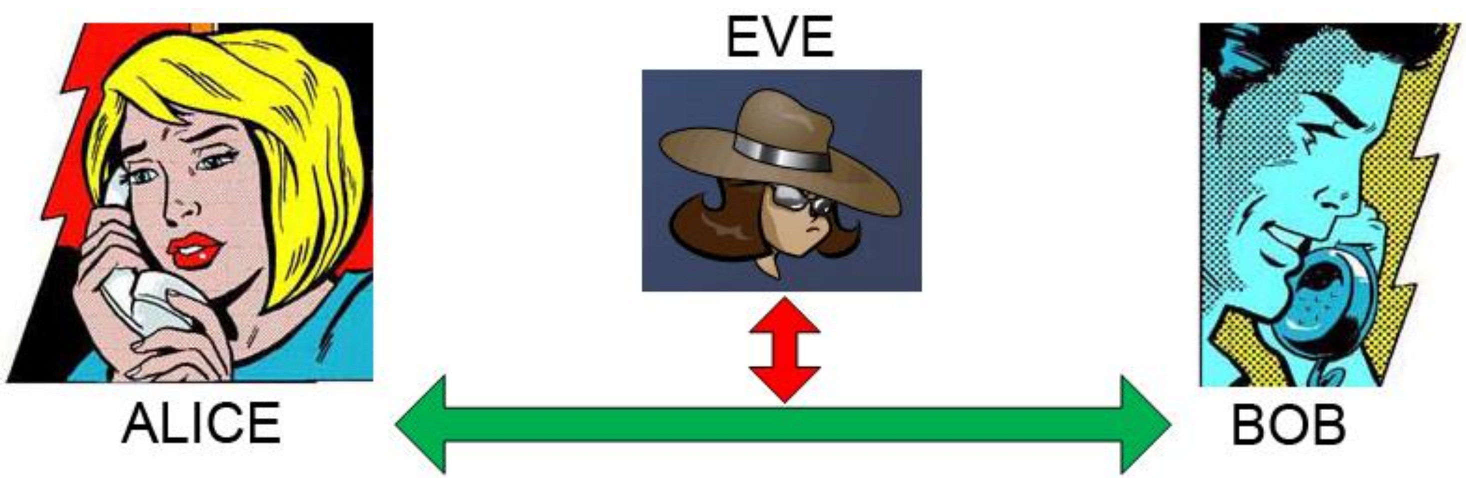


The idea of QKD: detect eavesdropping attempts and estimate security of the key.

Two main families of QKD protocols:

- **Discrete-variable, DV** (“particle-like” properties of light)
- **Continuous-variable, CV** (“wave-like” properties of light)

Quantum key distribution



Security analysis in QKD:

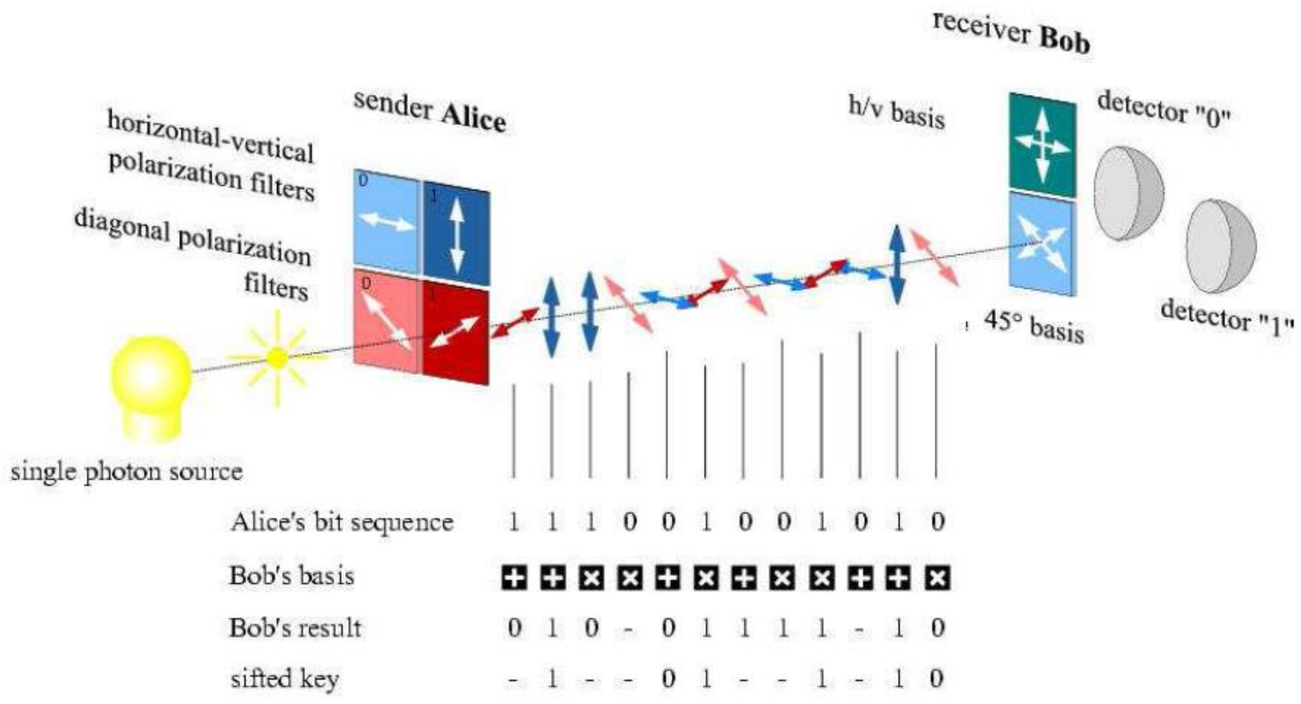
$$I_{AB} = H(A) + H(B) - H(A,B) = H(A) - H(A|B) = H(B) - H(B|A)$$

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

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

[*Csiszár, Körner, IEEE Trans. Inf. Theor., IT-24, 339-348 (1978)*]

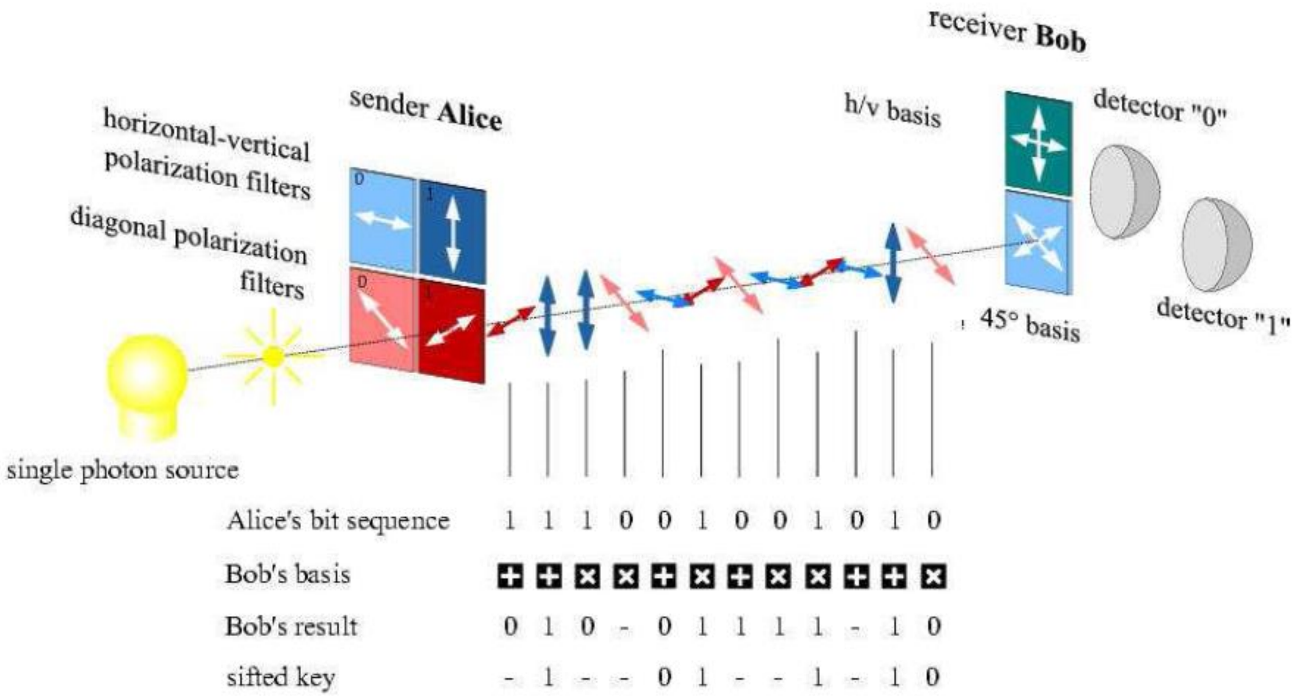
Discrete variables



Scheme of the BB84 protocol:

- Alice chooses a polarization basis
- Alice prepares a single photon in a given polarization state
- Bob chooses the detection basis
- Bob measures the state of the photon in a given basis
- Alice and Bob perform key sifting, error correction and privacy amplification

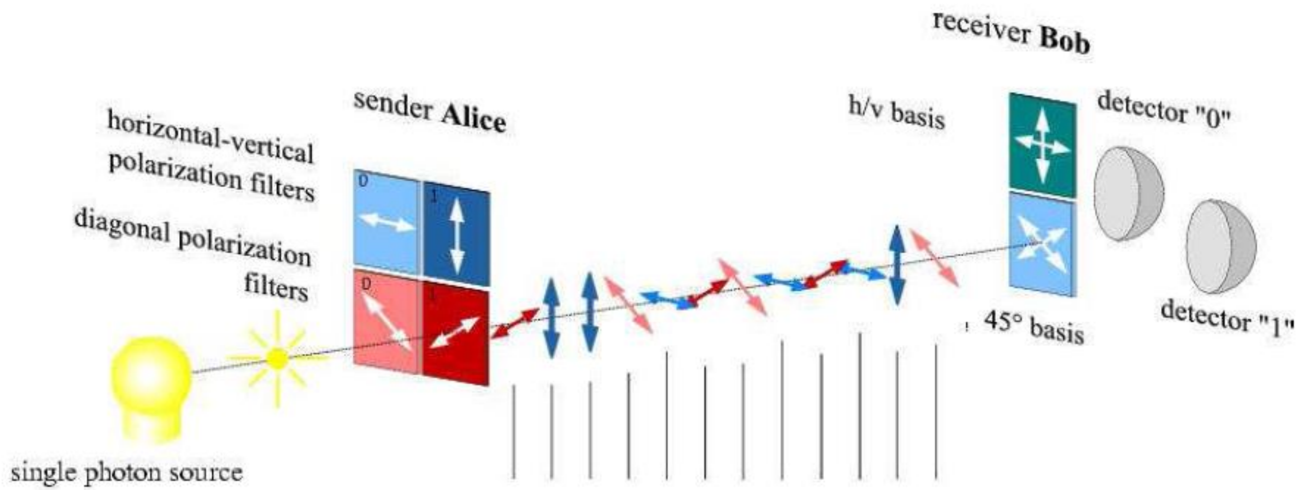
Discrete variables



Security analysis:

Estimate upper bound on Eve's information from the amount of errors (QBER).
For collective attacks bounds on QBER were derived (~12.6% for BB84)
[B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005)]

Discrete variables



Alice's bit sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's basis	+	+	×	×	+	×	+	×	×	+	+	×
Bob's result	0	1	0	-	0	1	1	1	1	-	1	0
sifted key	-	1	-	-	0	1	-	-	1	-	1	0

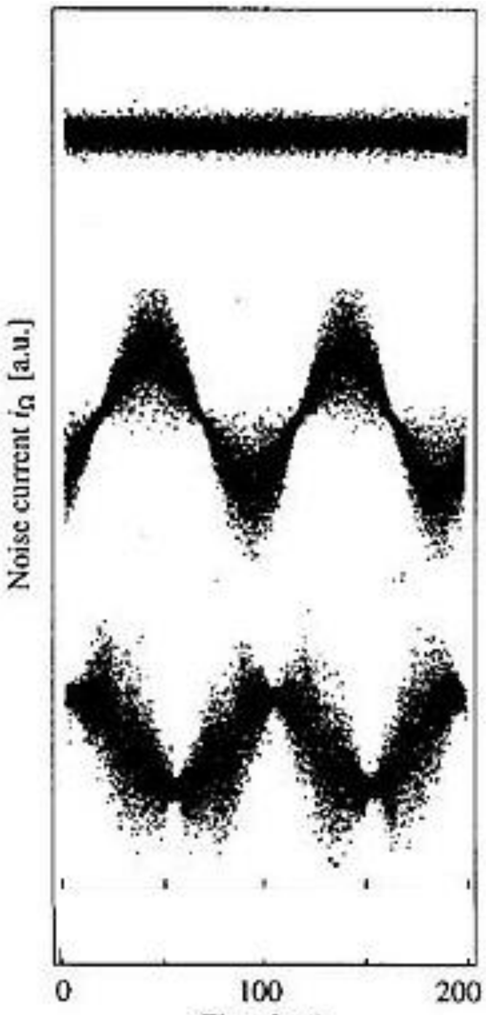
Physical systems: single photons (strongly nonclassical)
Detection method: photon counting
Issues:

- demanding and imperfect generation (in practice – weak laser pulses)
- imperfect detection (dark counts)
- lossy channels, stray light, implementation loopholes

Current achievements: tested in long-distance fiber and free-space channels (>100 km), devices are being sold and further developed

Continuous variables

Quadrature observables: in-phase and out-of-phase components of the electric field amplitude of a given mode (x- and p- quadratures).

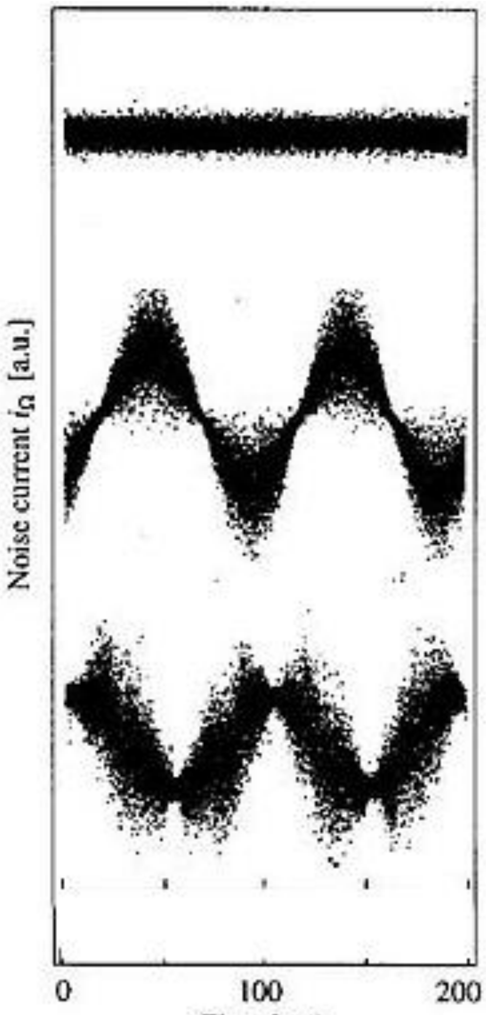


Coherent/vacuum states: have the same noise (quantum fluctuations) in both the quadratures (called shot noise)

Squeezed states: have noise in one of the quadratures suppressed below shot noise

Continuous variables

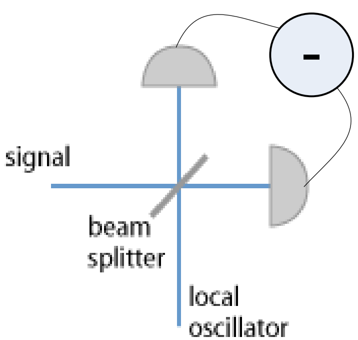
Quadrature observables: in-phase and out-of-phase components of the electric field amplitude of a given mode (x- and p- quadratures).



Coherent/vacuum states: have the same noise (quantum fluctuations) in both the quadratures (called shot noise)

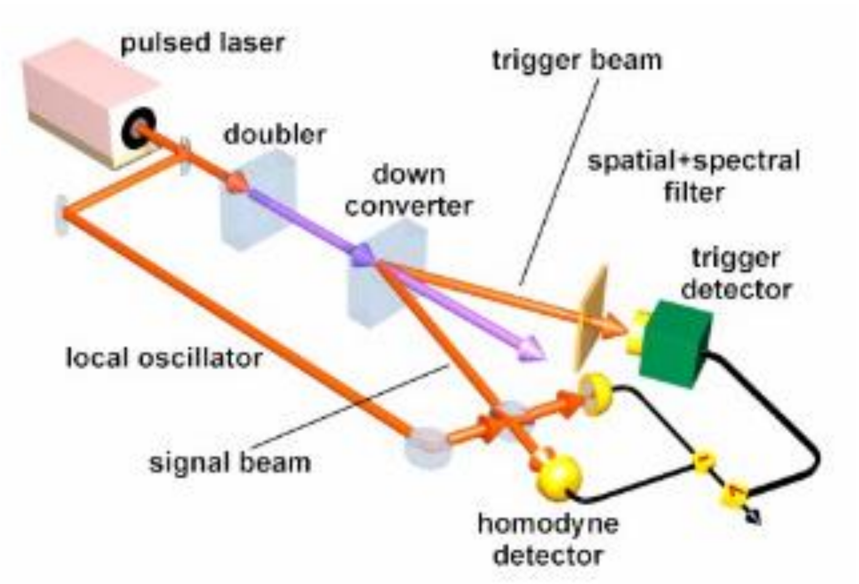
Squeezed states: have noise in one of the quadratures suppressed below shot noise

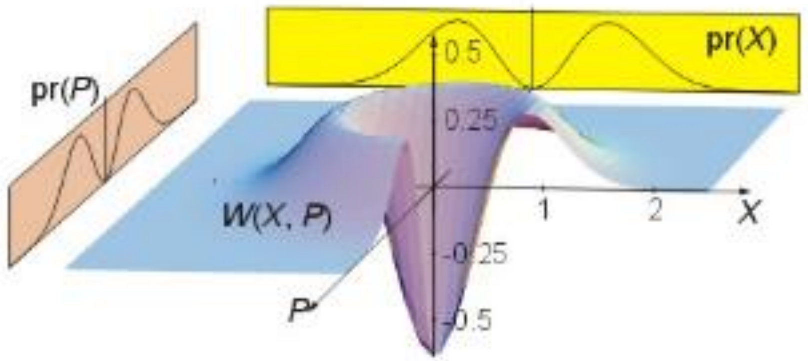
Quadratures can be measured using **homodyne detection**:



Continuous variables

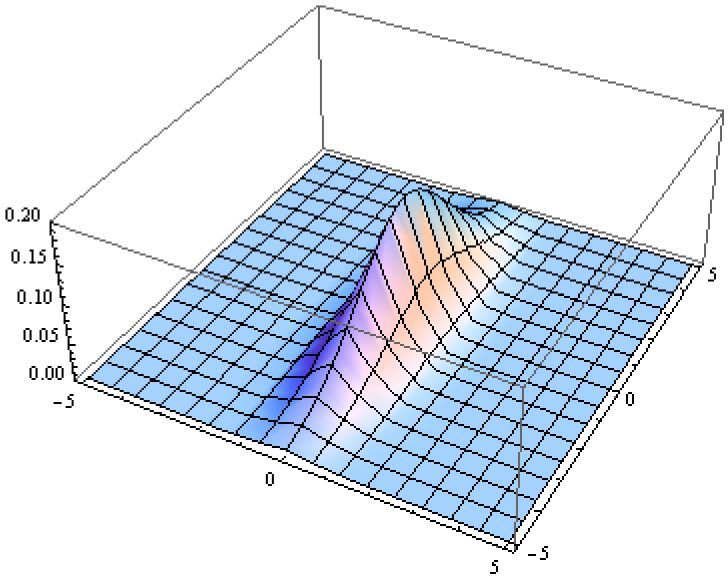
Quadrature distribution of a single-photon state:

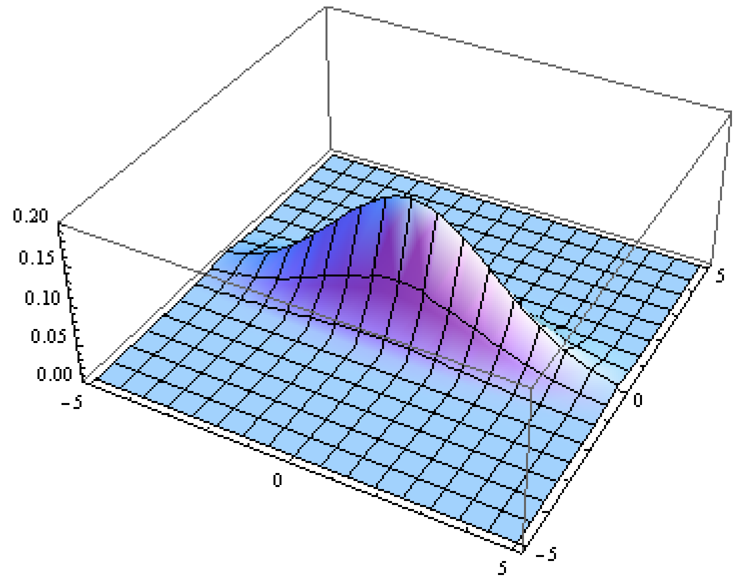




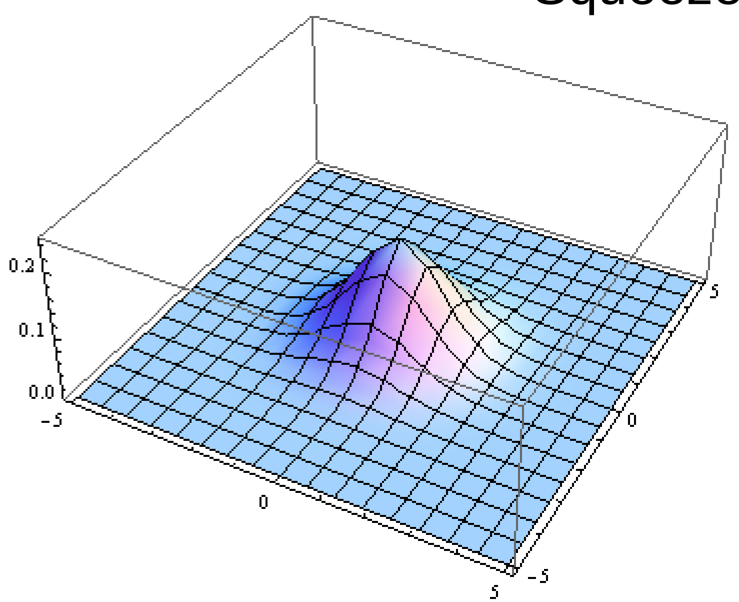
Negative quasiprobability distribution: clearly nonclassical feature

[Lvovsky et al., Phys. Rev. Lett. 87, 050402 (2001)]

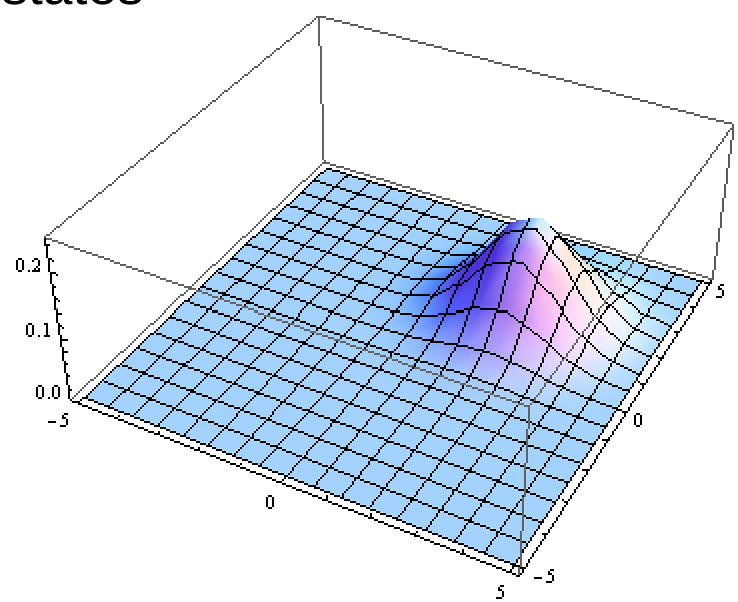




Squeezed states

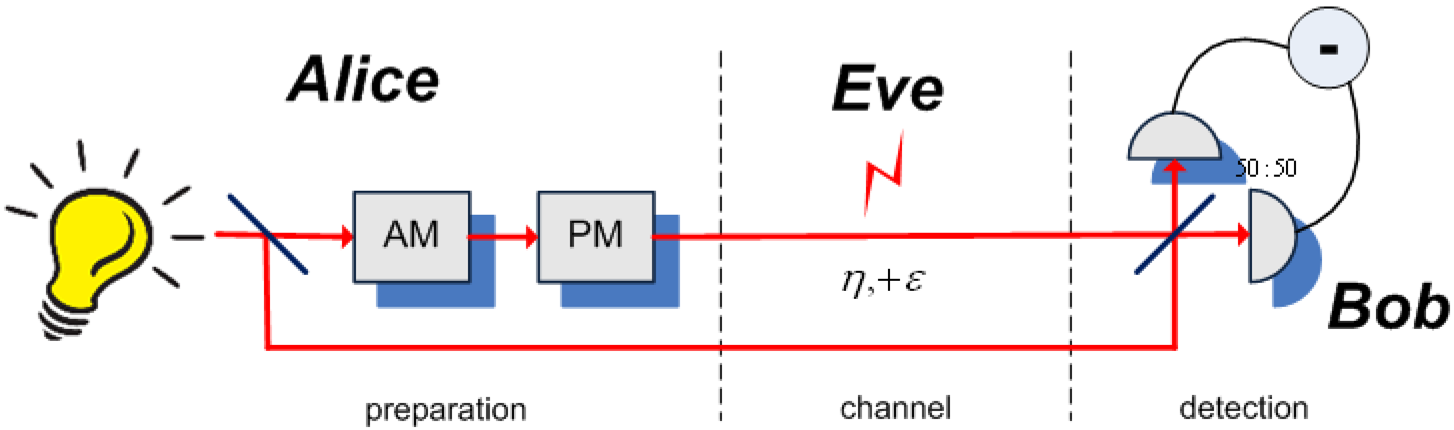


Vacuum state



Coherent state

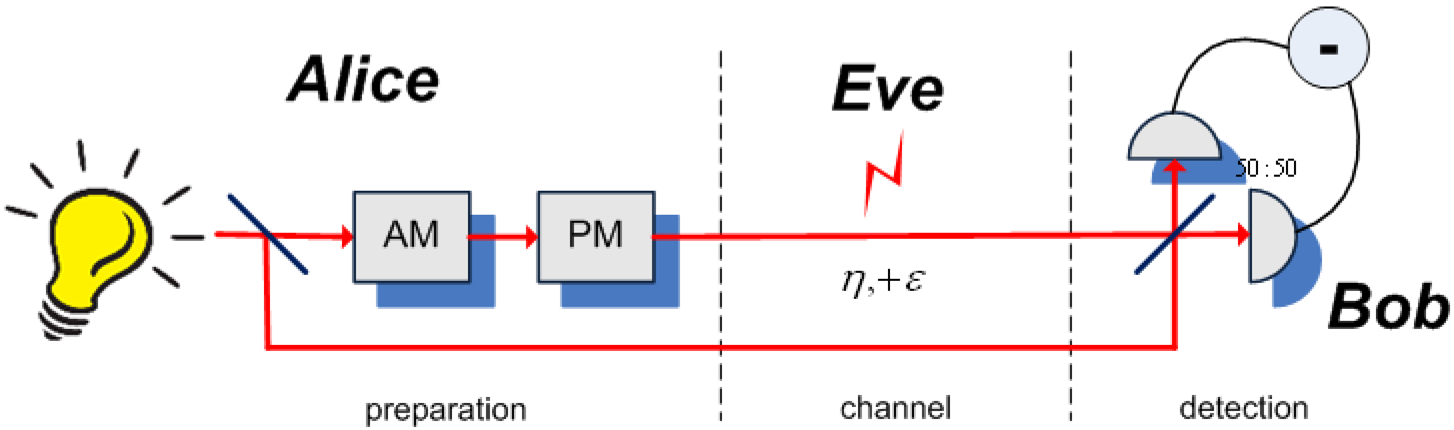
Continuous variables



Scheme of the squeezed-state protocol:

- Alice chooses a squeezing direction
- Alice prepares a respective squeezed state and displaces it randomly
- Bob chooses the detection basis
- Bob measures the state of the mode in a given basis
- Alice and Bob perform key sifting, error correction and privacy amplification

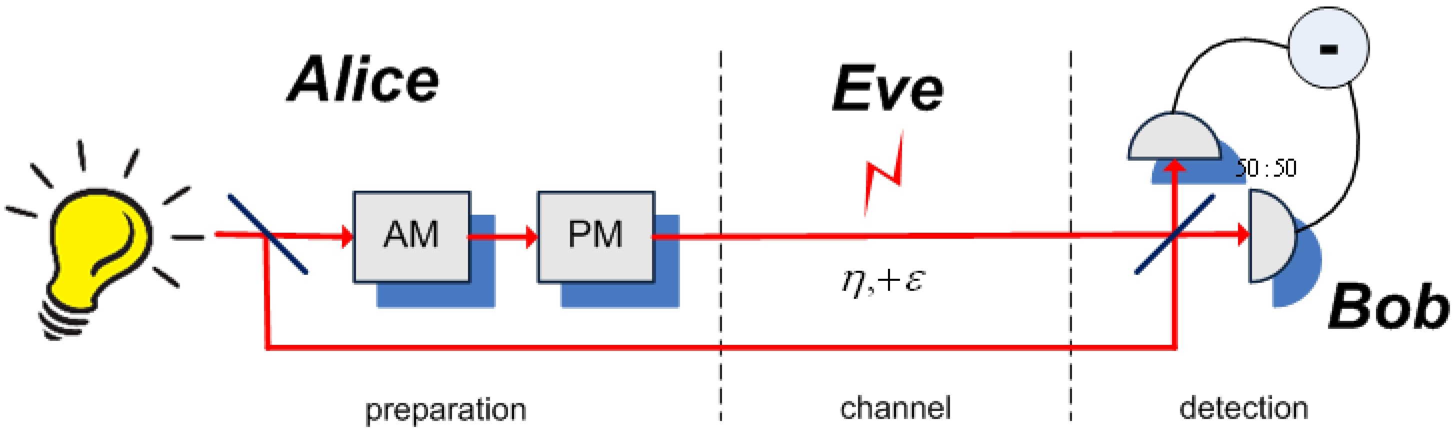
Continuous variables



Security analysis:

Estimate upper bound on Eve's information from the channel noise and loss.
Security against Gaussian collective attacks / general attacks was shown.
[M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett.
97, 190502 (2006); R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. 97,
190503 (2006)]

Continuous variables

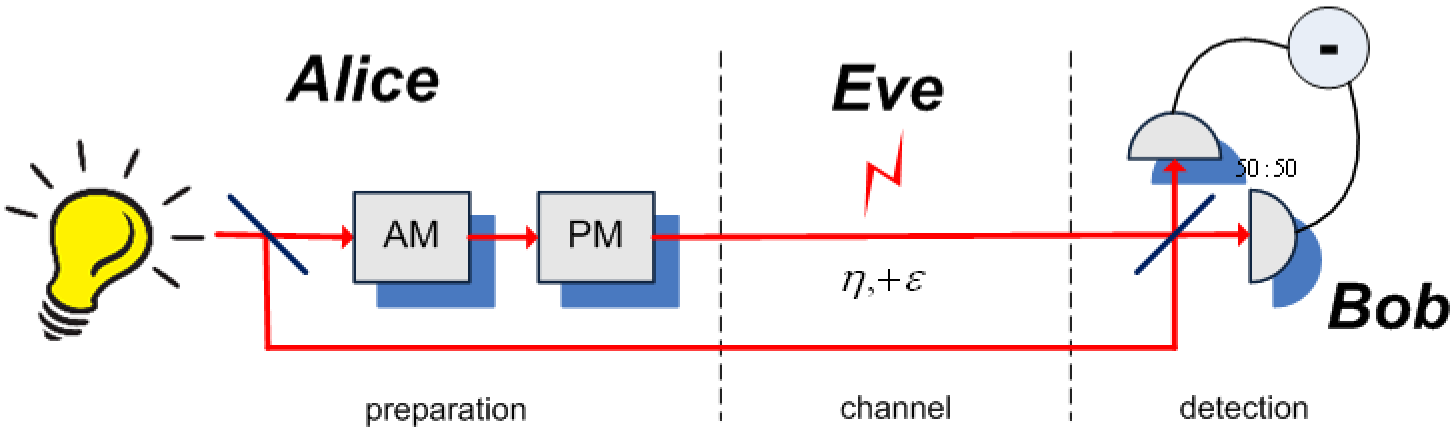


Physical systems: multiphoton states (weaker nonclassicality)
Detection method: homodyne detection
Issues:

- channel imperfections
- possible implementation loopholes

Current achievements: tested in fiber (up to 100 km) and free-space.
Prototypes in development.

Continuous variables



[Role of source noise: **Phys. Rev.** A 81, 022318 (2010),
Role of squeezing: **New J. Phys.** 13, 113007 (2011),
CV QKD over turbulent channels (exp.): **New J. Phys.** 14 (9), 093048 (2012),
Modulation-enhanced CV QKD (exp.): **Nature Communications** 3, 1083 (2012),
Optimization of channel estimation: **Phys. Rev. A** 90, 062310 (2014),
Multimode CV QKD: **Phys. Rev. A** 90, 062326 (2014),
Unidimensional protocol: **Phys. Rev. A** 92, 062337 (2015),
Role of “trusted noise” in CV QKD: **Entropy** 18, 20 (2016),
Effect of side-channels in CV QKD: **Phys. Rev. A** 93, 032309 (2016)]

Comparison between CV and DV?

For many years a comparison was either avoided or done in favor of any of the protocols.

We compare CV and DV in an perfect implementation and using the same channel parametrization.

Comparison between CV and DV?

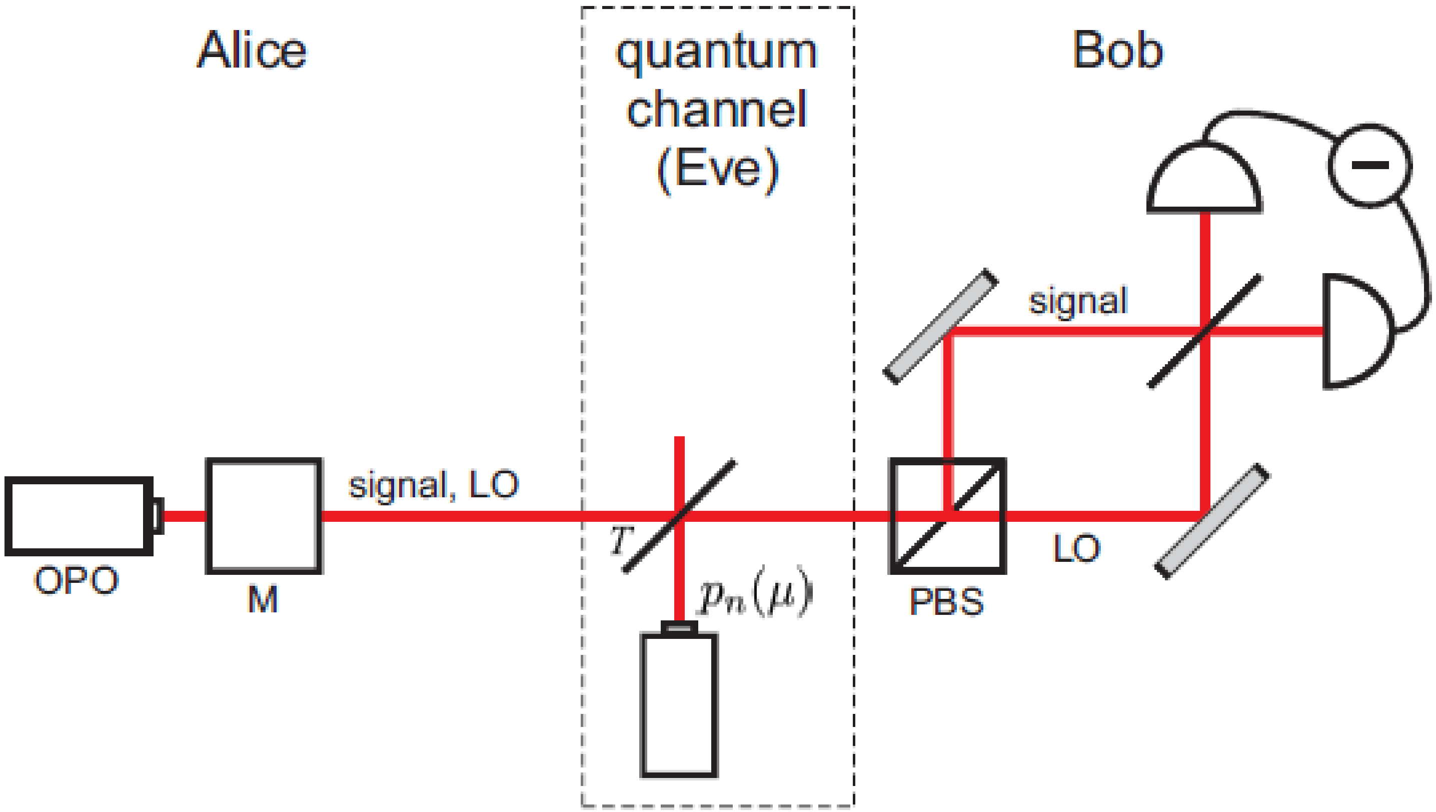
For many years a comparison was either avoided or done in favor of any of the protocols.

We compare CV and DV in an perfect implementation and using the same channel parametrization.

Perfect implementation:

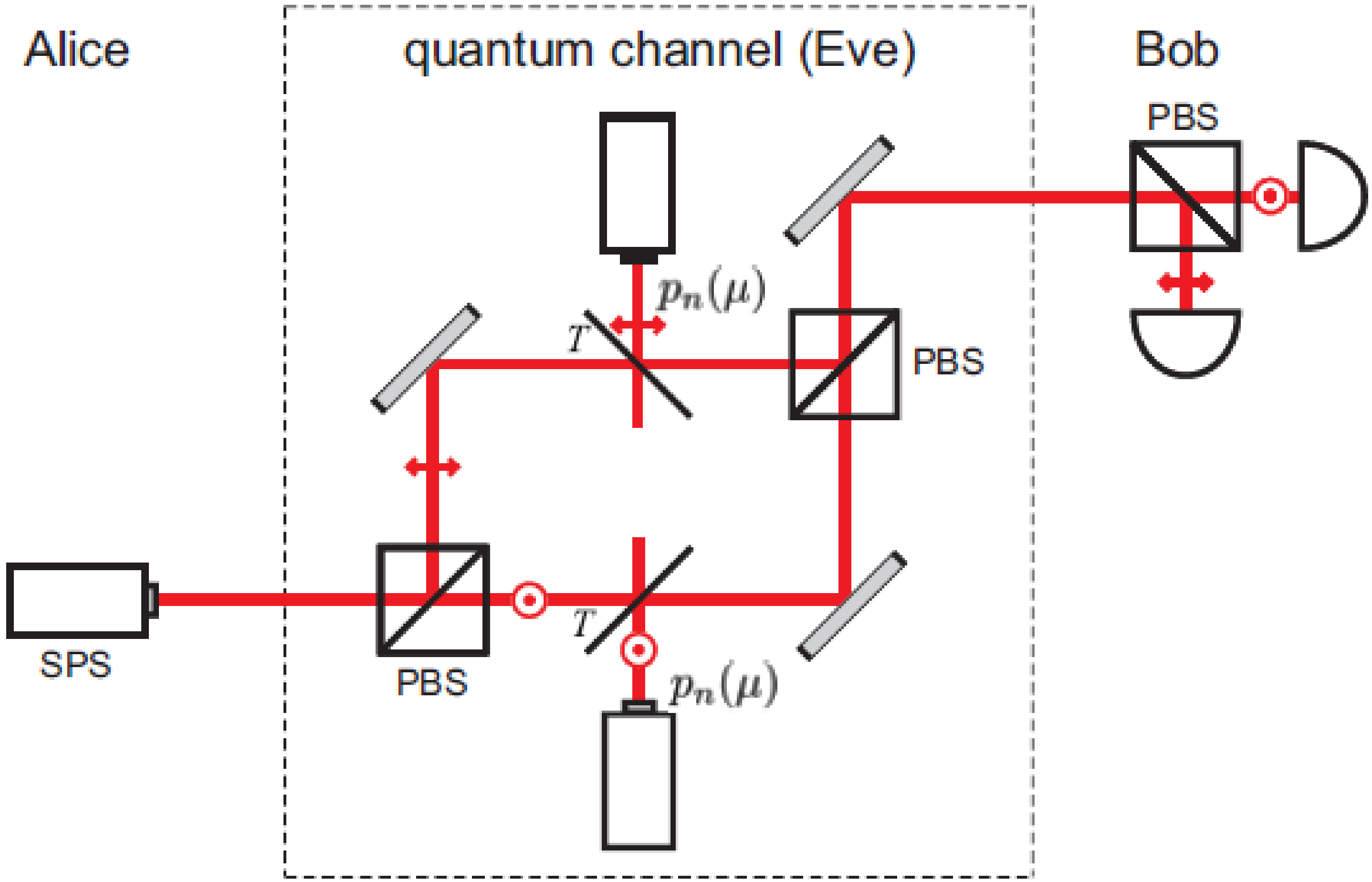
- Perfect single-photon source
- Arbitrary squeezed state generation
- Perfect detectors

CV vs DV



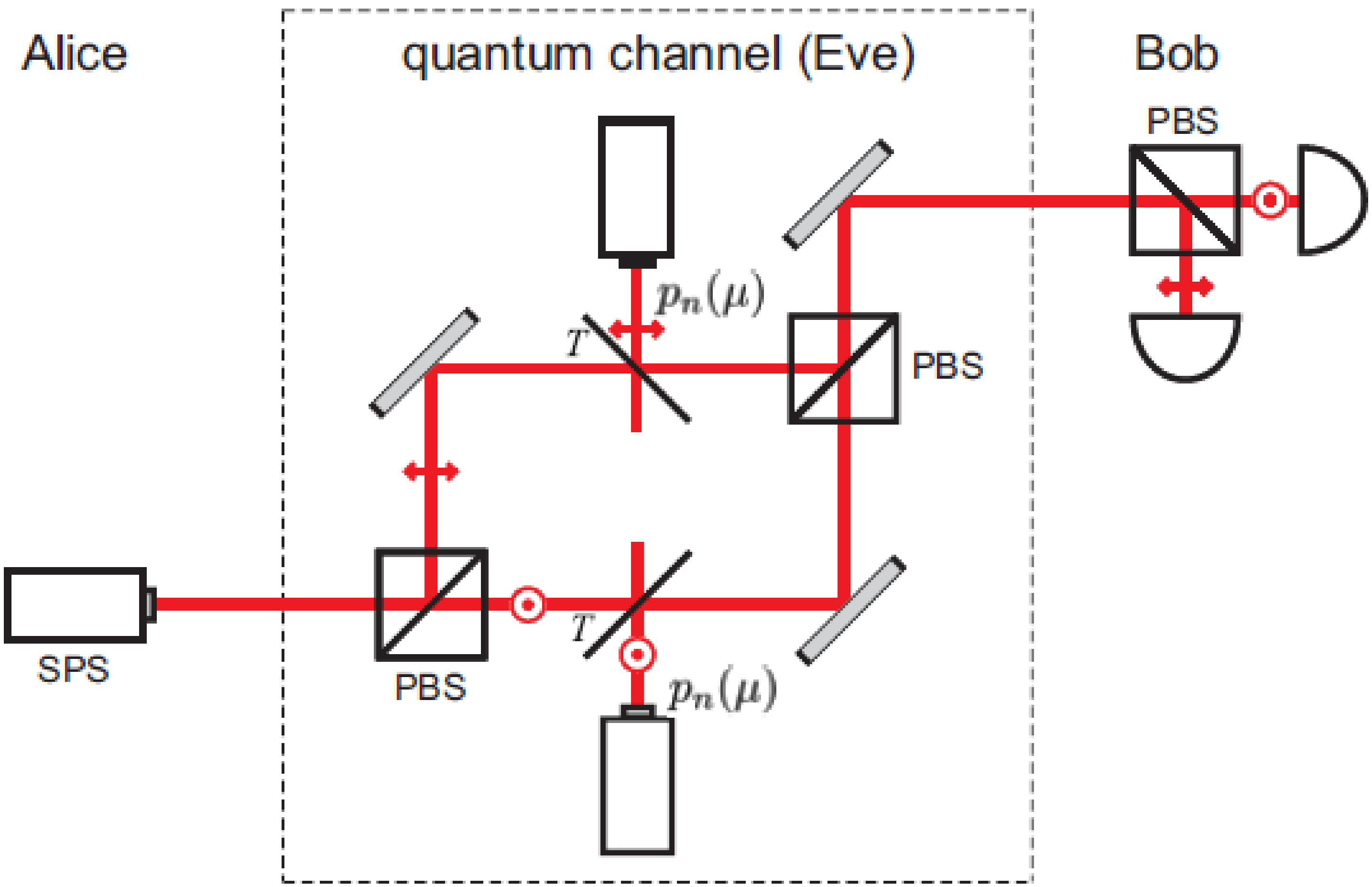
Typical noise model used in CV QKD and parametrized by a mean photon number

CV vs DV



The same noise model applied to DV QKD protocol

CV vs DV



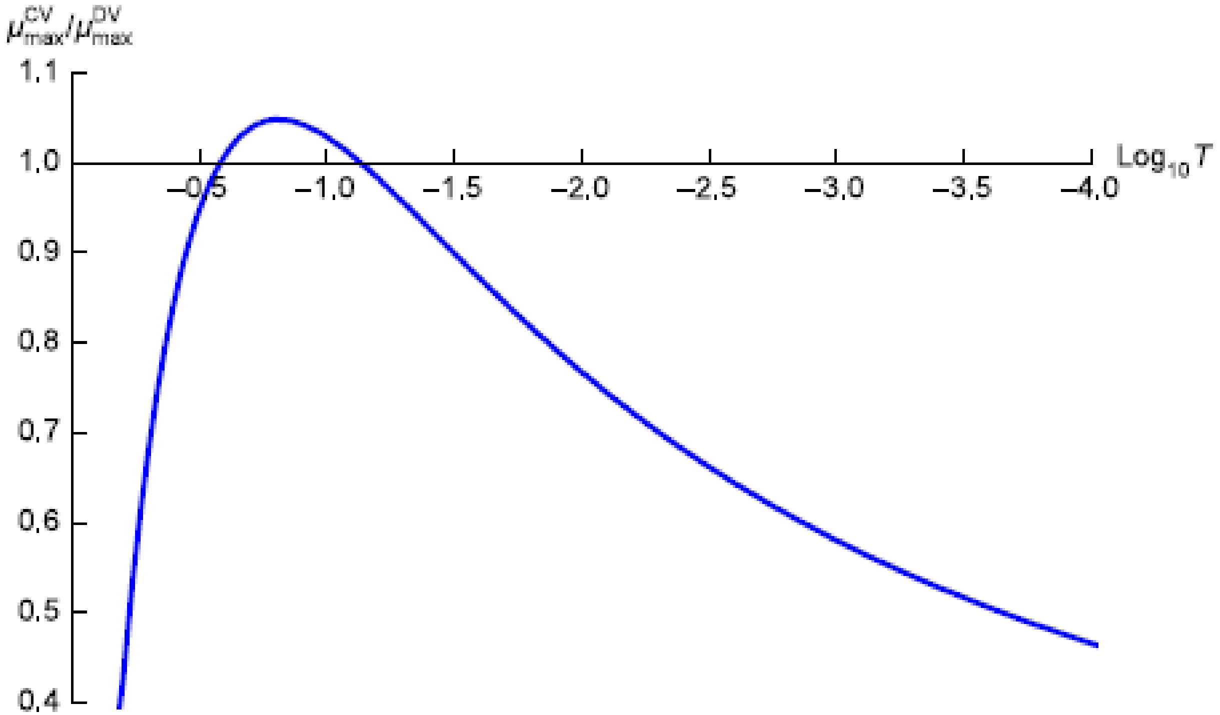
Photonic noise:

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

Quadrature noise:

$$W = 2\mu + 1$$

CV vs DV



Comparison between robustness to noise in DV and CV

CV vs DV

Analytical result for CV:

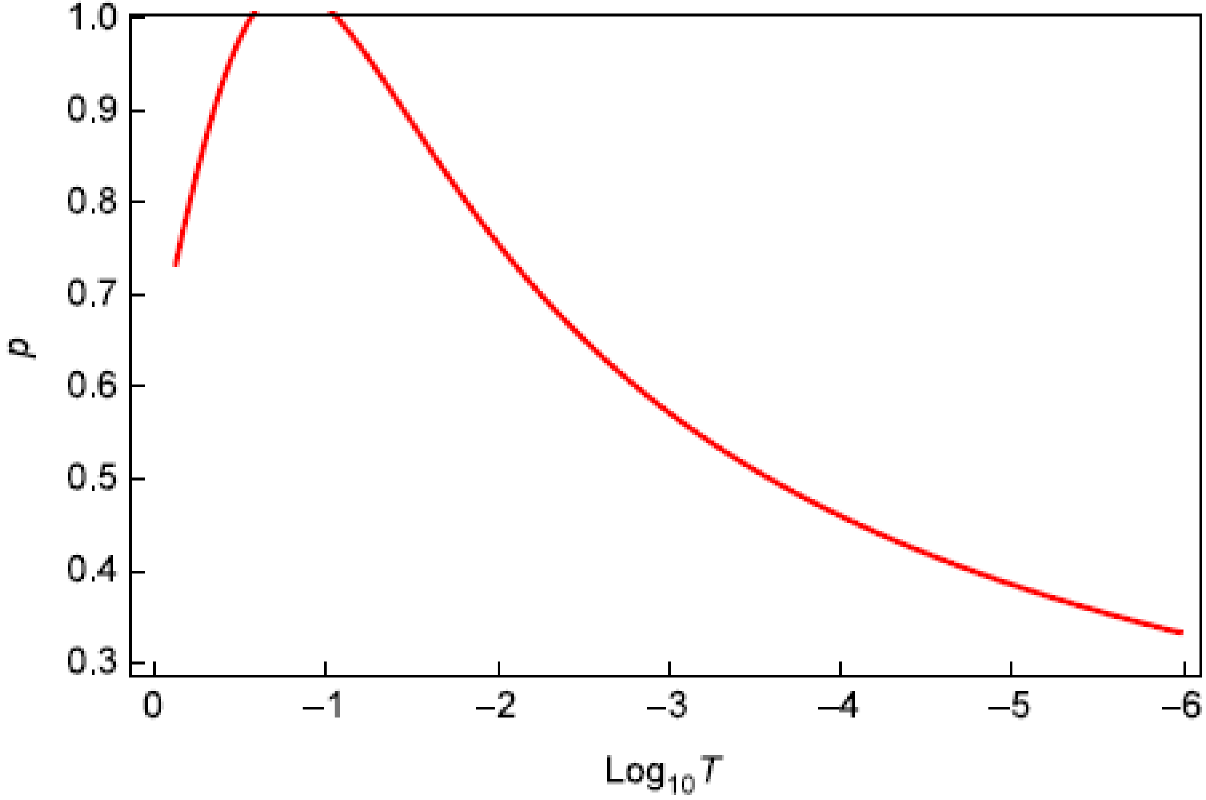
$$\mu_{max}(T) = \exp[1 + W_{-1}(-T/e)]$$

Analytical result for DV:

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

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

CV vs DV



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

Summary

• We developed the model of the channel noise allowing the same parametrization in CV and DV protocols

• Using the model we compared the robustness to channel noise of DV and CV protocols

• CV is more effective for mid-range channels, while DV is more effective for short-range or long-range channels with low or strong losses.

• The results are promising for planning QKD networks

See quant-ph **arXiv:1602.03122** for details.

Thank you for attention!

usenko@optics.upol.cz