CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION: ACHIEVEMENTS AND CHALLENGES

Vladyslav C. Usenko

Department of Optics, Palacký University,
Olomouc, Czech Republic

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

MUNI Brno, 2013

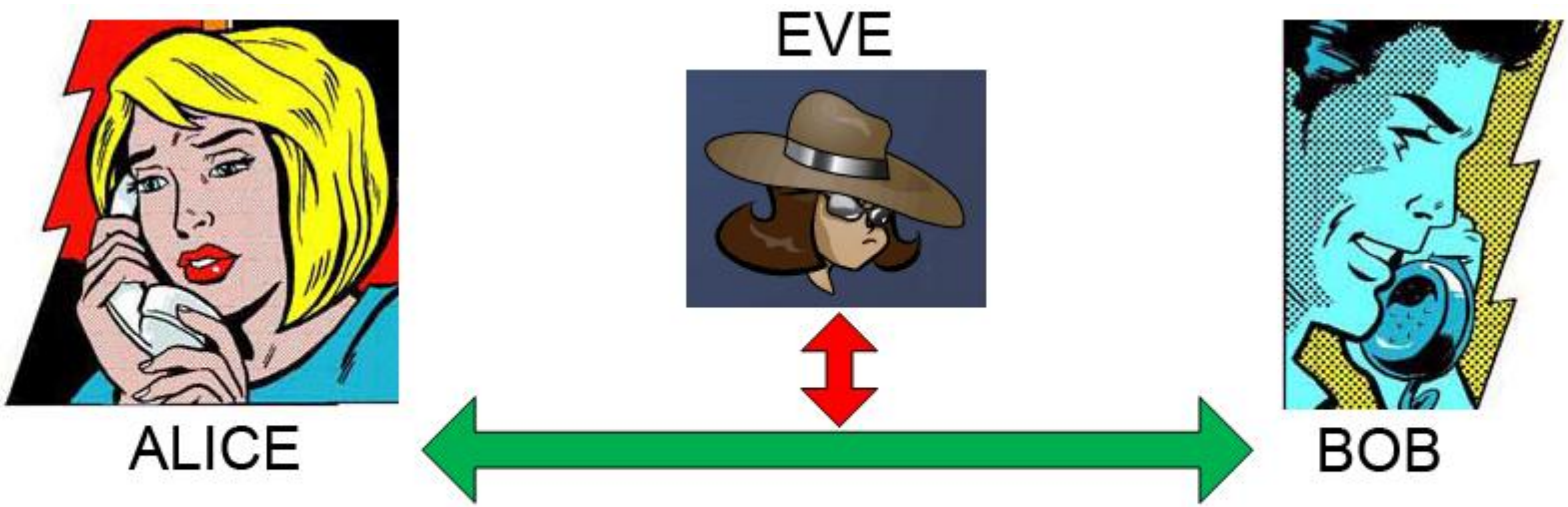
Outline

- Classical cryptography, motivation
- Discrete vs Continuous variables
- Continuous-variable quantum key distribution
- Security analysis
- Optimized protocol
- Resources and information leakage
- Challenges
- Summary

Quantum cryptography

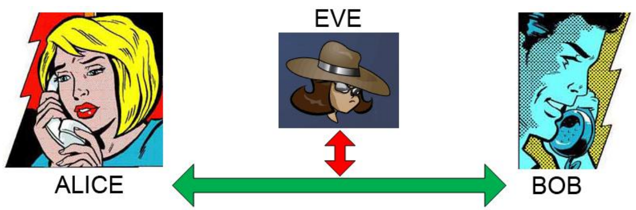
<u>Practical motivation:</u> necessity in secure communication between two trusted parties (**Alice** and **Bob**)

Quantum cryptography



Practical motivation: necessity in secure communication between two trusted parties (**Alice** and **Bob**)
Eve tries to eavesdrop

Quantum cryptography

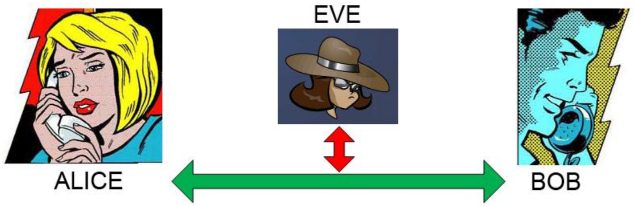


CLASSICAL CRYPTOGRAPHY

Asymmetrical schemes (RSA, DSA); symmetrical (DES, AES, RC4, MD5), mixed.

Problem: all methods are based on the mathematical complexity, thus are potentially vulnerable (due to progress in mathematical methods or quantum computation)

Quantum cryptography



CLASSICAL CRYPTOGRAPHY

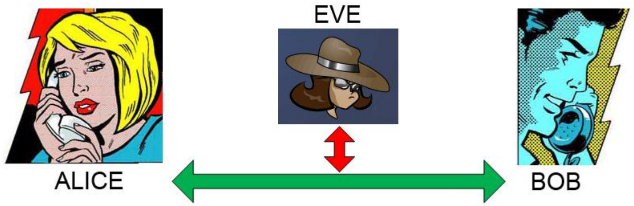
Asymmetrical schemes (RSA, DSA); symmetrical (DES, AES, RC4, MD5), mixed.

Problem: all methods are based on the mathematical complexity, thus are potentially vulnerable (due to progress in mathematical methods or quantum computation)

Alternative: **one-time pad** (*Vernam, 1919*) - the only crypto-system mathematically proven secure (*Shannon, 1949*)

Problem: both parties have to share a secure key

Quantum cryptography



CLASSICAL CRYPTOGRAPHY

Asymmetrical schemes (RSA, DSA); symmetrical (DES, AES, RC4, MD5), mixed.

Problem: all methods are based on the mathematical complexity, thus are potentially vulnerable (due to progress in mathematical methods or quantum computation)

Alternative: **one-time pad** (*Vernam, 1919*) - the only crypto-system mathematically proven secure (*Shannon, 1949*)

Problem: both parties have to share a secure key

Solution: Quantum key distribution (QKD)

Quantum key distribution

"Fundamental" motivation:

- Secrecy as a merit to test quantum properties (*H. J. Kimble, Nature 453, 1023-1030, 2008*)

- Inspiring to investigate the role of nonclassicality, coherence/decoherence, noise etc.

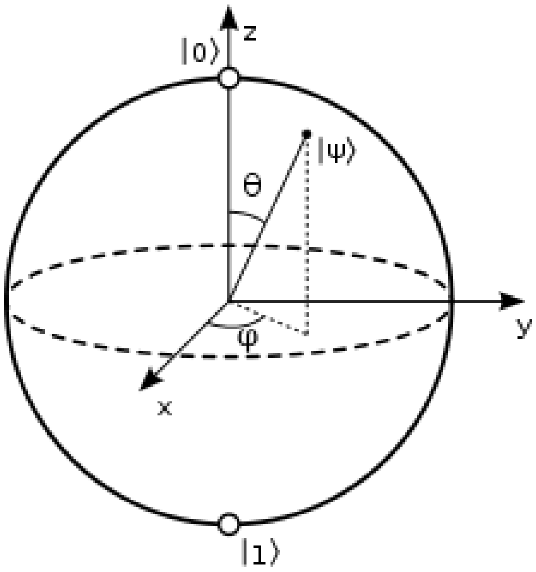
Quantum information: discrete variables

Quantum bit (qubit): two-level quantum system.

Superposition of the basis states:

$$\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

$$|\alpha|^2 + |\beta|^2 = 1$$



Bloch (Poincare) sphere

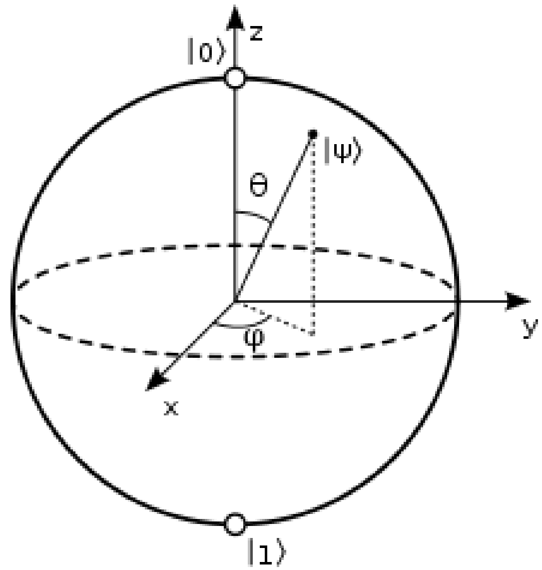
Quantum information: discrete variables

<u>Quantum bit (qubit):</u> two-level quantum system.

Superposition of the basis states:

$$\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

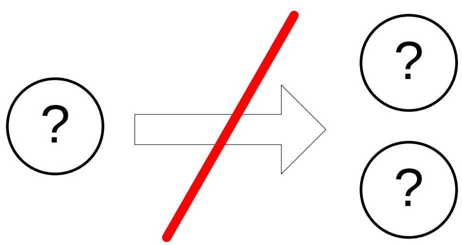
$$|\alpha|^2 + |\beta|^2 = 1$$



Bloch (Poincare) sphere

<u>No-cloning theorem.</u>

Unknown quantum state cannot be perfectly cloned!



[*W. Wootters and W. Zurek, Nature 299, 802 (1982)*]

$$U\,|s_1\rangle \otimes |b\rangle \otimes |0\rangle = |s_1\rangle \otimes |s_1\rangle \otimes |f_1\rangle$$

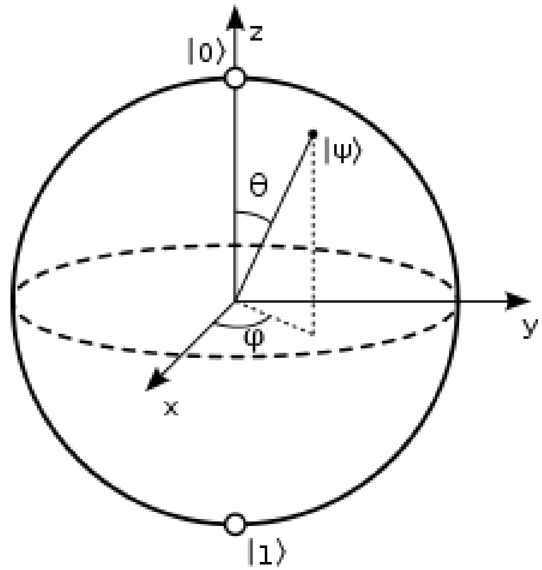
$$U\,|s_2\rangle \otimes |b\rangle \otimes |0\rangle = |s_2\rangle \otimes |s_2\rangle \otimes |f_2\rangle$$

$$U(\alpha\,|s_1\rangle + \beta\,|s_2\rangle) \otimes |b\rangle \otimes |0\rangle) = (\alpha\,|s_1\rangle + \beta\,|s_2\rangle) \otimes (\alpha\,|s_1\rangle + \beta\,|s_2\rangle) \otimes |f_a\rangle$$

$$U(\alpha\,|s_1\rangle + \beta\,|s_2\rangle) = \alpha U\,|s_1\rangle + \beta U\,|s_2\rangle \;\rightarrow\; |f_a\rangle = 0$$

Quantum information: discrete variables

Quantum bit (qubit): two-level quantum system.



Bloch (Poincare) sphere

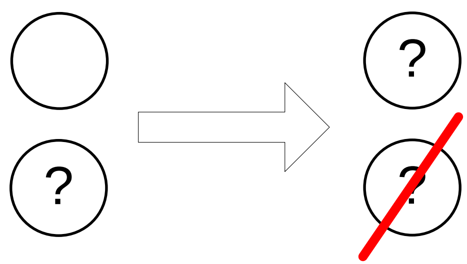
Superposition of the basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

No-cloning theorem.

However, imperfect cloning and quantum teleportation are possible.



Quantum information: discrete variables

Entangled qubits. Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

Schrödinger's cat

Quantum information: discrete variables

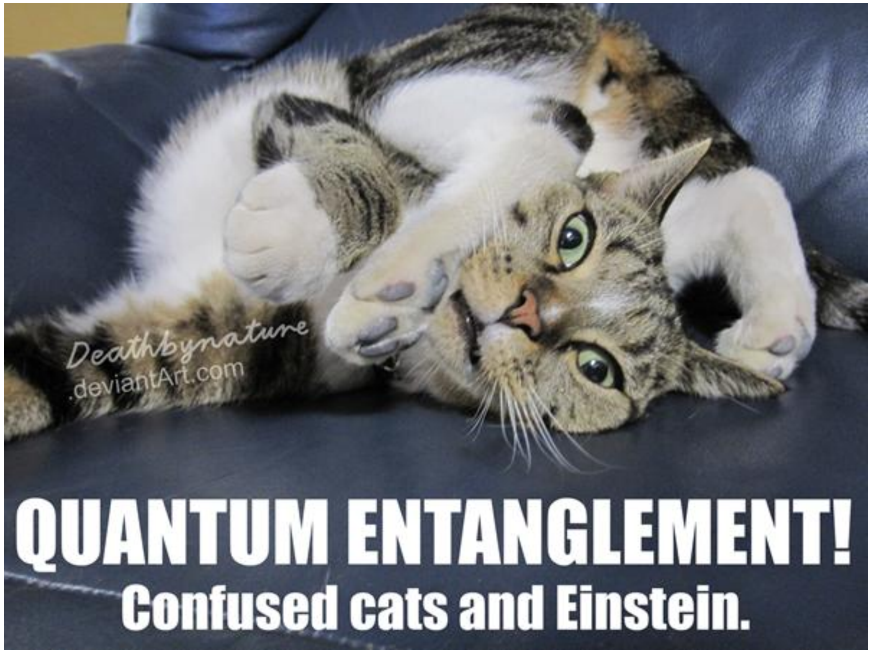
Entangled qubits. Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$



Schrödinger's cat

Bell inequalities. If local realism holds, then:

$$S(\mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}') := |E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b}')| + |E(\mathbf{a}', \mathbf{b}') + E(\mathbf{a}', \mathbf{b})| \leq 2$$

However, for a singlet state $S = 2\sqrt{2}$

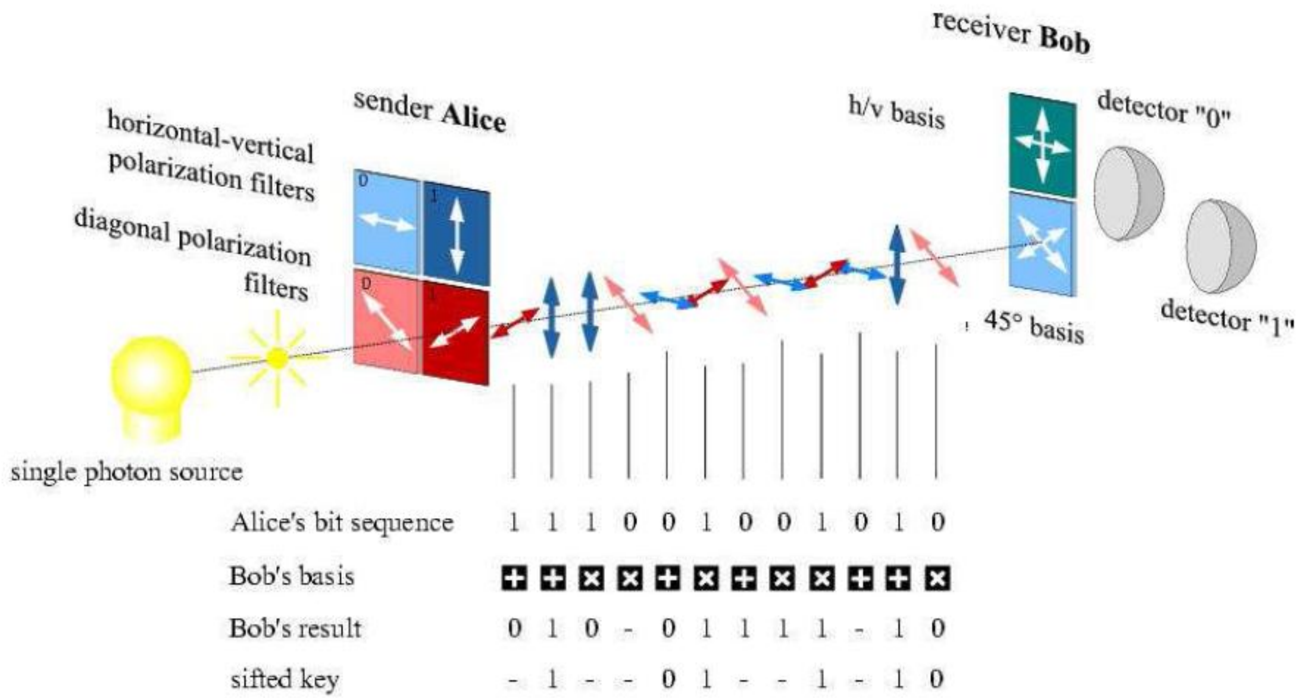
[*J. S. Bell, Speakable and Unspeakable in Quantum Mechanics (Cambridge UP, Cambridge, 1987)*]

Quantum information: applications

- Fundamental tests
- Quantum computing
- Super-dense coding
- Quantum teleportation
- Quantum key distribution

Quantum key distribution: BB84

- Alice generates a key (random bit string)
- Alice randomly chooses the basis and prepares a state
- Bob randomly chooses the basis and measures the state
- Key sifting (bases reconciliation)
- Error correction
- Privacy amplification



[C. H. Bennett and G. Brassard, in Proceedings of the International Conference on Computer Systems and Signal Processing (Bangalore, India, 1984), pp. 175–179]

Quantum key distribution: BB84

Security: No-cloning, measurement disturbance, Eve introduces errors.

Information-theoretical analysis

Classical (Shannon) mutual information: $I(X;Y) = H(X) - H(X|Y)$

$$H(X) = -\sum_{x\in X} p(x)\log p(x)$$

$$H(X|Y) = -\sum_{x,y} p(x,y)\log p(x|y) = H(X,Y) - H(Y)$$

Csiszar-Korner theorem, lower bound on the secure key rate:

$$\boxed{S(\alpha,\beta||\epsilon) \geq \max\{I(\alpha,\beta) - I(\alpha,\epsilon), I(\alpha,\beta) - I(\beta,\epsilon)\}}$$

i.e. Alice (or Bob) needs to have more information than Eve!

[Csiszar, I. and Korner, J., 1978, “Broadcast channels with confidential messages”, IEEE Transactions on Information Theory, Vol. IT-24, 339-348.]

Quantum key distribution: state-of-art

Commercial realizations: ~100 km, ~1 kbps

MagiQ

id Quantique

Quantum key distribution: state-of-art

Commercial realizations: ~100 km, ~1 kbps

Conceptual problems: simulation of fermionic statistics with bosons.

Practical problems: absence of effective single-photon sources VS high detectors “dark count” rates

Implementation issues: photons are [almost] never single, detectors are not exactly single-photon detectors. Leads to “Quantum hacking” (Makarov et al.), realistic security analysis (e.g. “squashing model” by Lutkenhaus) etc.

Quantum key distribution: state-of-art

Commercial realizations: ~100 km, ~1 kbps

Conceptual problems: simulation of fermionic statistics with bosons.

Practical problems: absence of effective single-photon sources VS high detectors "dark count" rates

Implementation issues: photons are [almost] never single, detectors are not exactly single-photon detectors. Leads to "Quantum hacking" (Makarov et al.), realistic security analysis (e.g. "squashing model" by Lutkenhaus) etc.

Perspectives: transition from single particles to multi-particle states (**continuous variables** coding).

Discrete vs Continuous Variables

Discrete variables (DV)	Continuous variables (CV)

Discrete vs Continuous Variables

Discrete variables (DV)	Continuous variables (CV)
Quantum states:	
single qubits, entangled qubit pairs	infinite-dimensional eigenvalues spectrum

Discrete vs Continuous Variables

Discrete variables (DV)	Continuous variables (CV)
Quantum states:	
single qubits, entangled qubit pairs	infinite-dimensional eigenvalues spectrum
Optical implementation:	
single photons (faint pulses), photon pairs (SPDC)	intense pulses, entangled beams (OPA, OPO)

Discrete vs Continuous Variables

Discrete variables (DV)	Continuous variables (CV)
Quantum states:	
single qubits, entangled qubit pairs	infinite-dimensional eigenvalues spectrum
Optical implementation:	
single photons (faint pulses), photon pairs (SPDC)	intense pulses, entangled beams (OPA, OPO)
Performance:	
work “sometimes” but “perfectly”	work “always” but never perfectly

Braunstein and van Loock, Rev. Mod. Phys. ***77****. 513 (2004);*
Weedbrook et al., Rev. Mod. Phys. ***84****, 621 (2012)*

Discrete vs Continuous Variables

Discrete variables (DV)	Continuous variables (CV)
Quantum states:	
single qubits, entangled qubit pairs	infinite-dimensional eigenvalues spectrum
Optical implementation:	
single photons (faint pulses), photon pairs (SPDC)	intense pulses, entangled beams (OPA, OPO)
Performance:	
work “sometimes” but “perfectly”	work “always” but never perfectly

Our task: analysis and optimization of CV QIP in realistic conditions

Continuous-variable states

Canonical infinite-dimensional quantum system, defined on a Hilbert space:

$$\mathscr{H} = \bigotimes_{i=1}^{N} \mathscr{H}_i$$

Bosonic commutation relations:

$$[a_k, a_{k'}] = [a_k^\dagger, a_{k'}^\dagger] = 0, \quad [a_k, a_{k'}^\dagger] = \delta_{kk'}$$

Continuous-variable states

Canonical infinite-dimensional quantum system, defined on a Hilbert space:

$$\mathscr{H} = \bigotimes_{i=1}^{N} \mathscr{H}_i$$

Bosonic commutation relations:

$$[a_k, a_{k'}] = [a_k^\dagger, a_{k'}^\dagger] = 0, \quad [a_k, a_{k'}^\dagger] = \delta_{kk'}$$

Field Hamiltonian: $H = \sum_k \hbar\omega_k (a_k^\dagger a_k + \frac{1}{2})$

<u>Fock states</u>: $|n_k\rangle$ eigenstates of photon-number operator

$$a_k^\dagger a_k |n_k\rangle = n_k |n_k\rangle$$

Continuous-variable states

Canonical infinite-dimensional quantum system, defined on a Hilbert space:

$$\mathscr{H} = \bigotimes_{i=1}^{N} \mathscr{H}_i$$

Bosonic commutation relations:

$$[a_k, a_{k'}] = [a_k^\dagger, a_{k'}^\dagger] = 0, \quad [a_k, a_{k'}^\dagger] = \delta_{kk'}$$

Field Hamiltonian: $H = \sum_k \hbar\omega_k (a_k^\dagger a_k + \frac{1}{2})$

Fock states: $|n_k\rangle$ eigenstates of photon-number operator

$$a_k^\dagger a_k |n_k\rangle = n_k |n_k\rangle$$

Coherent states - eigenstates of annihilation operator: $a|\alpha\rangle = \alpha|\alpha\rangle$

In the Fock states basis: $$|\alpha\rangle = e^{-|\alpha|^2/2} \sum \frac{\alpha^n}{(n!)^{1/2}} |n\rangle$$

Continuous-variable states

Field quadratures: analogue of the position and momentum operators of a particle:

$$x = a^{+} + a, \quad p = i(a^{+} - a)$$

$$\hat{r} = (\hat{r}_1, ..., \hat{r}_{2N})^T = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, ..., \hat{x}_N, \hat{x}_N)^T$$

Commutation relations: $[x, p] = 2i$

Continuous-variable states

Field quadratures: analogue of the position and momentum operators of a particle: $\boxed{x = a^+ + a, \quad p = i(a^+ - a)}$

$$\hat{r} = (\hat{r}_1, ..., \hat{r}_{2N})^T = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, ..., \hat{x}_N, \hat{x}_N)^T$$

Commutation relations: $[x, p] = 2i$

Uncertainty: $\Delta A = \langle A^2 \rangle - \langle A \rangle^2$

Heisenberg relation: $\Delta x \Delta p \geq 1$

For coherent states: $\Delta x = \Delta p = 1$

Continuous-variable states

Phase-space representation.

Characteristic function: $\chi_\rho(\xi) = \mathrm{Tr}[\rho D_\xi]$. , $D_\xi = D(\xi^\star) = e^{-i\xi^T \hat{r}}$

State density matrix $\rho = \frac{1}{(2\pi)^N} \int d^{2N}\xi \chi_\rho(-\xi) D_\xi$

Wigner function: Fourier transform of the characteristic function. $W(\xi) = \frac{1}{(2\pi)^N} \int d^{2N}\zeta e^{i\xi^T \Omega \zeta} \chi_\rho(\zeta)$

Continuous-variable states

Gaussian states:

characteristic function / Wigner function is Gaussian

Continuous-variable states

Gaussian states:

characteristic function / Wigner function is Gaussian

Covariance matrix:
Explicitly describes Gaussian states

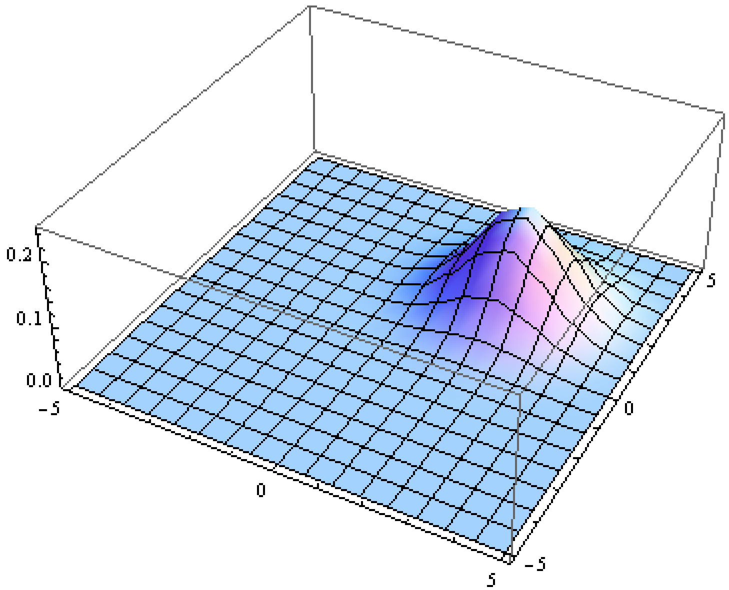
$$\boxed{\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle}$$

Generalized Heisenberg uncertainty principle: $\gamma + i\Omega \geq 0$

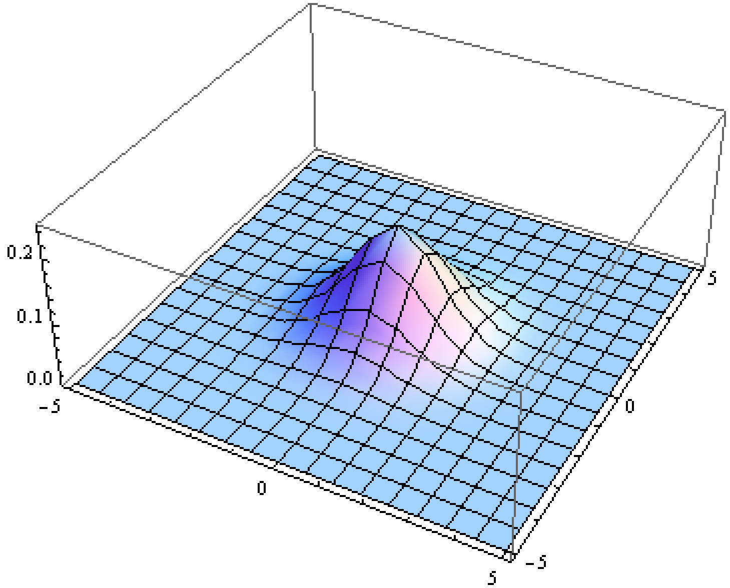
$$\Omega = \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$ - symplectic form

Bosonic commutation relations: $[\hat{r}_k, \hat{r}_l] = i\Omega_{kl}$

Continuous-variable states



Coherent state



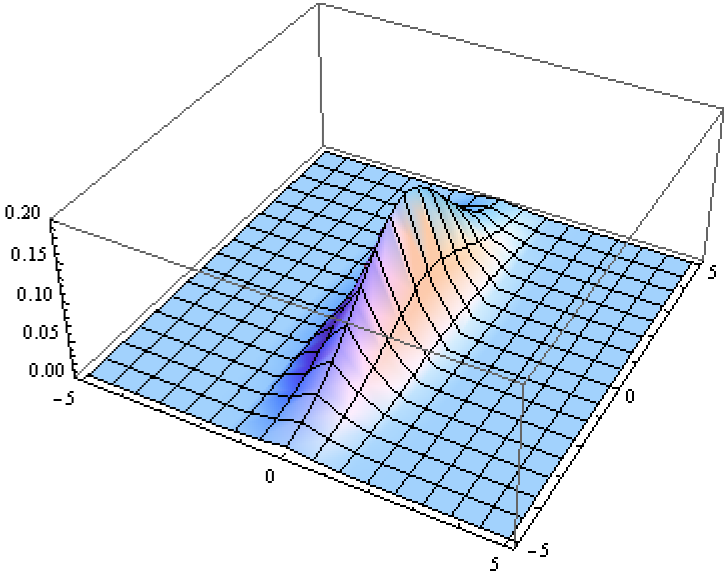
Vacuum state

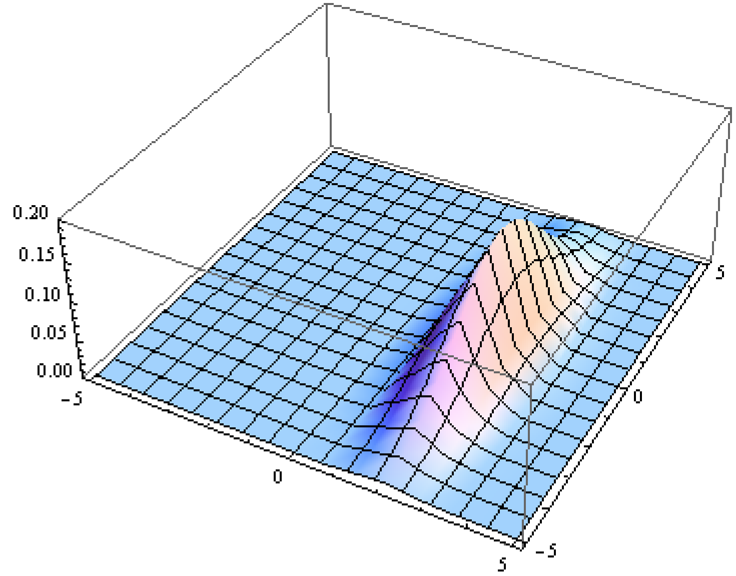
Continuous-variable states

Squeezed states: quadrature uncertainty is less than shot-noise limit

$$\Delta x < 1$$

$$\Delta x \Delta p = 1 \Rightarrow \Delta p > 1$$





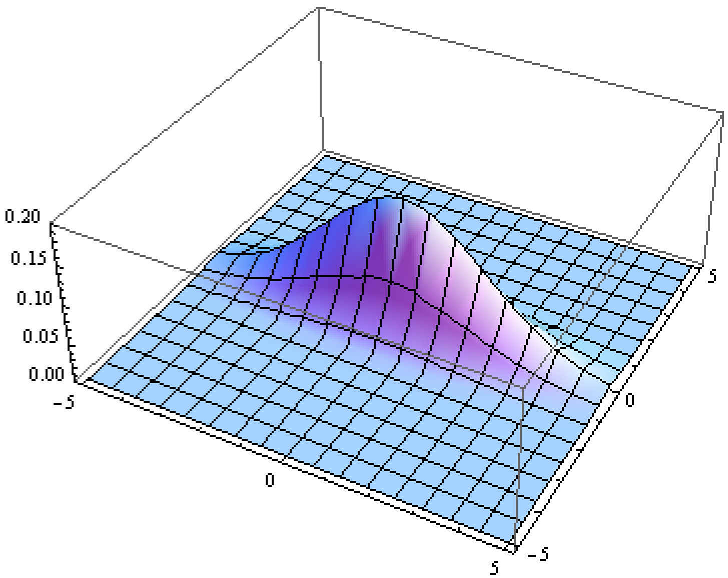
X-squeezed states: vacuum (left) and coherent (right)

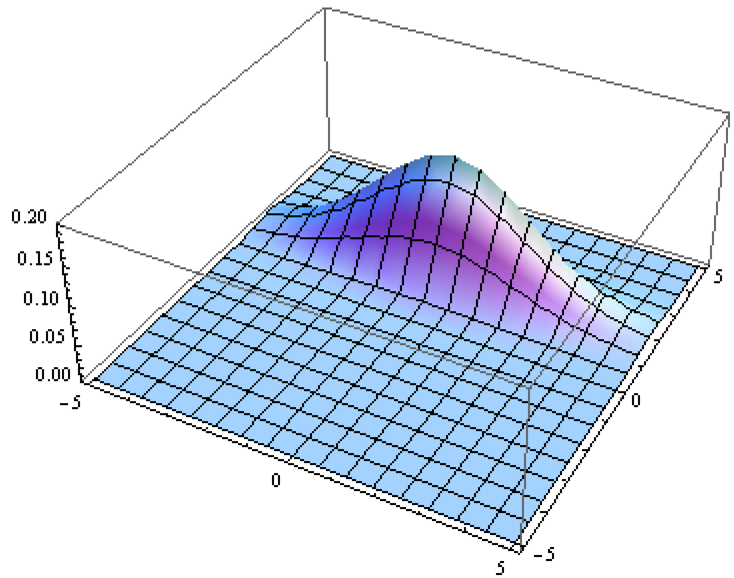
Continuous-variable states

Squeezed states: quadrature uncertainty is less than shot-noise limit

$$\Delta x < 1$$

$$\Delta x \Delta p = 1 \Rightarrow \Delta p > 1$$





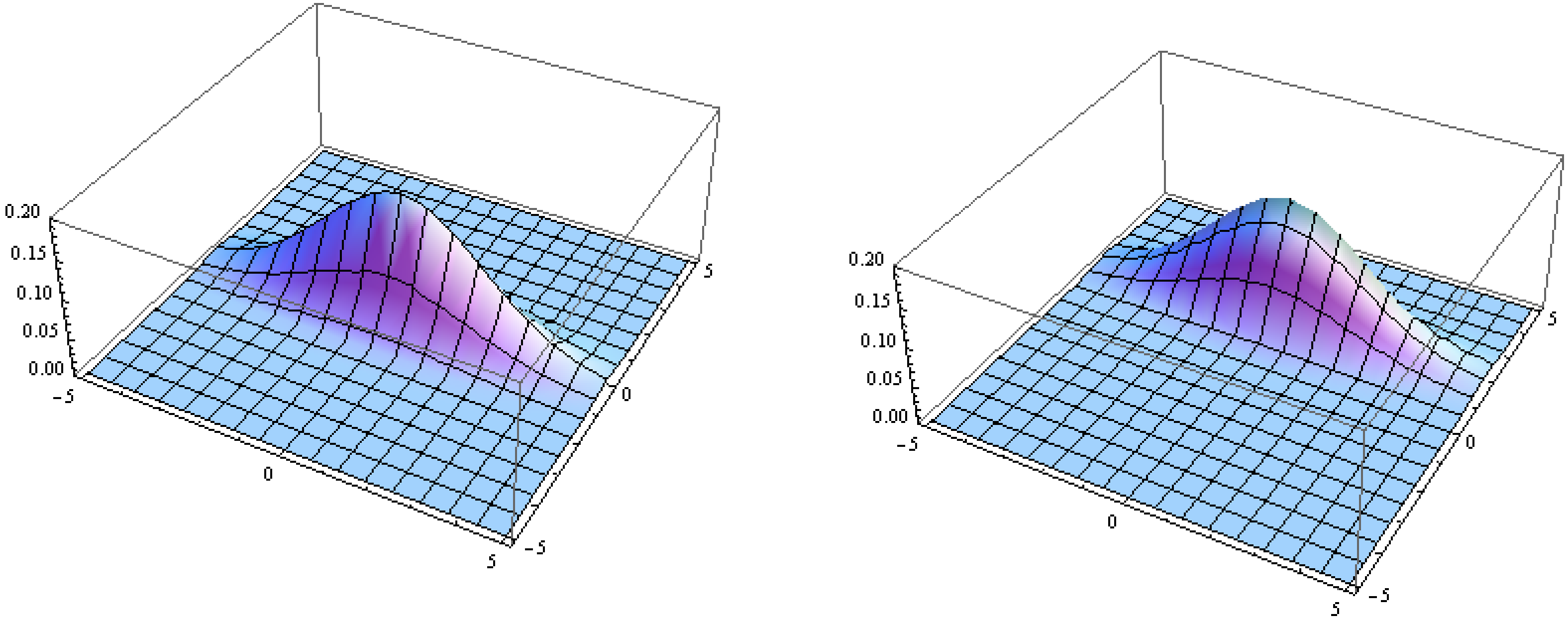
P-squeezed states: vacuum (left) and coherent (right)

Continuous-variable states

Squeezed states: quadrature uncertainty is less than shot-noise limit

$$\Delta x < 1$$

$$\Delta x \Delta p = 1 \Rightarrow \Delta p > 1$$



Achievements: **-10 dB** (i.e. 10% SNU)
[Eberle et al., Optics Express 21, 11546-11553 (2013)]

Gaussian CV Quantum Information

Entanglement measure: logarithmic negativity $E_{LN}(\gamma) = max[0, -ln(\tilde{\lambda}_-)]$

Quantifies to which extent PT covariance matrix fails to be positive;
Is the upper bound on the distillable Gaussian entanglement.

$\tilde{\lambda}_-$ - smallest symplectic eigenvalue of the PT covariance matrix
(smallest of eigenvalues of $|i\Omega\tilde{\gamma}|$

[G. Vidal, R. F. Werner, PRA 65, 032314 (2002), also Adesso, Paris]

Other measures: entanglement of formation, distillable entanglement (require optimization), entropy of reduced states (for pure states)

Purity (Gaussian mixedness): $p(\gamma_{AB}) = 1/\sqrt{Det\gamma_{AB}}$

Gaussian CV Quantum Information

Protocols:

• Quantum teleportation [Braunstein, Kimble 1998; Ralph, Lam 1998; Vaidman 1994; Furusawa et al., 1998)

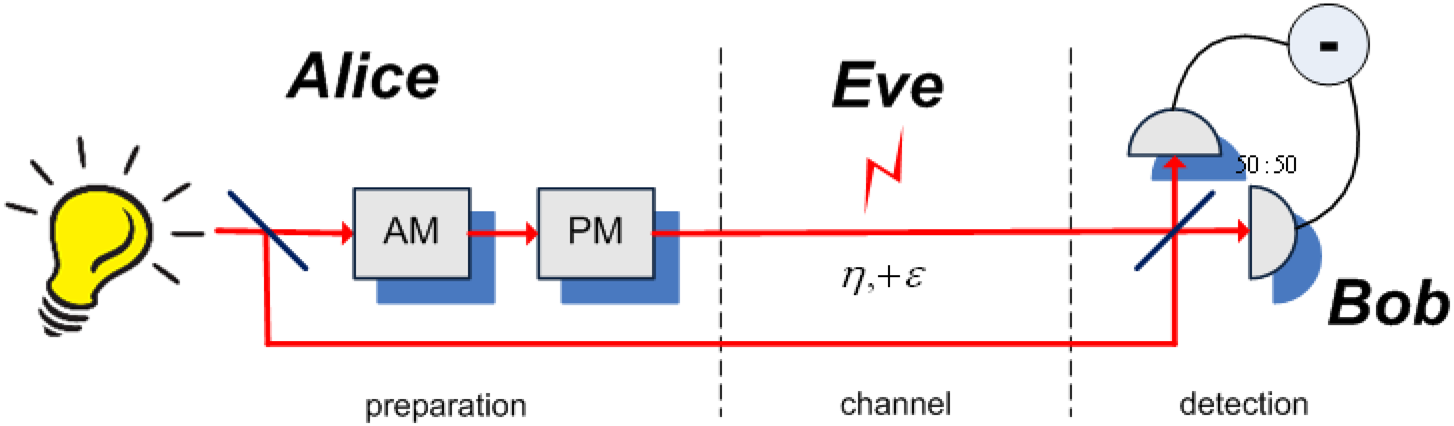
• Cloning [Cerf et al. 2000]

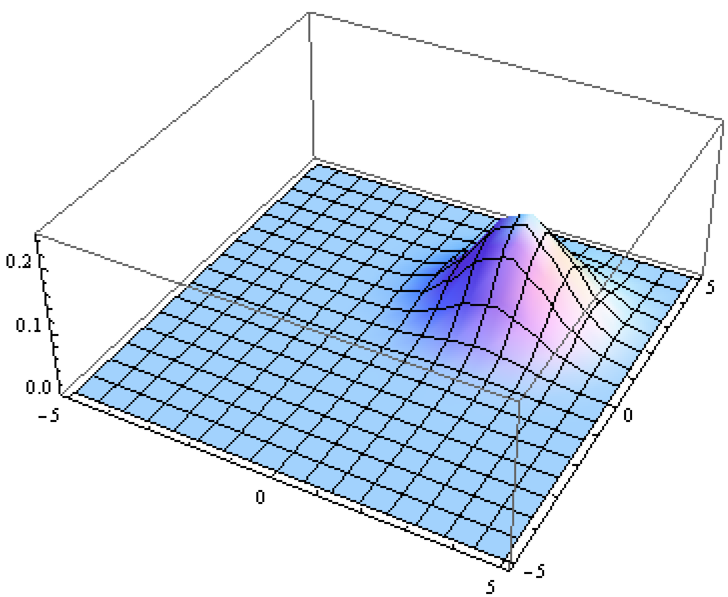
• Quantum computation [Zhang, Braunstein 2006, work in progress for Gaussian cluster states]

• Bell inequality violation [Polkinghorne, Ralph 1999]

• Quantum key distribution

CV Quantum Key Distribution

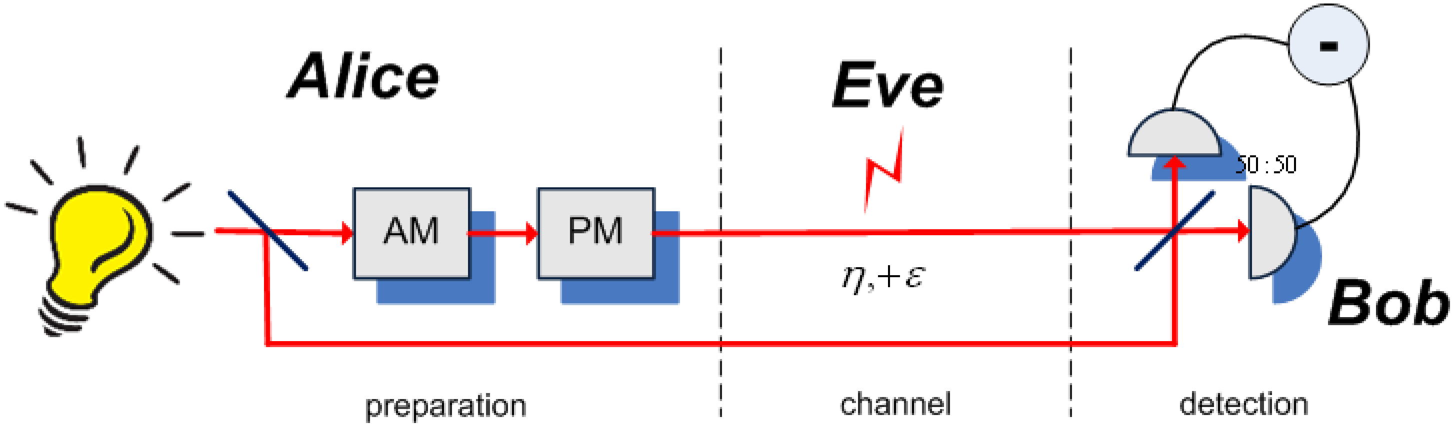


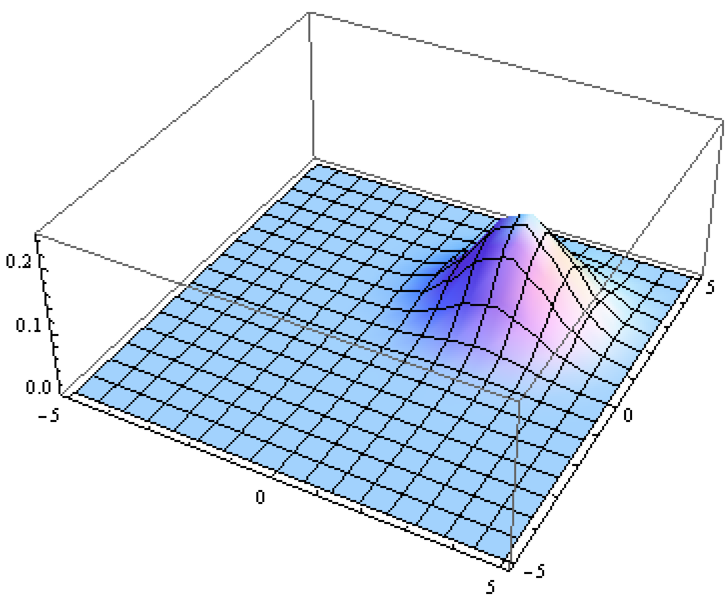


Coherent states-based protocol:
Laser source, modulation

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

CV Quantum Key Distribution

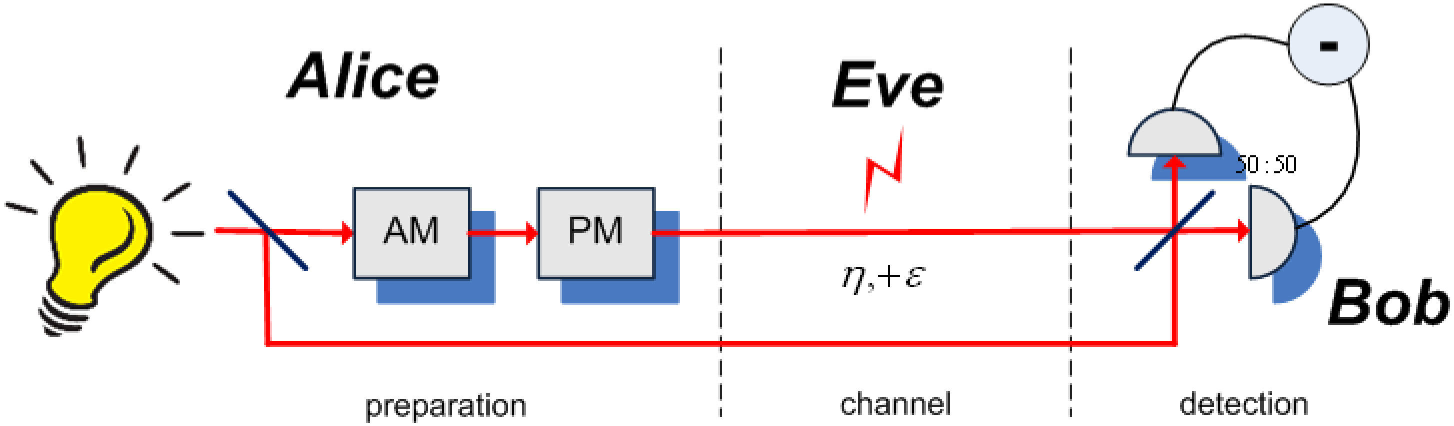


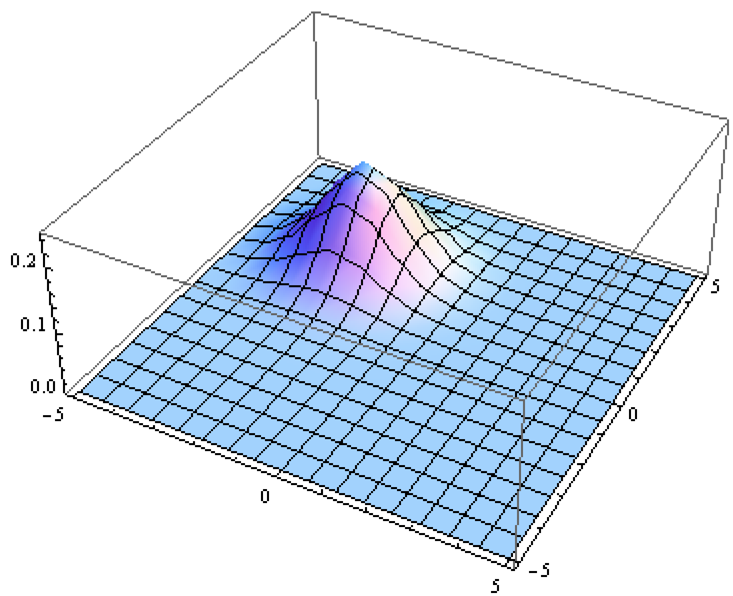


Coherent states-based protocol:

- 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

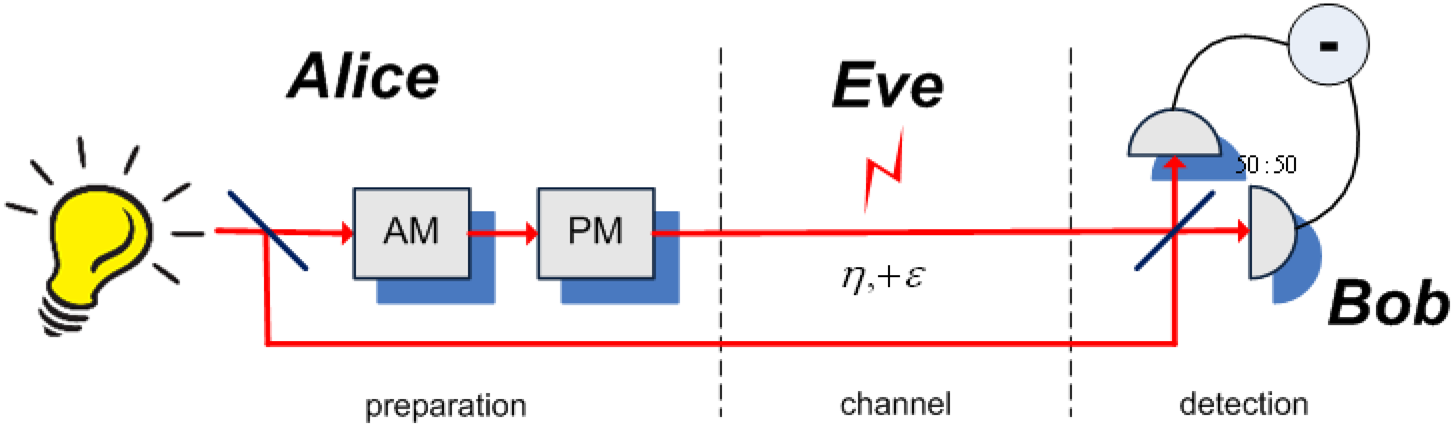


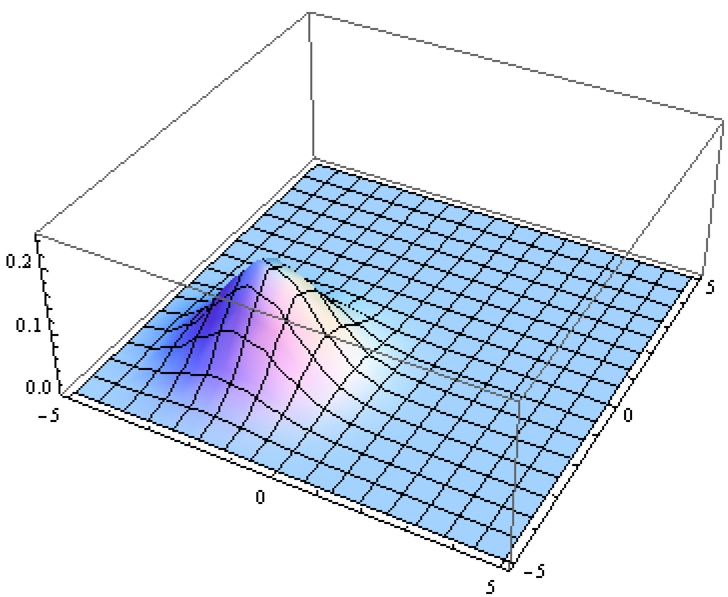


Coherent states-based protocol:

- 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

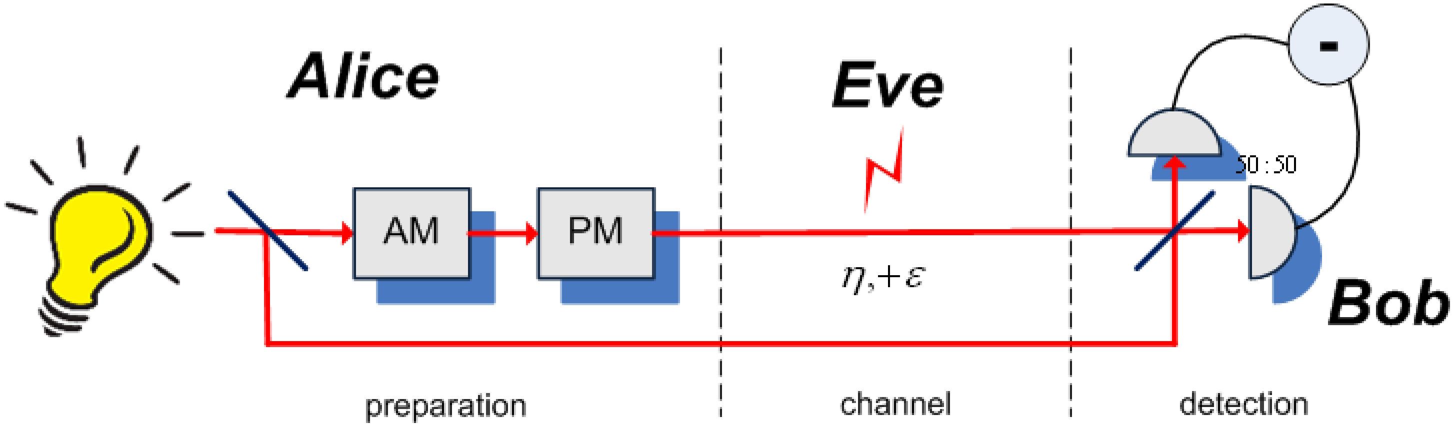


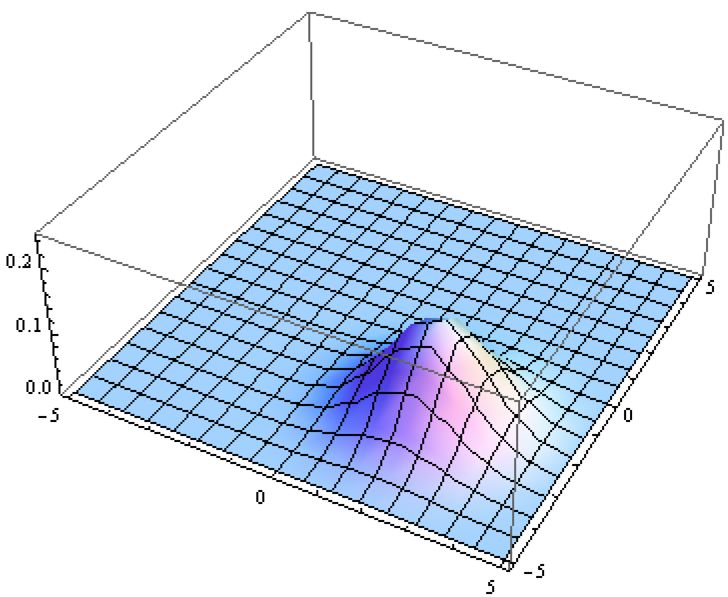


Coherent states-based protocol:

- 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

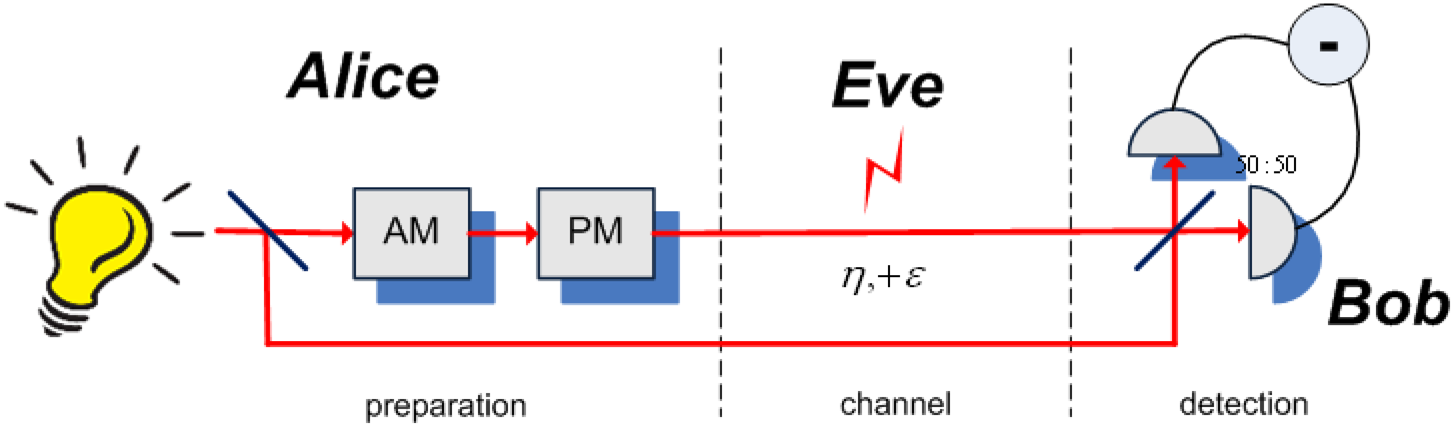


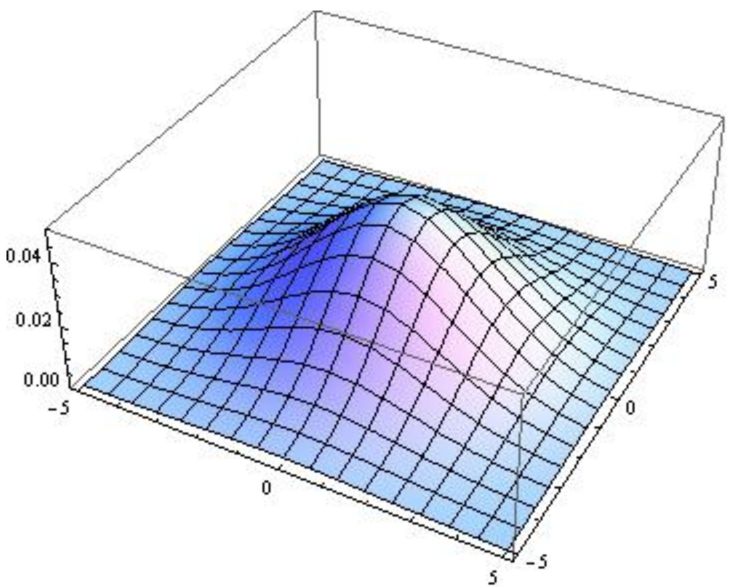


Coherent states-based protocol:

- 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



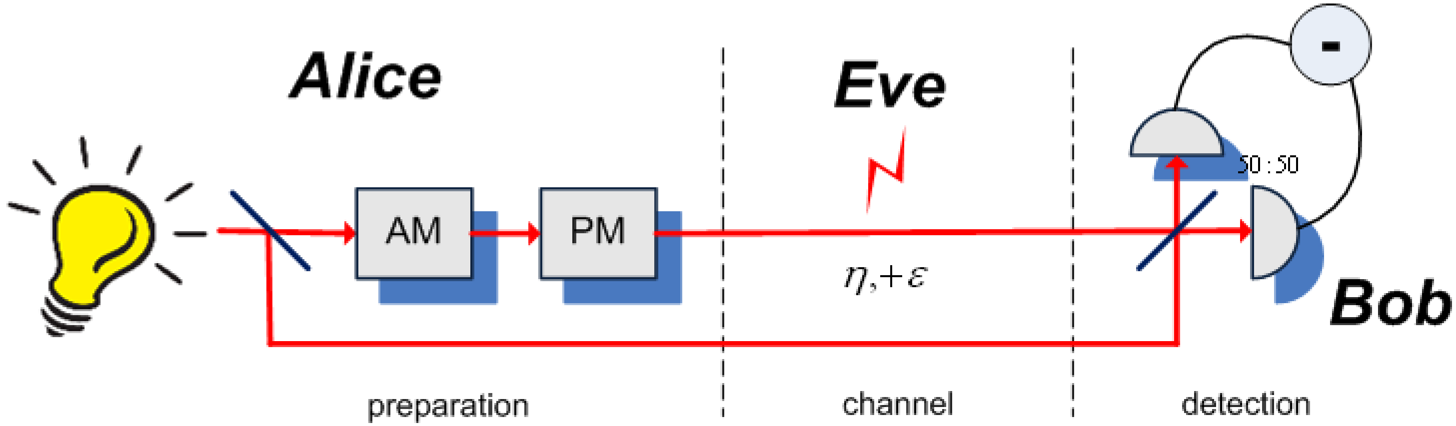


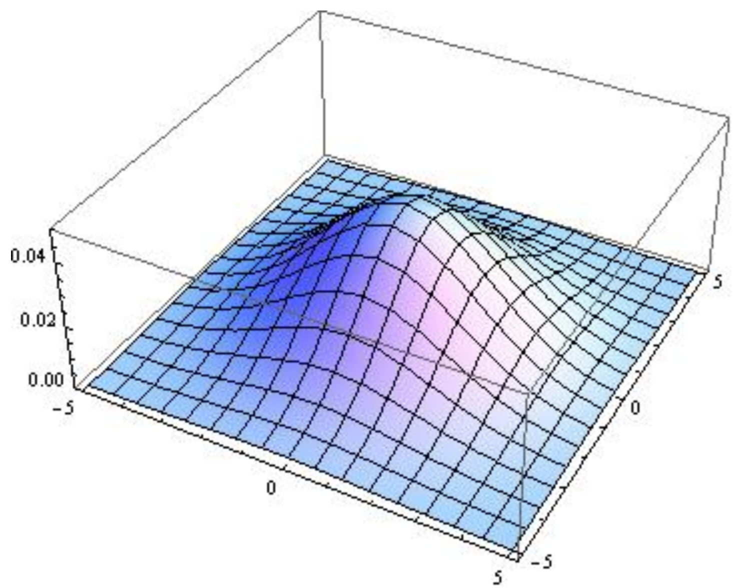
Mixture

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





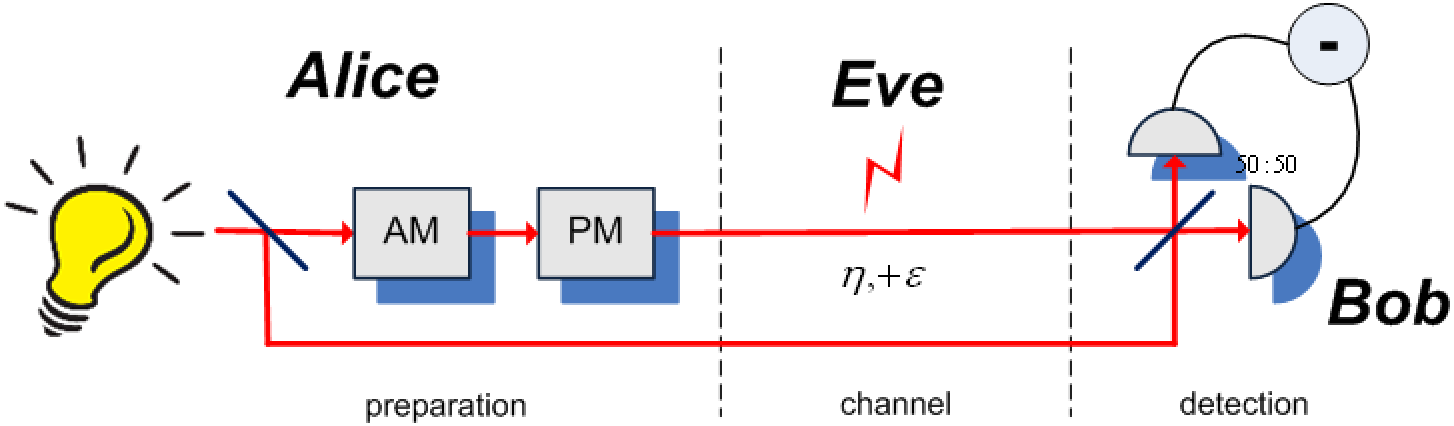
Mixture

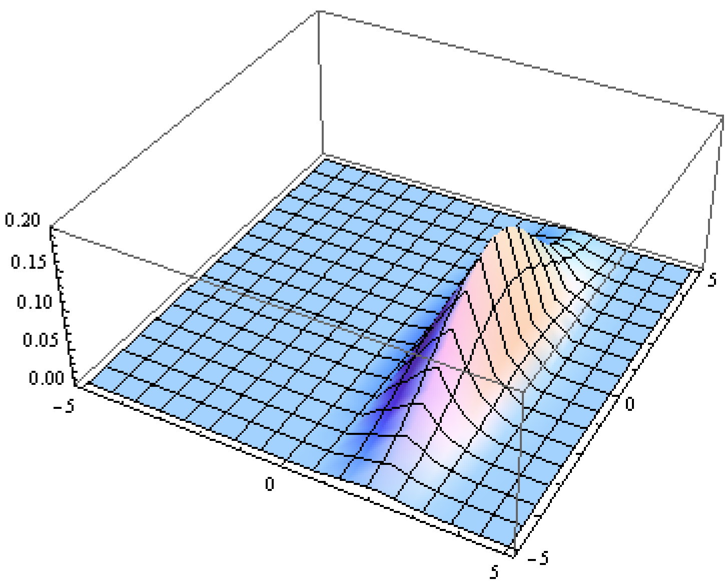
Coherent states-based protocol:

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

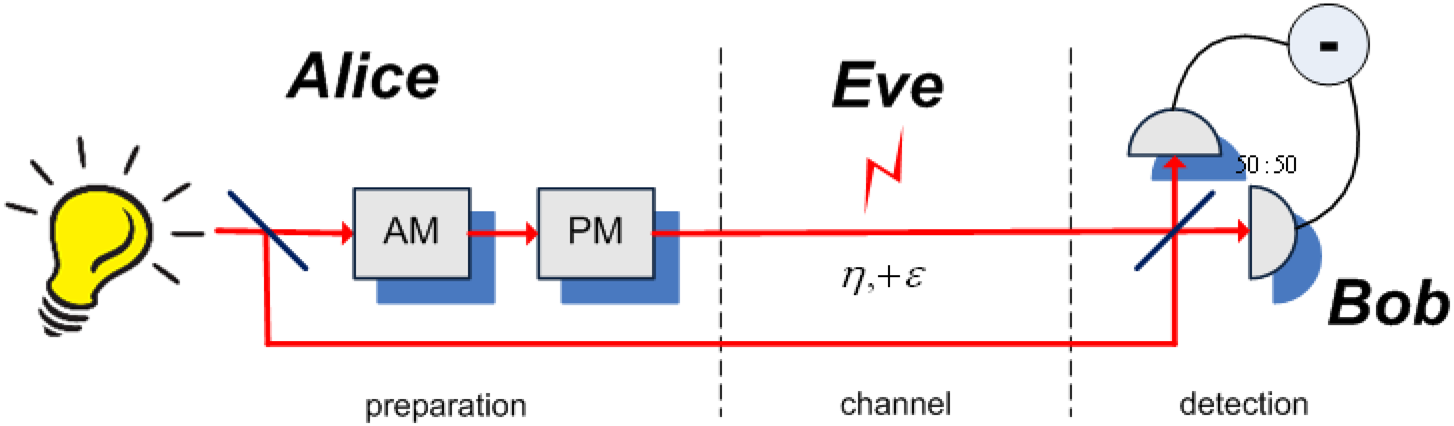


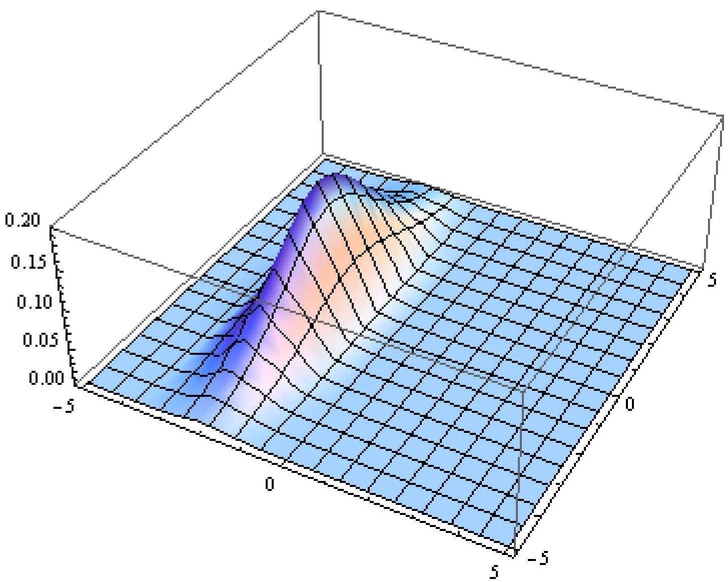


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

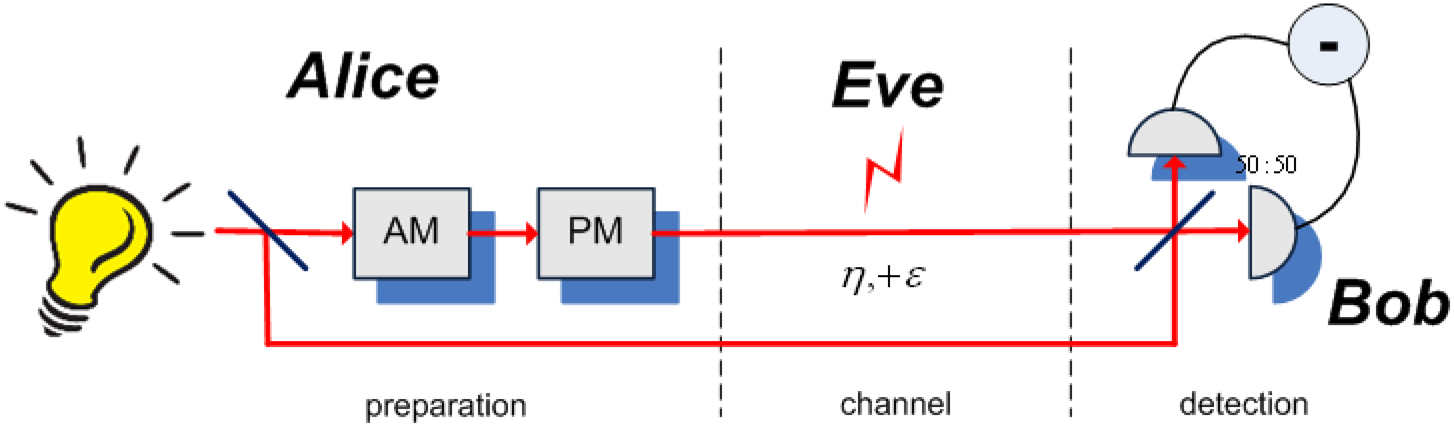


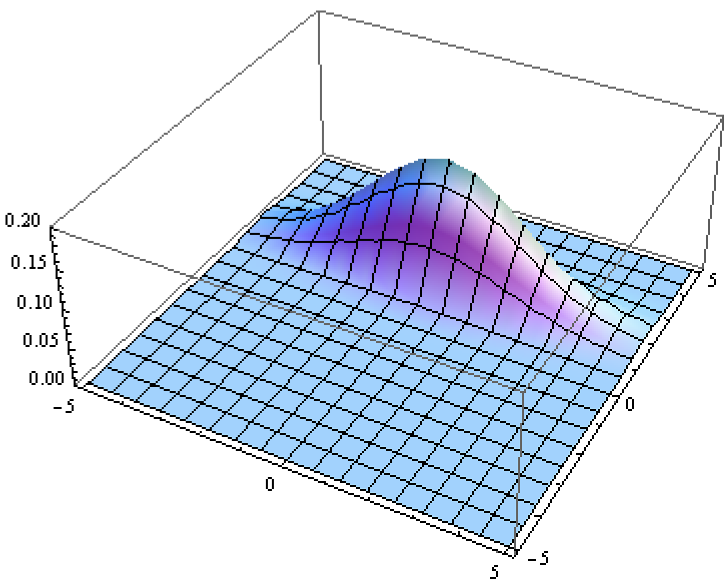


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

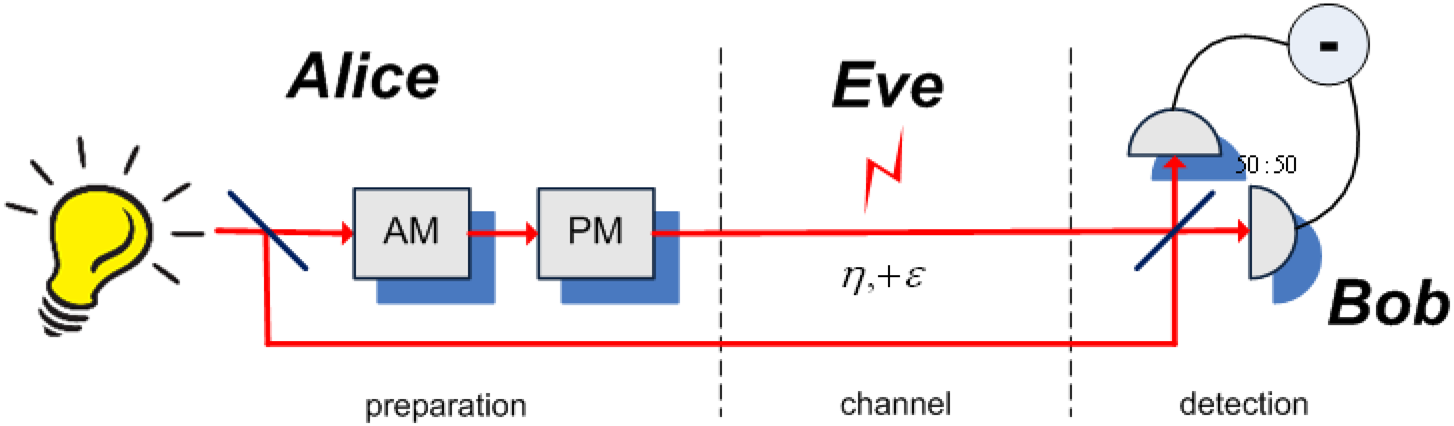


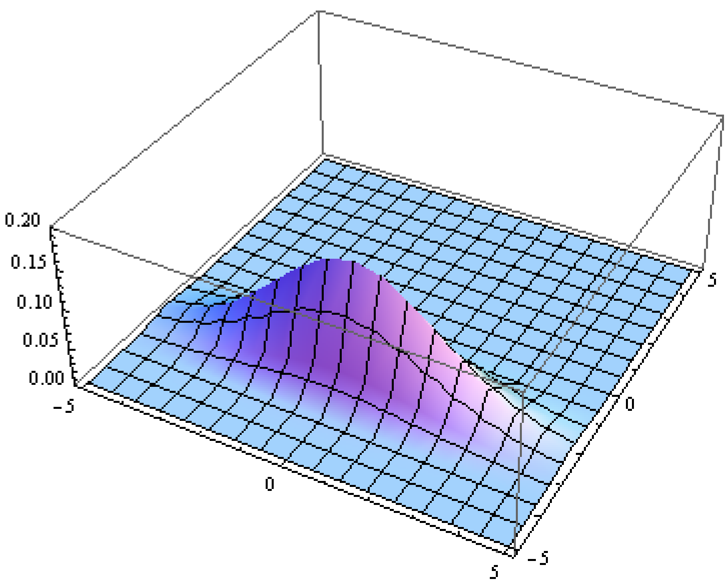


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

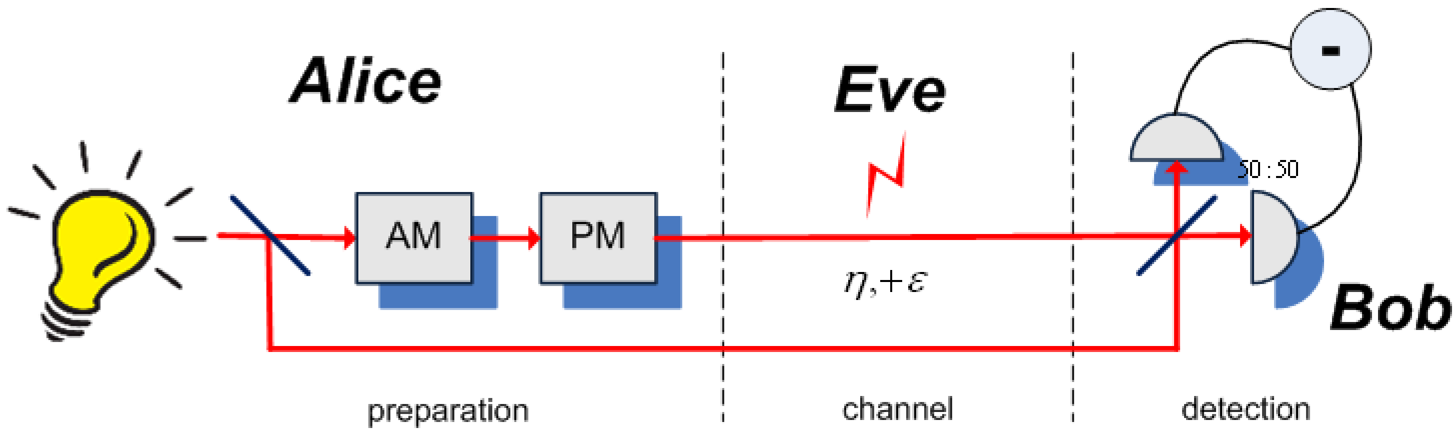


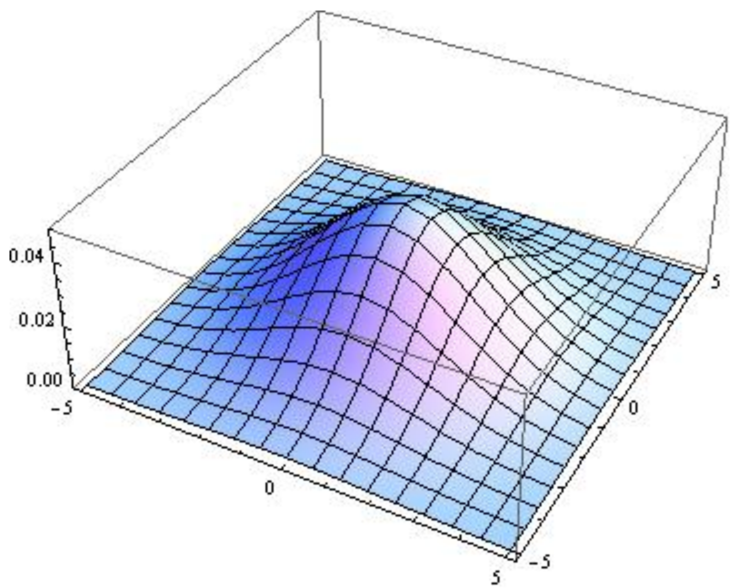


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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



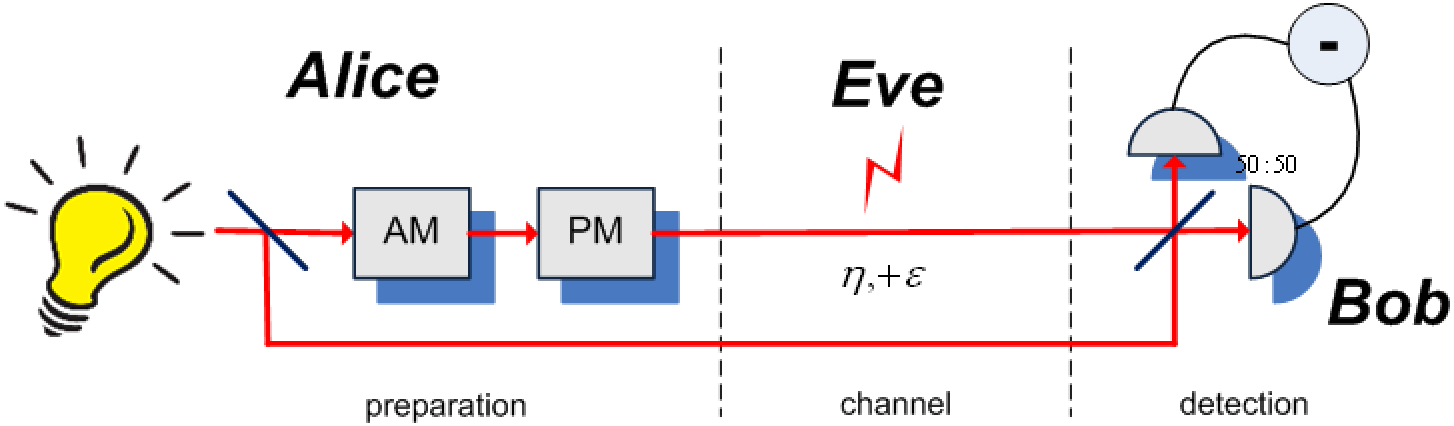


Mixture

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 →

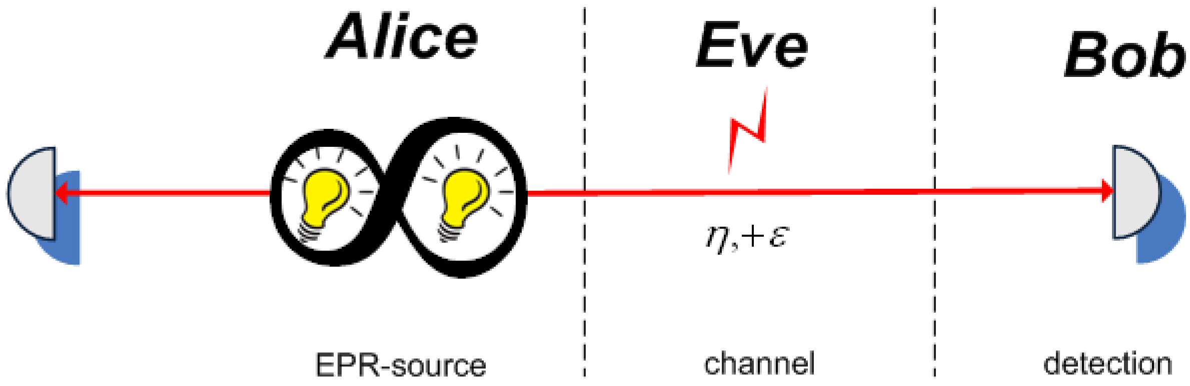
Direct reconciliation

Tolerates any pure loss

← Classical Information

Reverse reconciliation

CV QKD: entangled-based

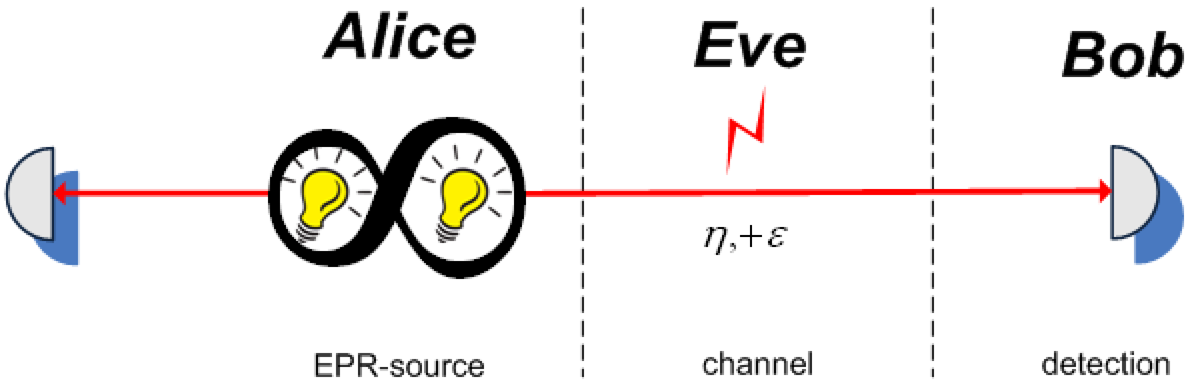


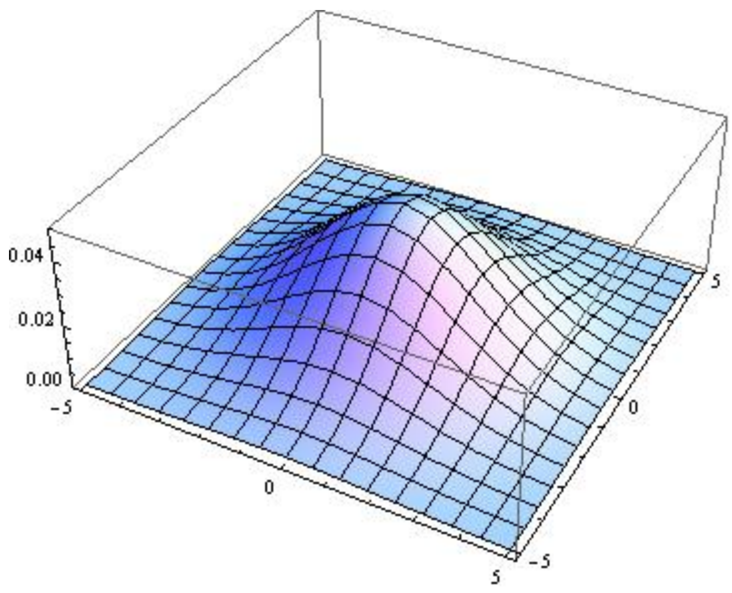
Two-mode squeezed vacuum state:

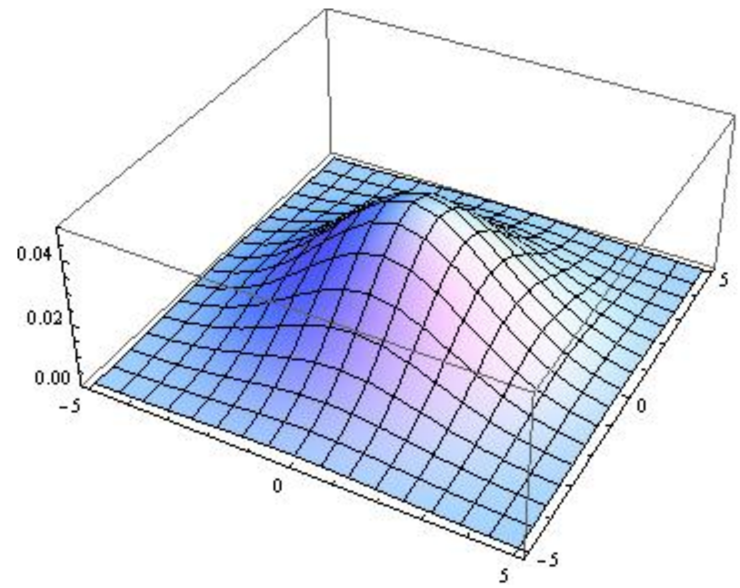
$$|x\rangle\rangle = \sqrt{(1-x^2)} \sum_n x^n \, |n,n\rangle\rangle$$

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

CV QKD: entangled-based

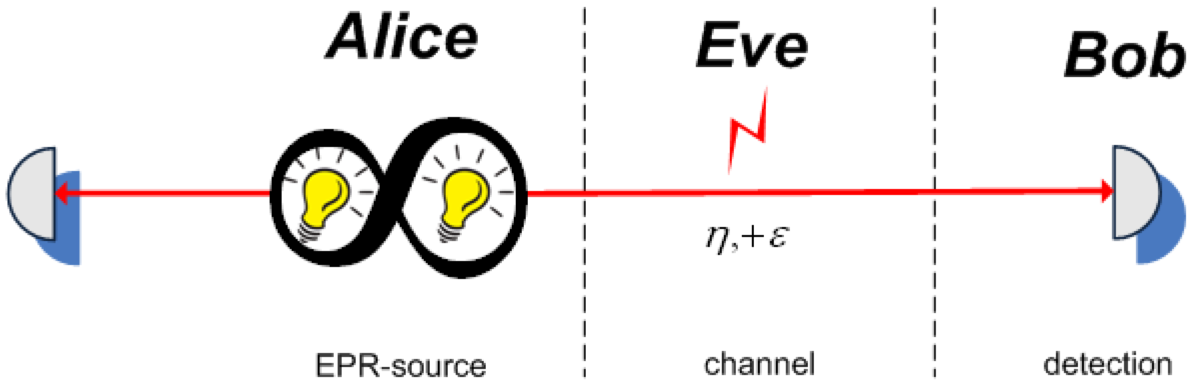




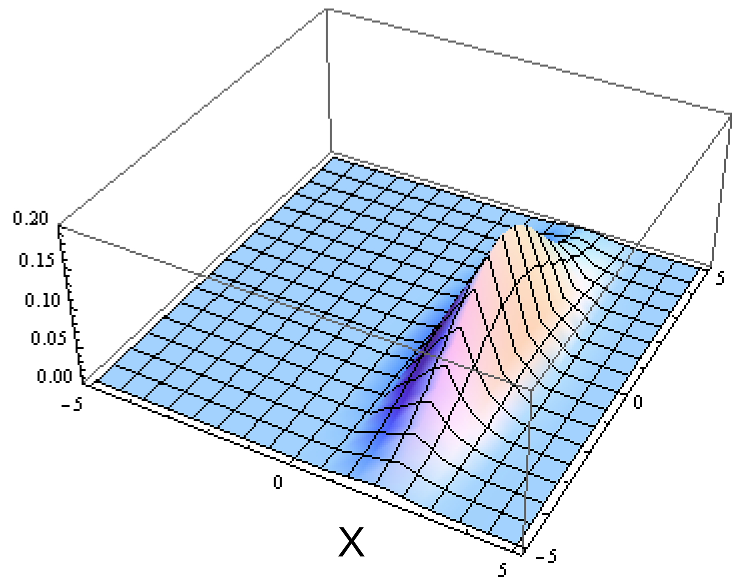


Before homodyne measurement

CV QKD: entangled-based

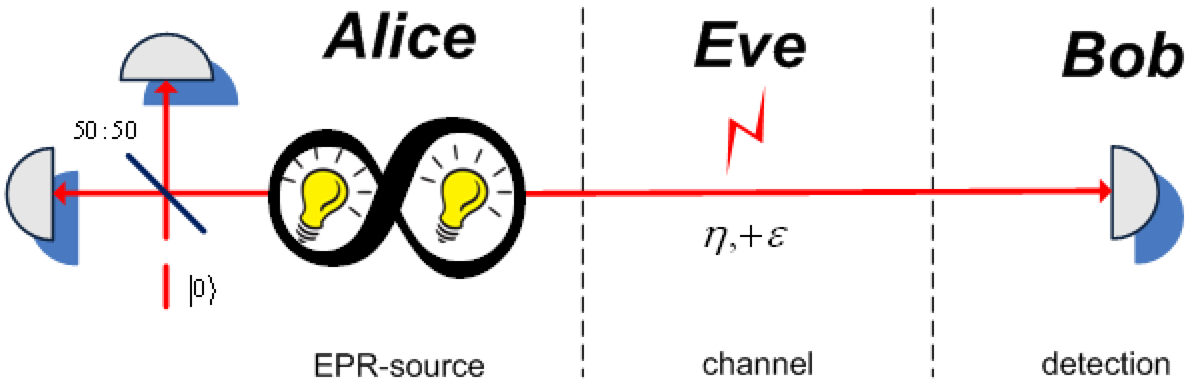


X

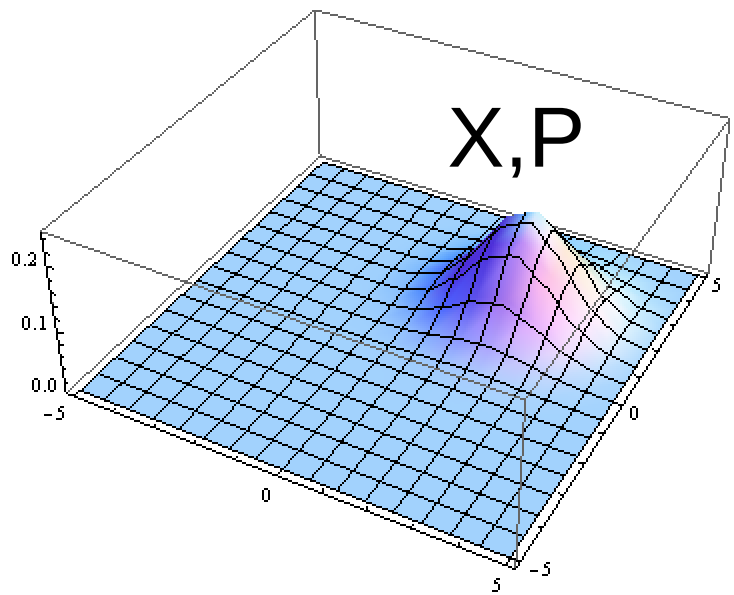


After homodyne measurement

CV QKD: entangled-based

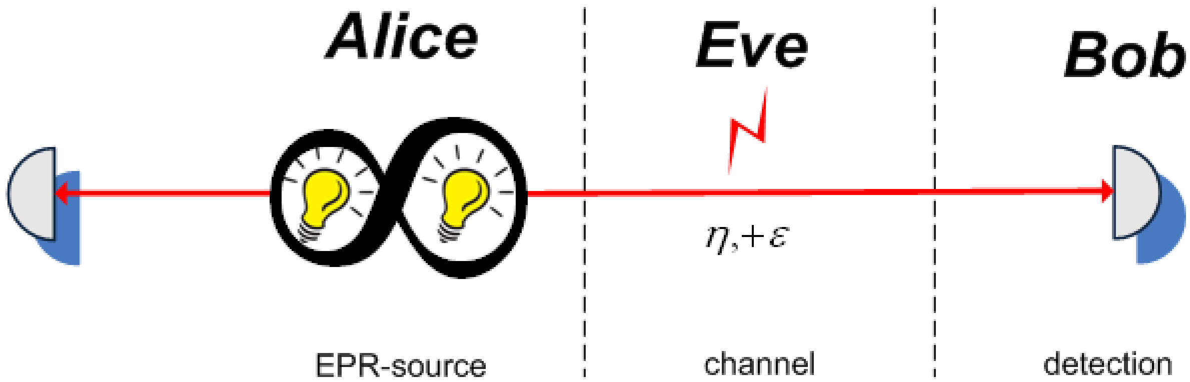


X,P



After heterodyne measurement

CV QKD: entangled-based



Advantages:

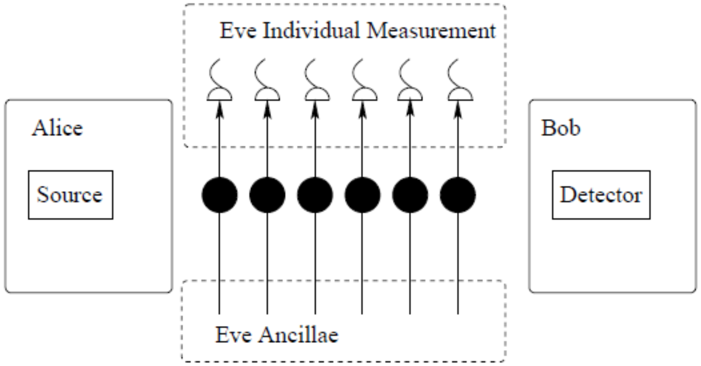
- Complete theoretical description of coherent/squeezed protocol
- Potential scalability

CV QKD: security

<u>Individual attacks.</u> Key rate: $$I_i = I_{AB} - I_{BE}$$

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

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

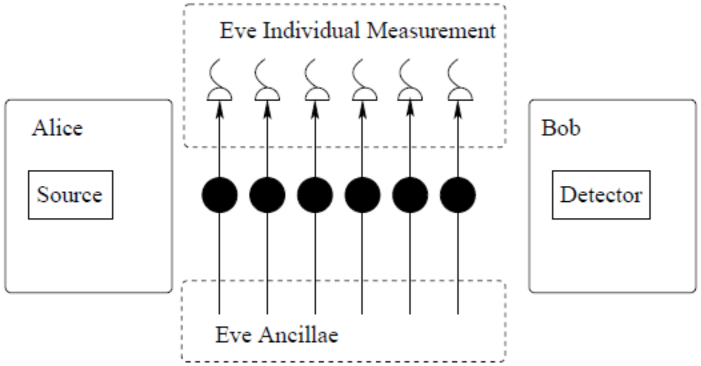


CV QKD: security

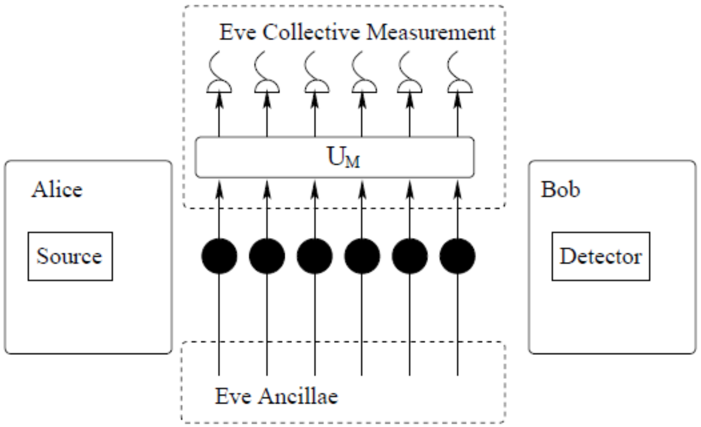
Individual attacks. Key rate: $I_i = I_{AB} - I_{BE}$

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

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



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



Holevo quantity – upper limit on the information available to Eve, calculated through von Neumann (quantum) entropy of the respective states:

$$\chi_{BE} = S_E - \int P(B) S_{E|B} dB$$

$$S(\rho) = -Tr\, \rho \log \rho$$

Extremality of Gaussian states

Wolf-Giedke-Cirac theorem. If *f* satisfies:

1. Continuity in trace norm (if $\|\rho_{AB}^{(n)} - \rho_{AB}\|_1 \to 0$ when $n \to \infty$, then $f(\rho_{AB}^{(n)}) \to f(\rho_{AB})$
1. Invariance over local "Gaussification" unitaries $f(U_G^\dagger \otimes U_G^\dagger \, \rho_{AB}^{\otimes N} \, U_G \otimes U_G) = f(\rho_{AB}^{\otimes N})$
2. Strong sub-additivity $f(\rho_{A_{1\ldots N}B_{1\ldots N}}) \leq f(\rho_{A_1B_1}) + \ldots + f(\rho_{A_NB_N})$

Then , for every bipartite state ρ_{AB} with covariance matrix γ_{AB} we have

$$\boxed{f(\rho_{AB}) \leq f(\rho_{AB}^G)}$$

[*M. M. Wolf, G. Giedke, and J. I. Cirac. Phys. Rev. Lett. 96, 080502 (2006)]*

Extremality of Gaussian states

Wolf-Giedke-Cirac theorem. If *f* satisfies:

1. Continuity in trace norm (if $\|\rho_{AB}^{(n)} - \rho_{AB}\|_1 \to 0$ when $n \to \infty$, then $f(\rho_{AB}^{(n)}) \to f(\rho_{AB})$
1. Invariance over local "Gaussification" unitaries $f(U_G^\dagger \otimes U_G^\dagger \, \rho_{AB}^{\otimes N} \, U_G \otimes U_G) = f(\rho_{AB}^{\otimes N})$
2. Strong sub-additivity $f(\rho_{A_{1\ldots N}B_{1\ldots N}}) \leq f(\rho_{A_1B_1}) + \ldots + f(\rho_{A_NB_N})$

Then , for every bipartite state ρ_{AB} with covariance matrix γ_{AB} we have

$$\boxed{f(\rho_{AB}) \leq f(\rho_{AB}^G)}$$

[*M. M. Wolf, G. Giedke, and J. I. Cirac. Phys. Rev. Lett. 96, 080502 (2006)]*

Consequence:

Gaussian states maximize the information leakage.
Covariance matrix description is enough to prove security.

[R. Garcıa-Patron and N.J. Cerf. Phys. Rev. Lett. 97, 190503, (2006);
M. Navascus, F. Grosshans and A. Acin, Phys. Rev. Lett. 97, 190502 (2006)]

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

λ_i - symplectic eigenvalues of the covariance matrix γ_E ,

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

CV Quantum key distribution: security

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

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

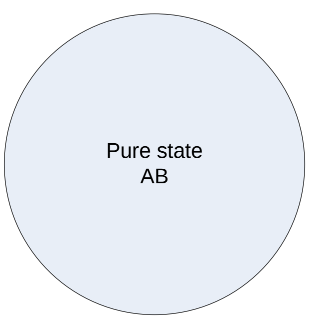
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

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

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:



CV Quantum key distribution: security

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

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

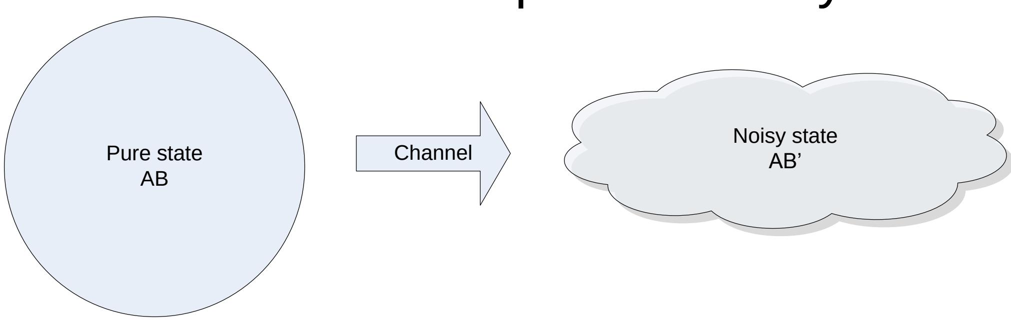
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

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:



CV Quantum key distribution: security

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

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

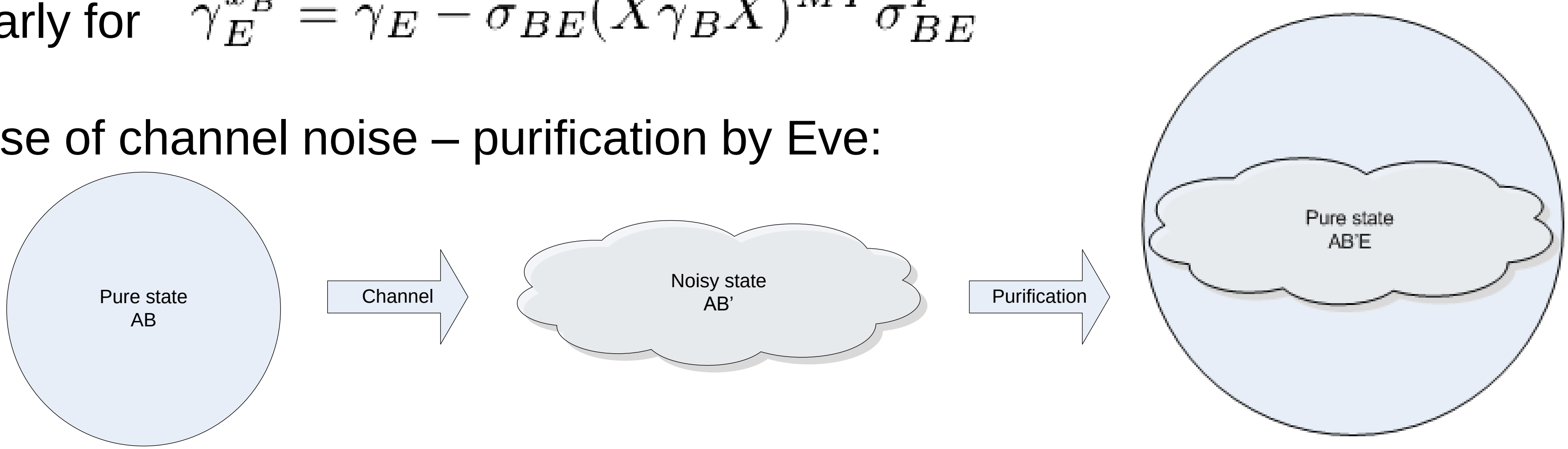
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

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

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:



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:

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

$$\gamma_A^{x_B} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T \qquad X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

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

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:

It is important to distinguish between trusted and untrusted noise.

All trusted noise must be purified.

CV Quantum key distribution: security

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

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

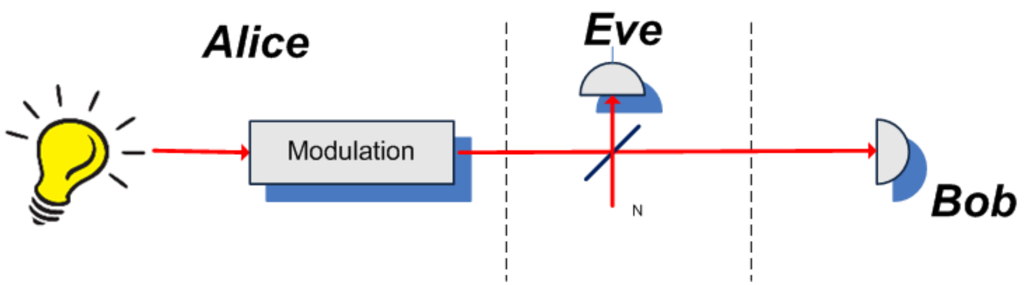
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

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

λ_i - symplectic eigenvalues of the covariance matrix γ_E ,

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

Example of purification:



CV Quantum key distribution: security

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

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

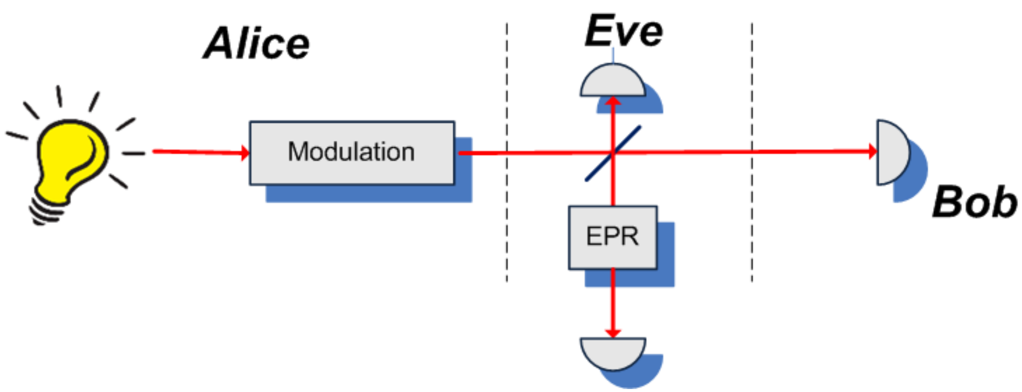
(*Renner, Gisin, Kraus, Phys. Rev. A 72, 012332, 2005)*

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

λ_i - symplectic eigenvalues of the covariance matrix γ_E ,

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

Example of purification:



CV QKD: security

Source covariance matrix:

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

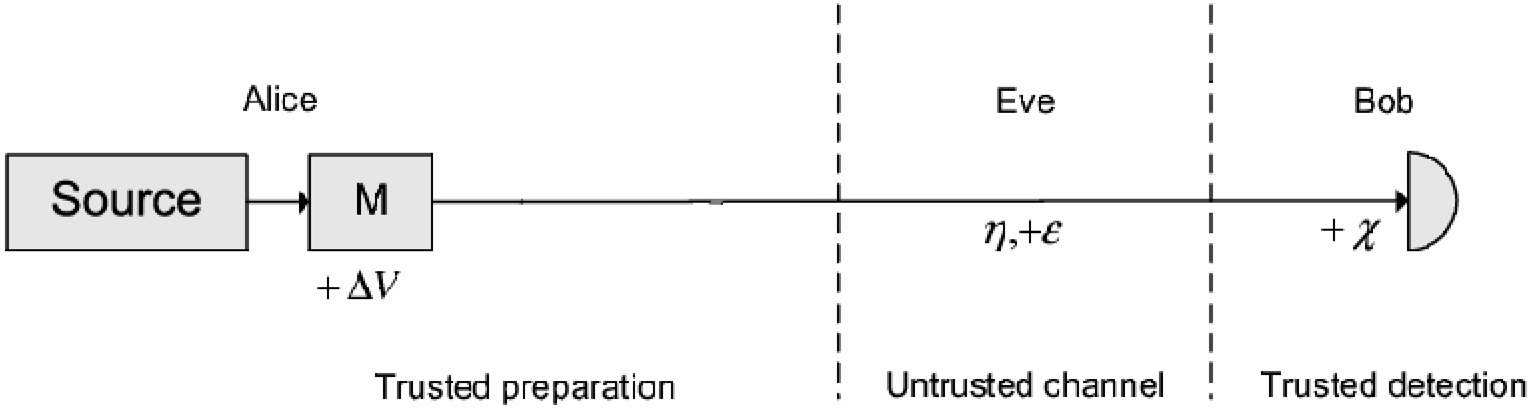
$$\gamma_A = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}$$

After noisy and lossy channel:

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

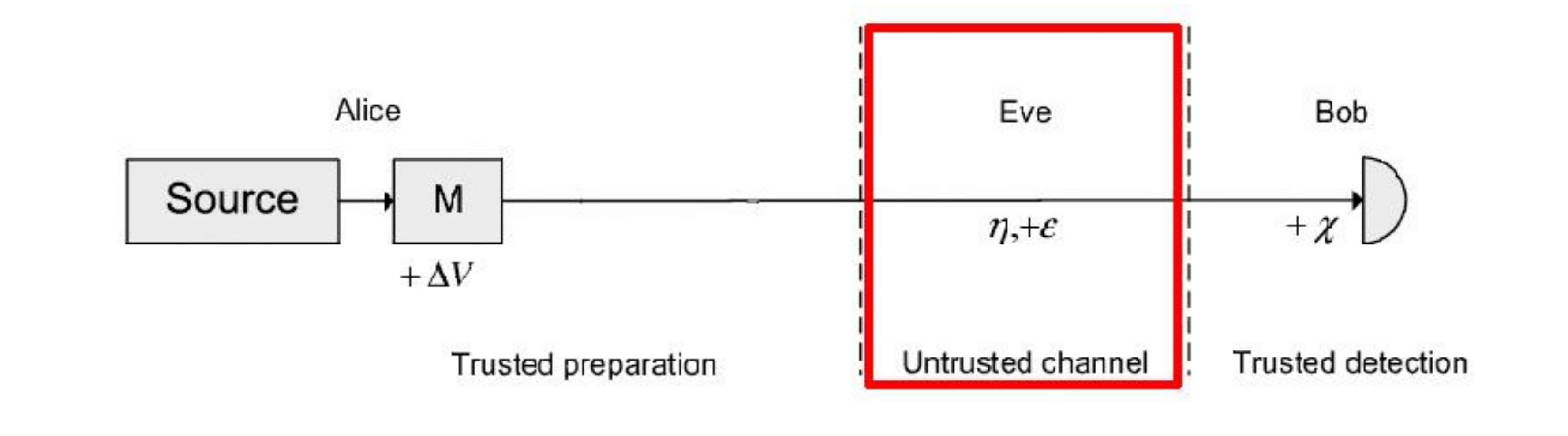
Influence of noise

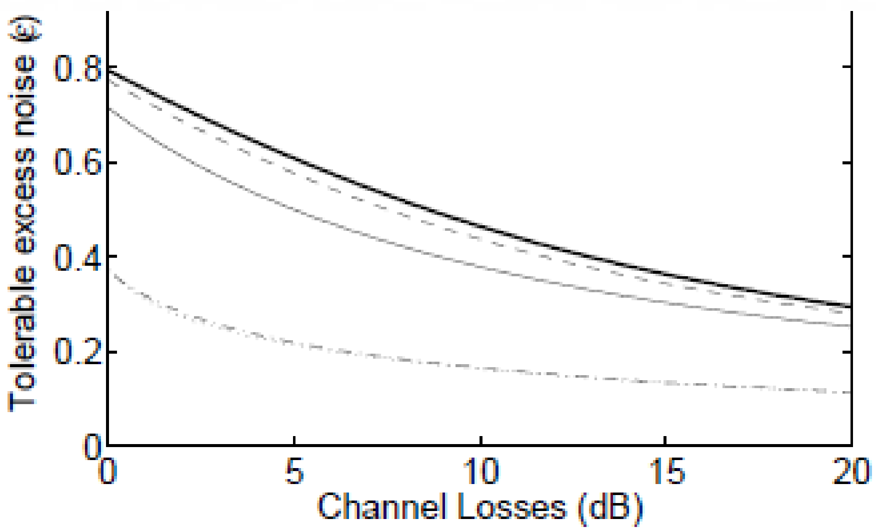
Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



Influence of noise

Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



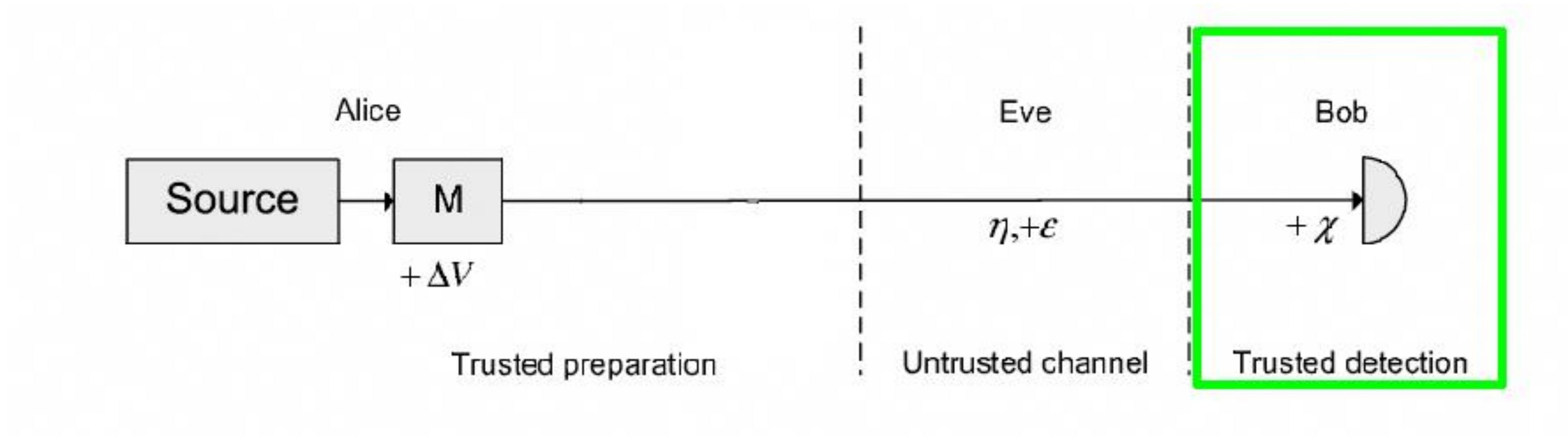


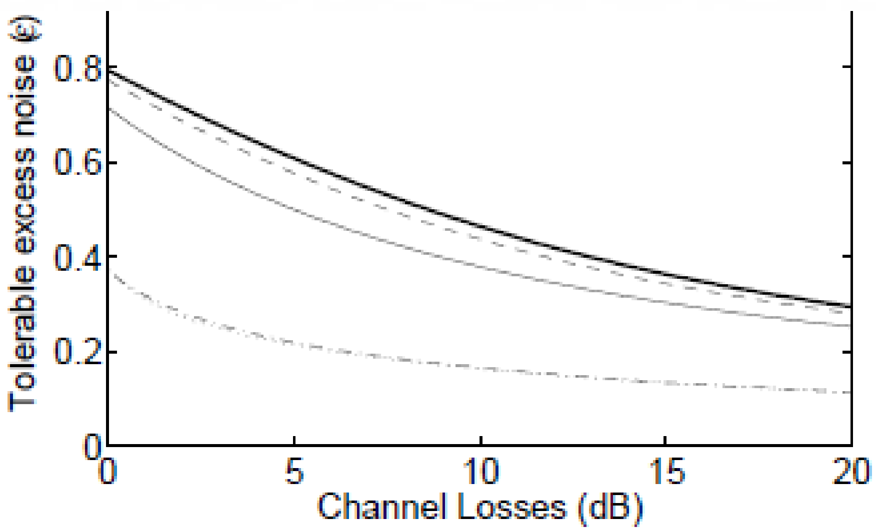
Untrusted noise limits security.

◀Typical dependence of maximum tolerable channel excess noise versus loss

Influence of noise

Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)





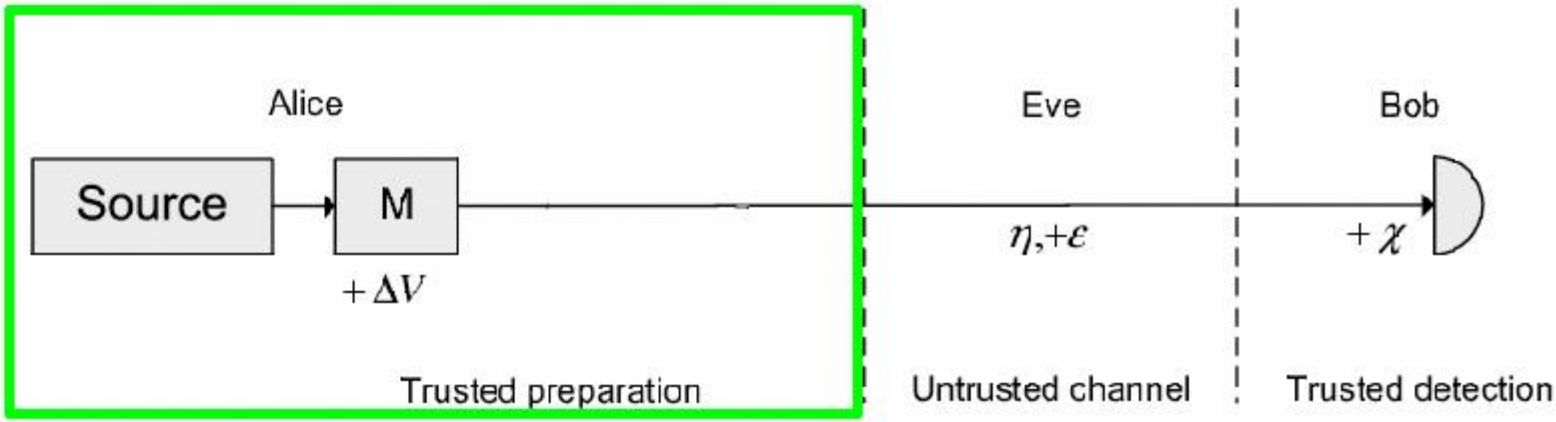
Trusted detection noise improves (!) security.

◀Typical dependence of maximum tolerable channel excess noise versus loss

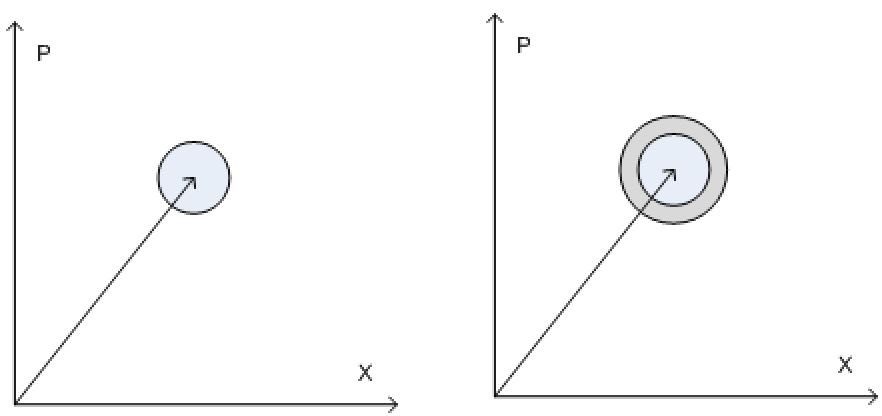
R. Garcia-Patron, N. Cerf, PRL 102 120501 (2009)

Influence of noise

<u>Distinguishing the noise types:</u> **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)

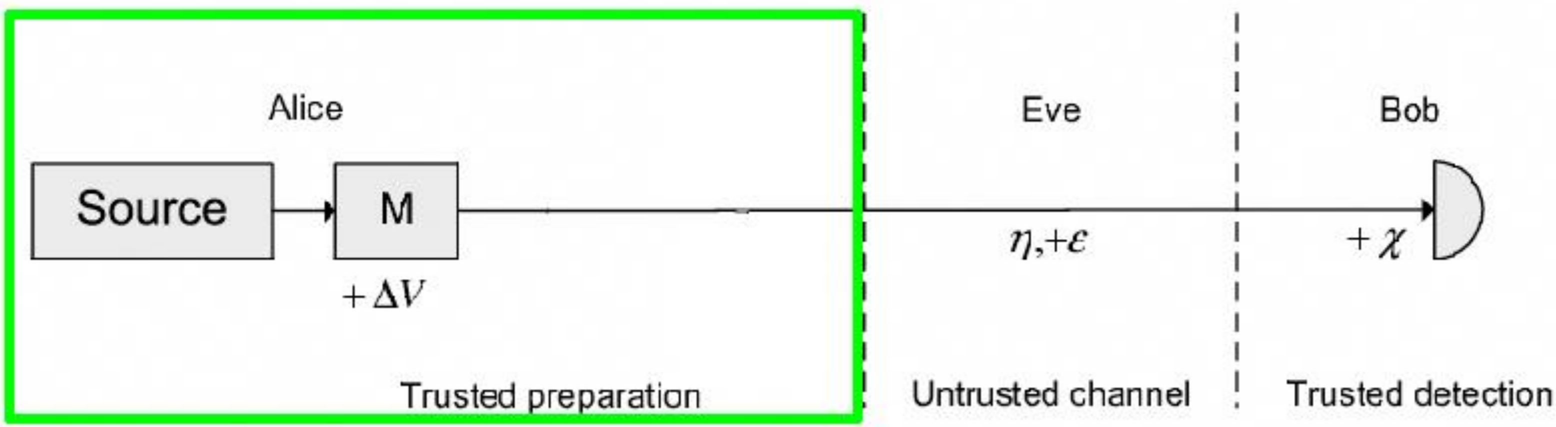


Trusted preparation noise. Coherent states: phase-insensitive excess noise



Influence of noise

Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



Trusted preparation noise. Coherent states: phase-insensitive excess noise

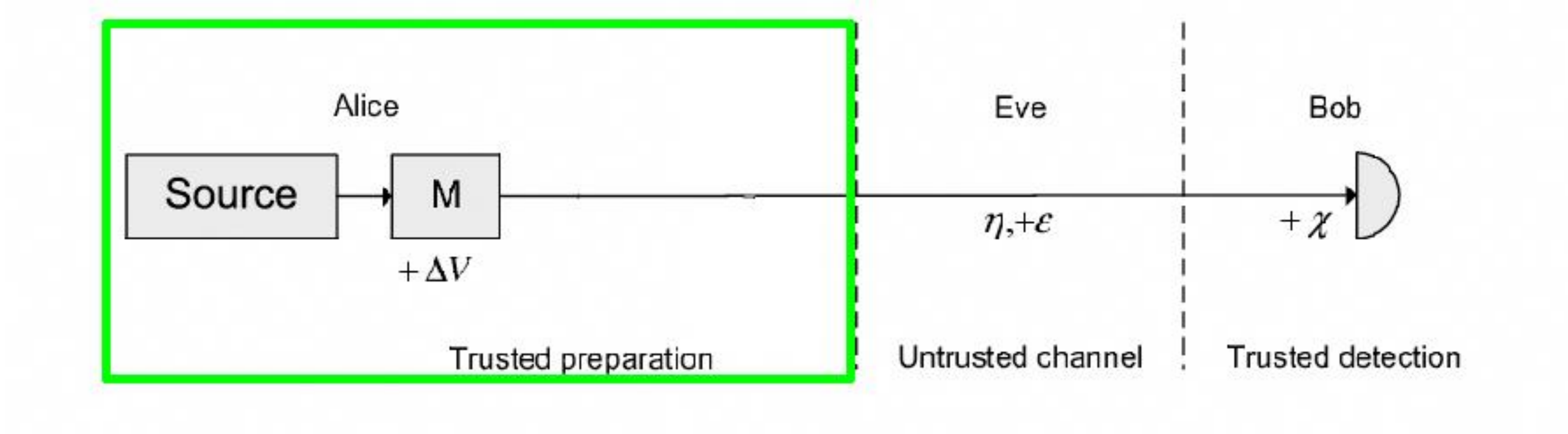
Is security breaking:

$$\boxed{\Delta V_{I,\max} = \frac{1}{1-\eta}}$$

η - channel transmittance

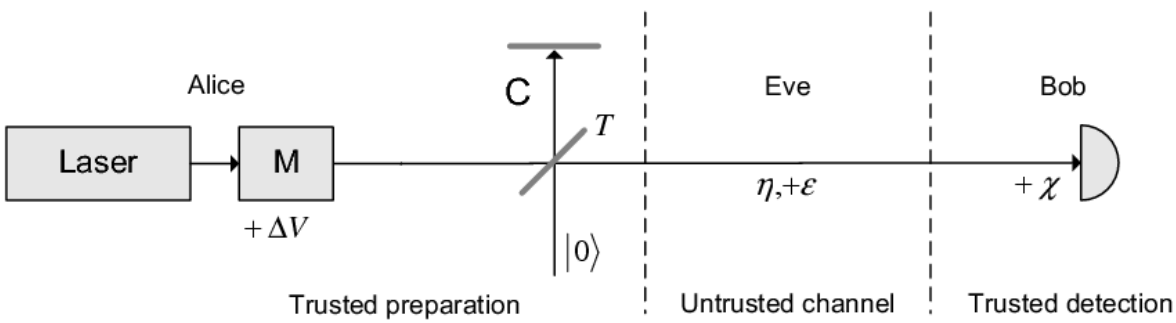
Influence of noise

Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



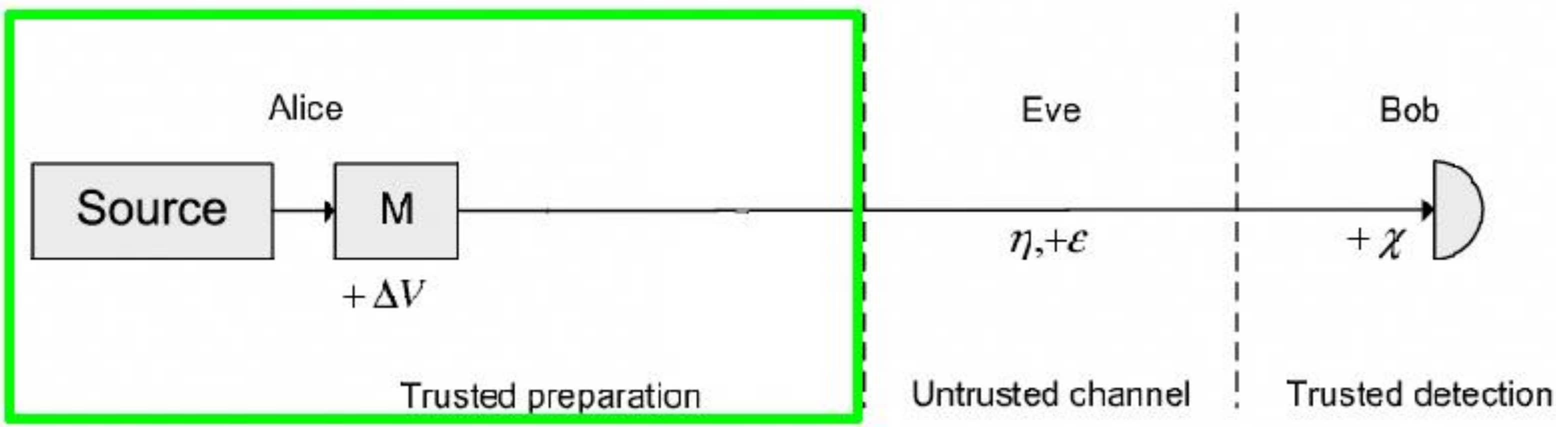
Trusted preparation noise. Coherent states: phase-insensitive excess noise

Purification:



Influence of noise

Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



Trusted preparation noise. Coherent states: phase-insensitive excess noise

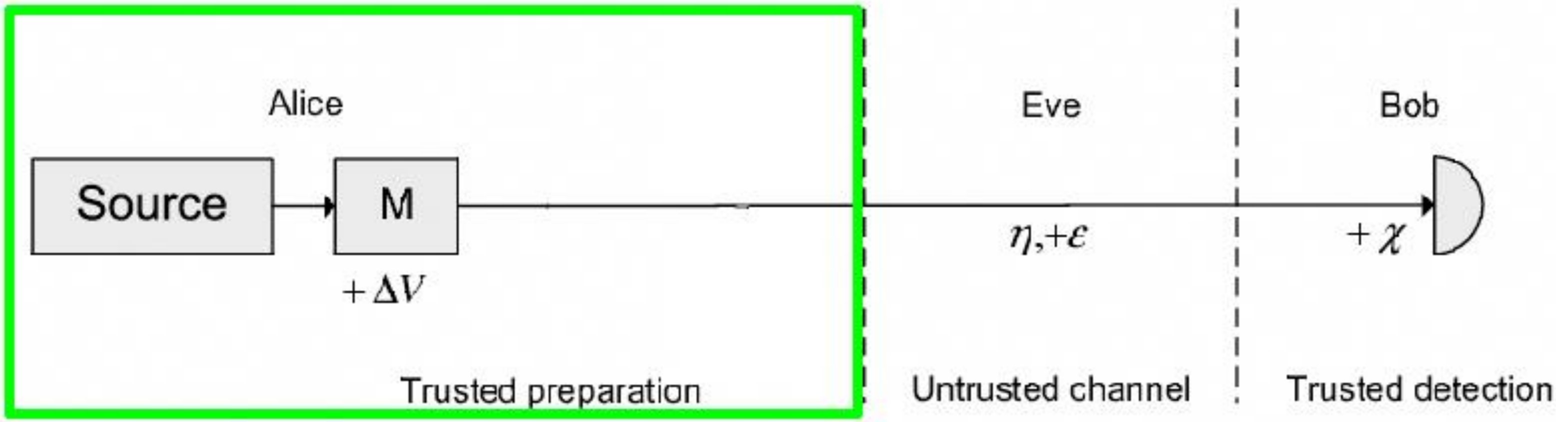
Purification restores security:

$$\Delta V_{I,max} = \frac{1}{T(1-\eta)}$$

*[V. Usenko, R. Filip, Phys. Rev. A **81**, 022318 (2010) / arXiv:0904.1694]*

Influence of noise

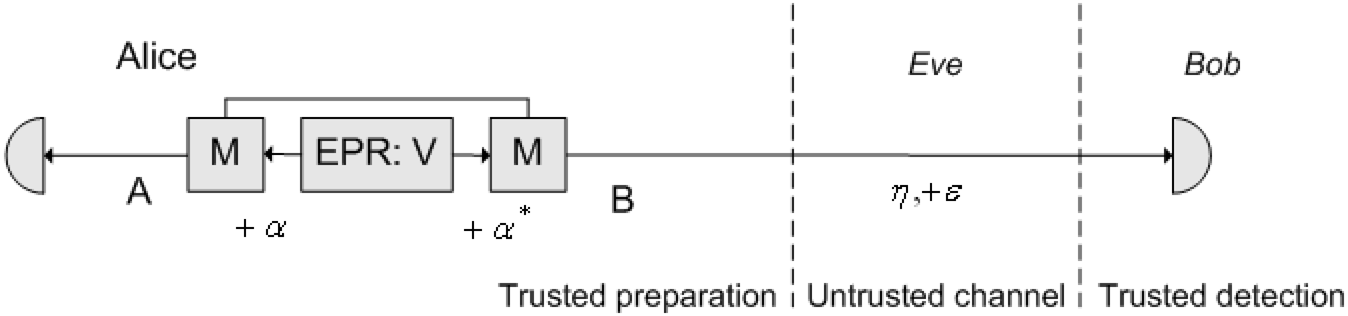
Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



Trusted preparation noise. Coherent states: phase-insensitive excess noise

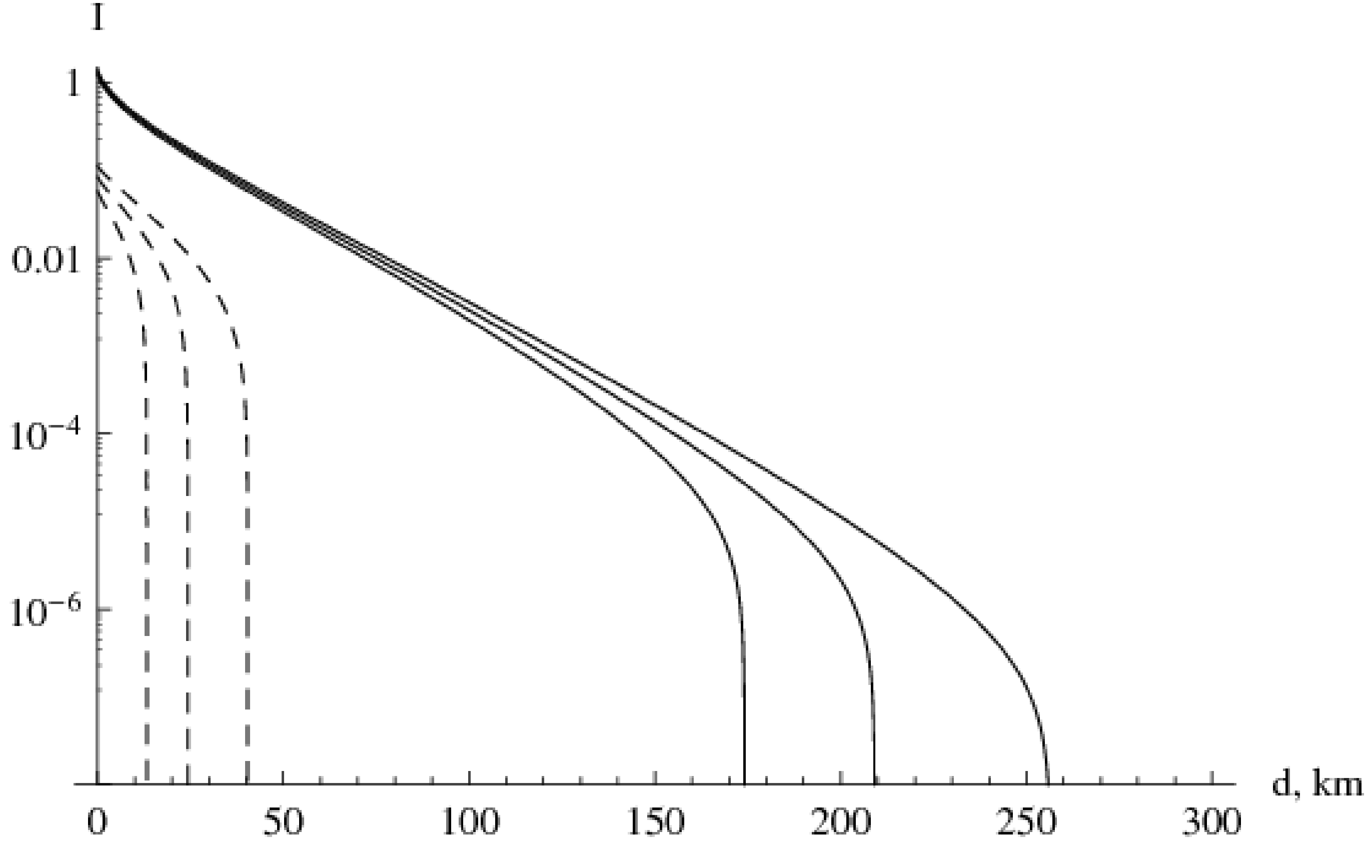
What if noise is correlated?

Modulation of entangled states



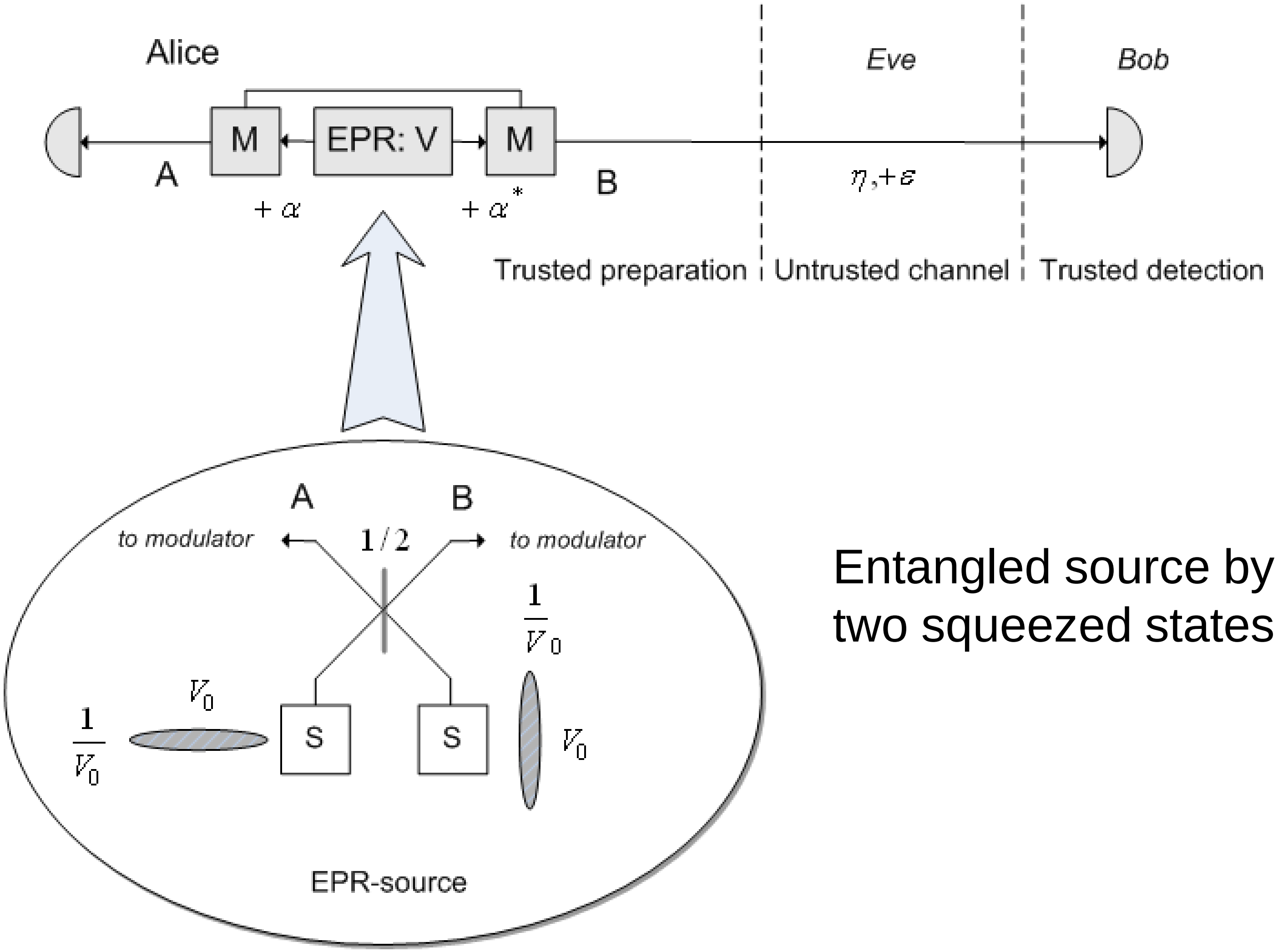
Turning noise to correlations: additional modulator

Modulation of entangled states



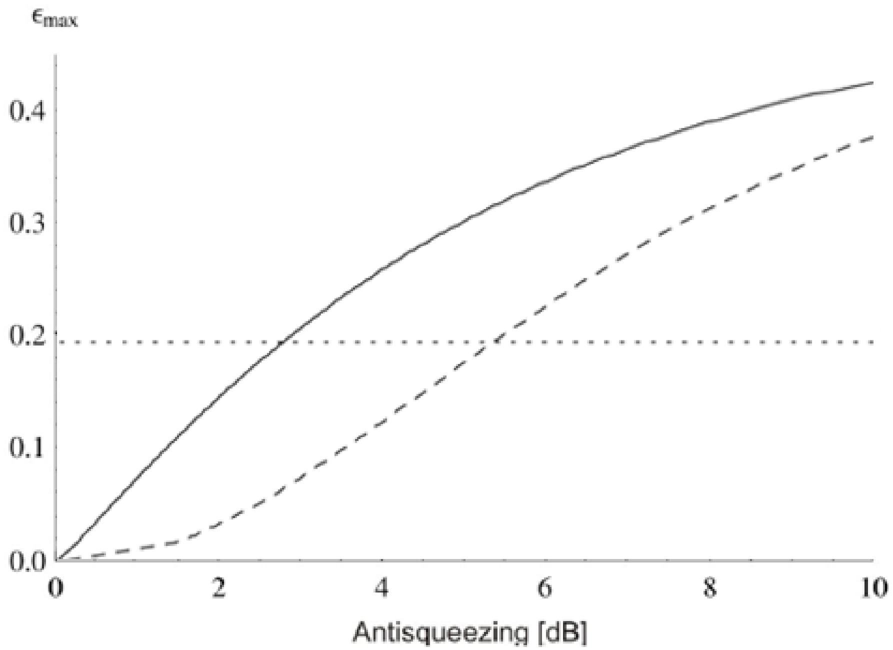
Key rate vs channel distance (standard attenuation).
Dashed line: no additional modulation;
Solid line: additional strong modulation (50 SNU).
Moderate squeezing of -3 dB.
Channel noise: left to right 8%, 7%, 6% SNU.

Modulation of entangled states



Entangled source by coupling of two squeezed states

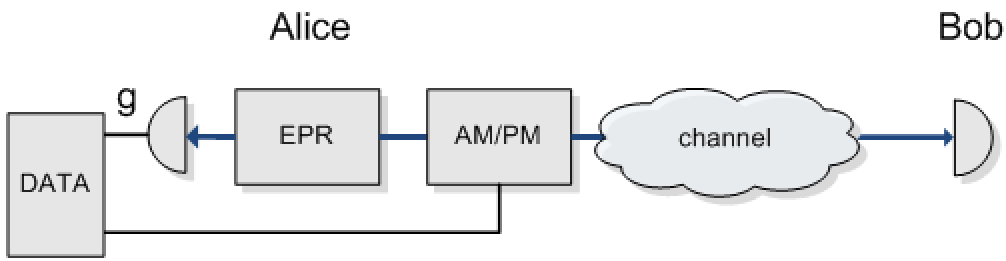
Modulation of entangled states



Channel noise security threshold for collective attacks.
Solid line: high additional modulation variance $\Delta V = 100$
Dashed line – no additional modulation.
Dotted line: strongly modulated coherent state
Channel transmittance: $\eta = 0.01$

*[V. Usenko and R. Filip, New J. Phys., **13**, 113007, (2011) / arXiv:1111.2311]*

Super-optimized protocol



Alice applies gain factor to her data:

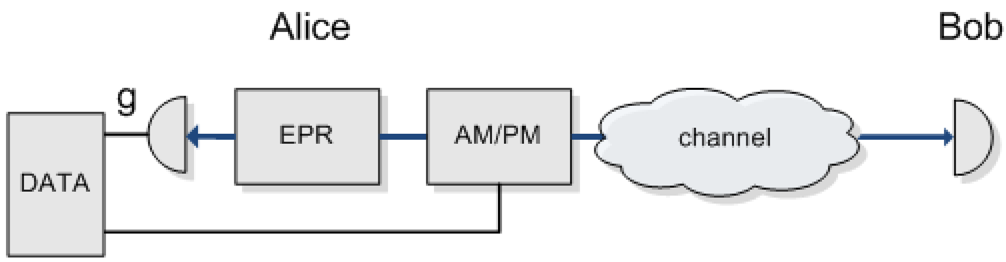
$$x'_A = g x_A + x_M$$

Covariance and correlation matrices:

$$\gamma_A = \left[g^2 \frac{1}{2}\left(\frac{1+V_0^2}{V_0} + \Delta V_0\right) + \Delta V\right]\mathbb{I}$$

$$\sigma_{AB} = \left[g \frac{1}{2}\left(\frac{1-V_0^2}{V_0} + \Delta V_0\right) + \Delta V\right]\sigma_z$$

Super-optimized protocol

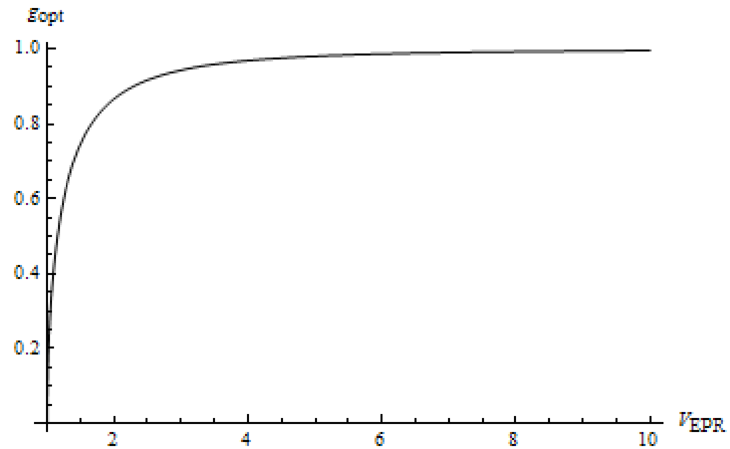


Alice applies gain factor to her data:

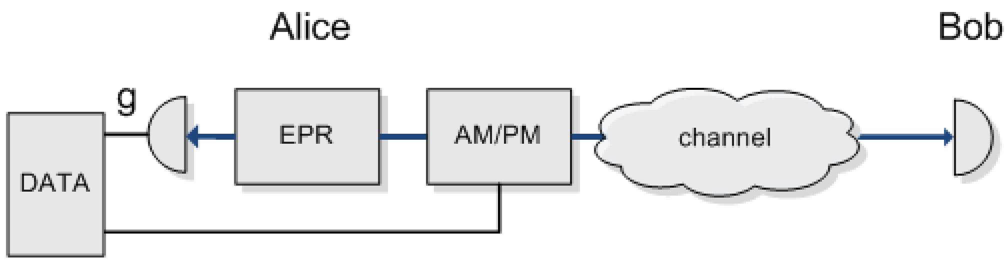
$$x'_A = g x_A + x_M$$

Optimal gain:

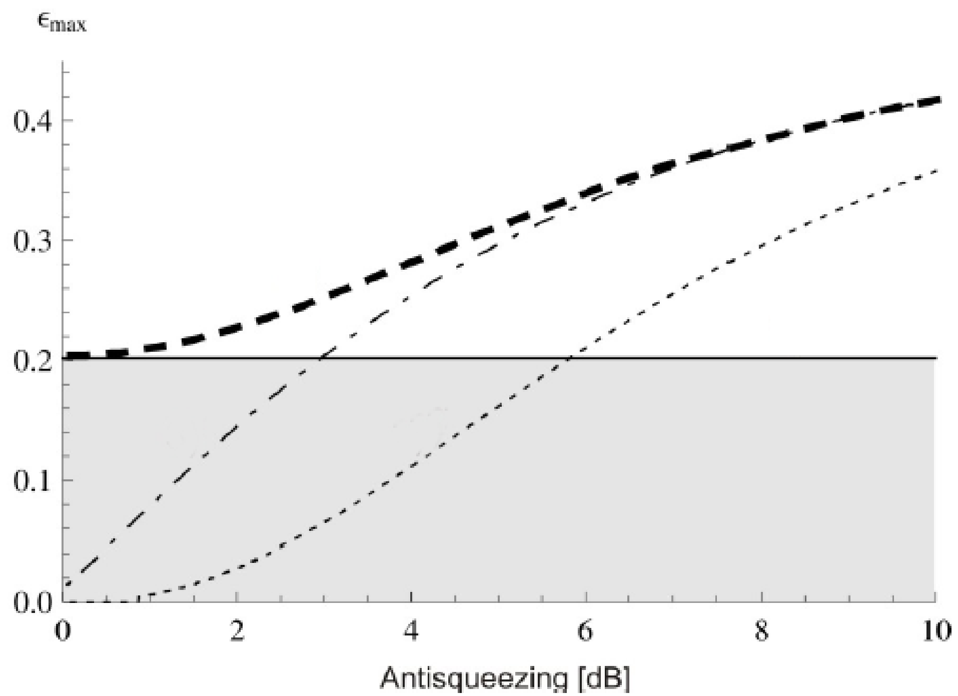
$$g_{opt} = \frac{\sqrt{V_{EPR}^{\;2} - 1}}{V_{EPR}} \equiv \frac{C_{EPR}}{V_{EPR}}$$



Super-optimized protocol

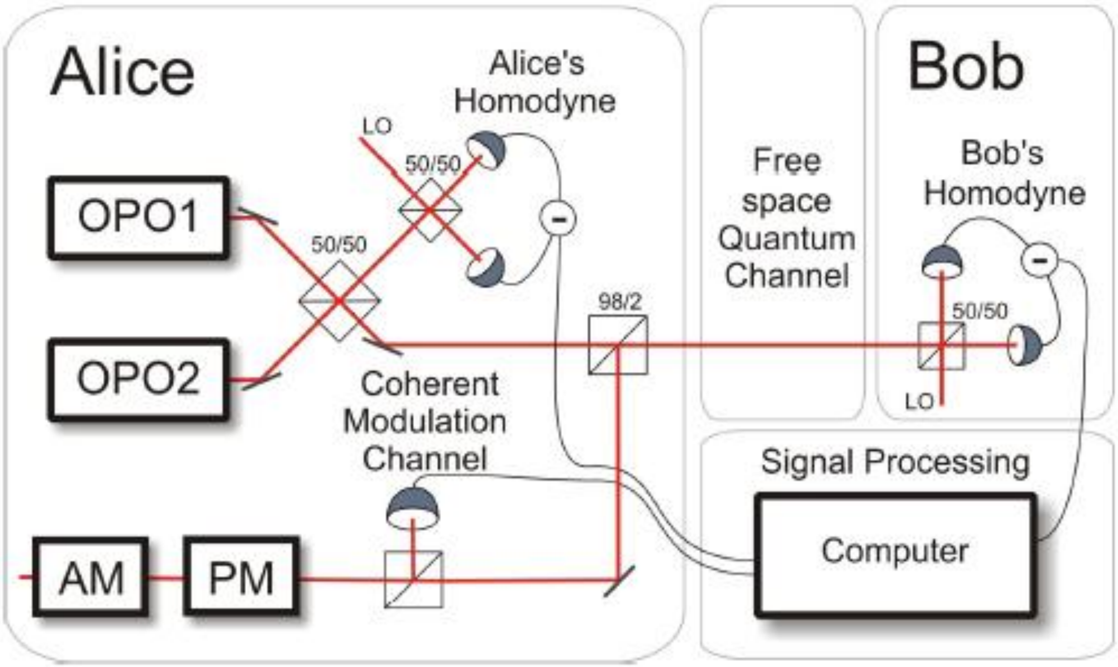


The protocol overcomes the coherent-state protocol upon any degree of squeezing



Proof-of-principle

Performed in DTU, Lyngby



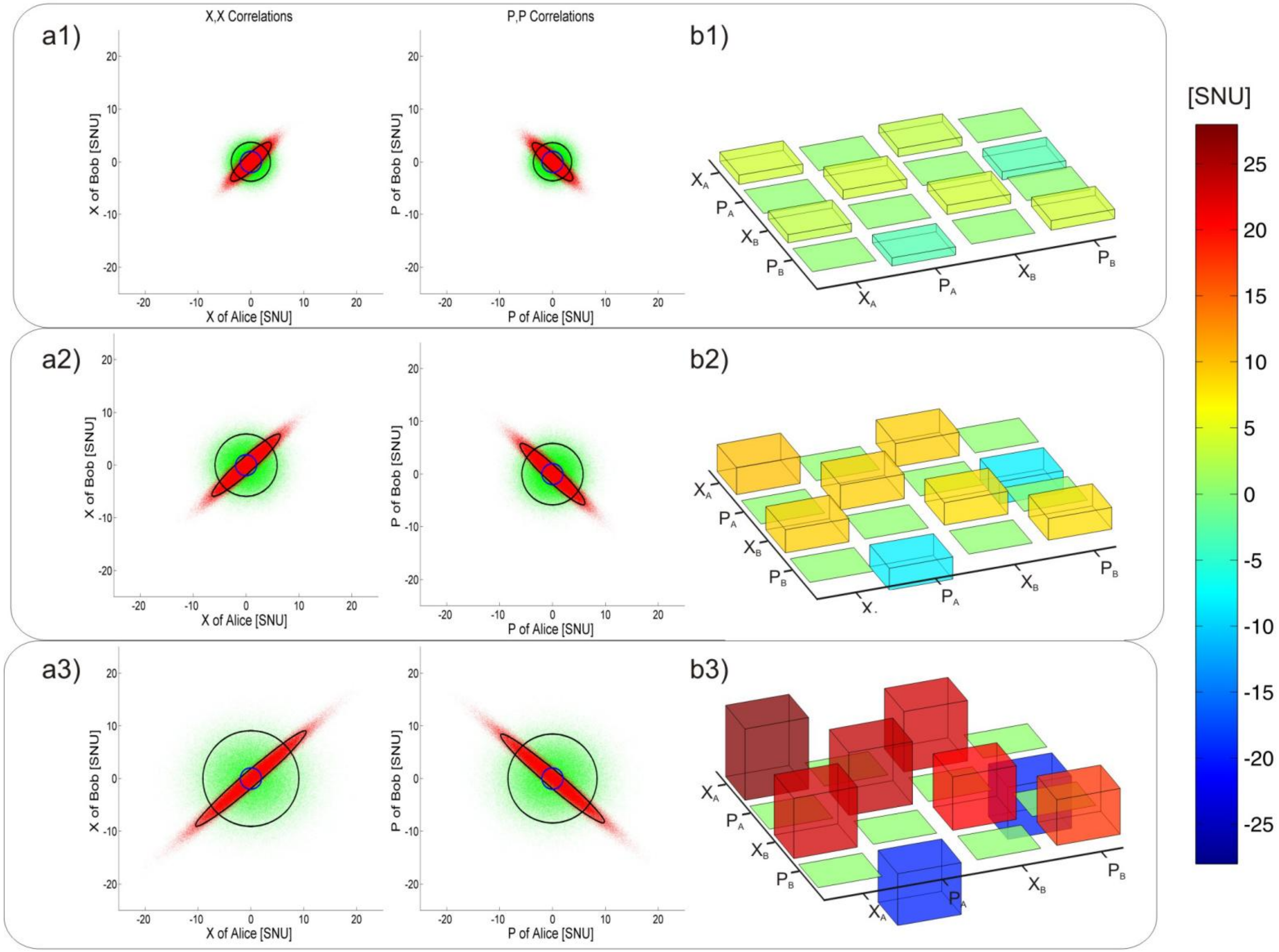
Sketch of the set-up

Proof-of-principle

No modulation

3.6 SNU

23.8 SNU



Raw quadrature data (left); covariance matrices (right)

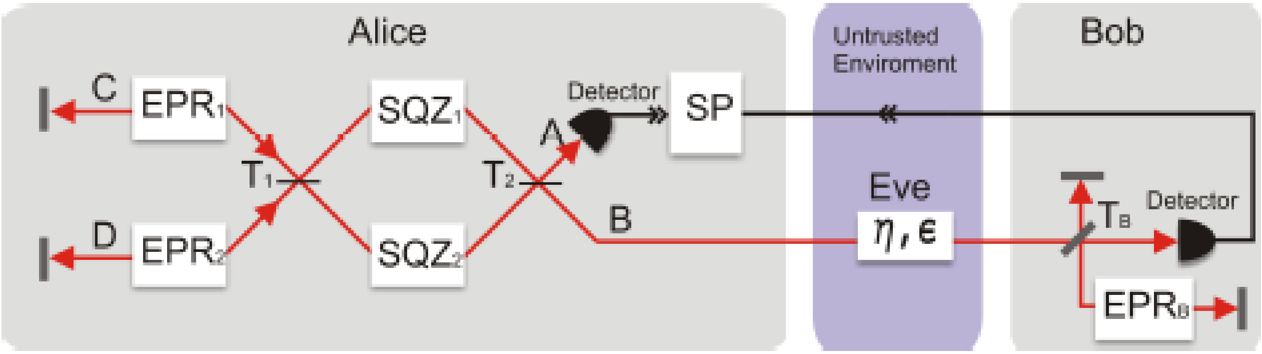
Proof-of-principle

Arbitrary (experimentally obtained) state purification using Bloch-Messiah reduction (*Braunstein, PRA 71, 055801, 2005*)

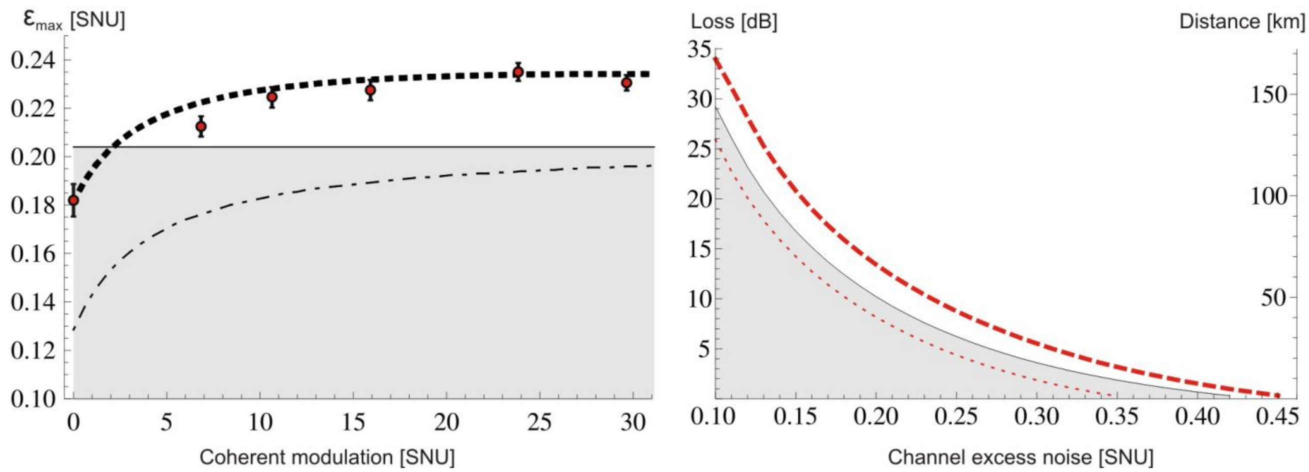
Experimental covariance matrix:

$$\gamma_{AB} = \begin{pmatrix} V_A^x & & & \\ 0 & V_A^p & & \\ C_{AB}^x & 0 & V_B^x & \\ 0 & C_{AB}^p & 0 & V_B^p \end{pmatrix}$$

Equivalent scheme:



Proof-of-principle



Untrusted channel simulation results: the squeezed-state protocol with the obtained states outperforms any coherent-state protocol (in tolerable noise and distance)

L. Madsen, V. Usenko, M. Lassen, R. Filip, U. Andersen, Nature Communications 3, 1083 (2012)

Resources

Modulation improves entangled protocol,
what is the role of squeezing then?

Generally, how much nonclassical is CV QKD?

Resources

Modulation improves entangled protocol,
what is the role of squeezing then?

Generally, how much nonclassical is CV QKD?

Let’s distinguish the resources!

Post-processing efficiency

Lower bound on secure key rate (collective attacks) upon realistic reconciliation:

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

$\beta \in [0,1]$ - post-processing efficiency.

Generally depends on SNR and algorithms.

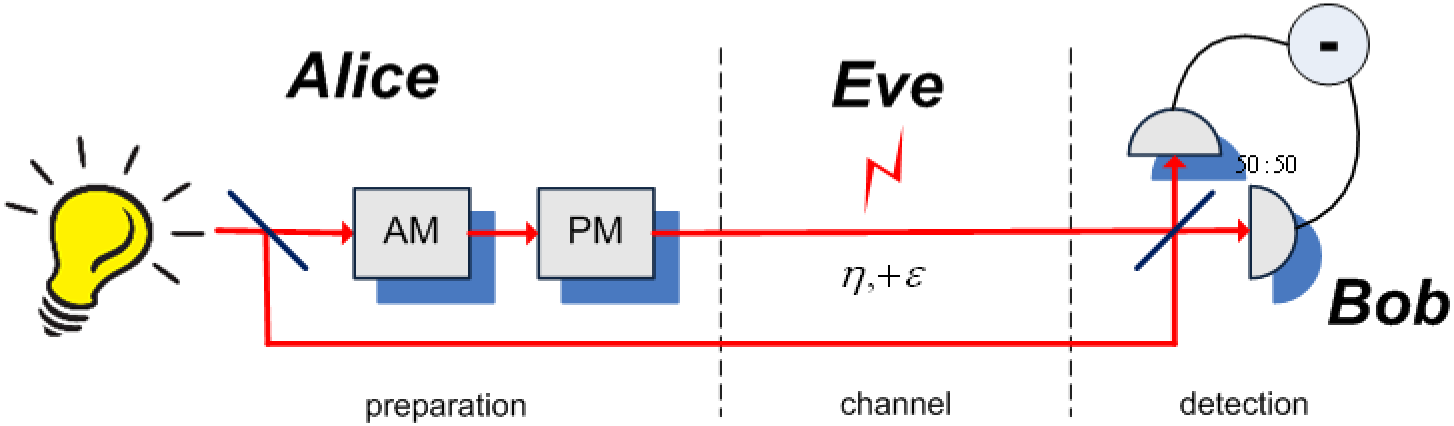
Together with channel noise – main limitation for Gaussian CV QKD (up to 25 km with coherent states at efficiency around 0.8-0.9: *J. Lodewyck et al., PRA 76, 042305, 2007*).

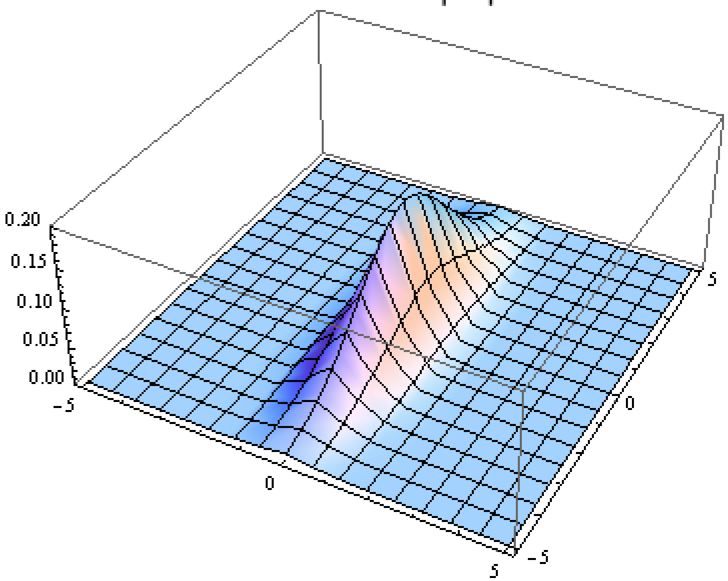
Together with information – a classical resource.

Resources:

- **Classical: information, post-processing**
- **Quantum: states (classical/nonclassical)**

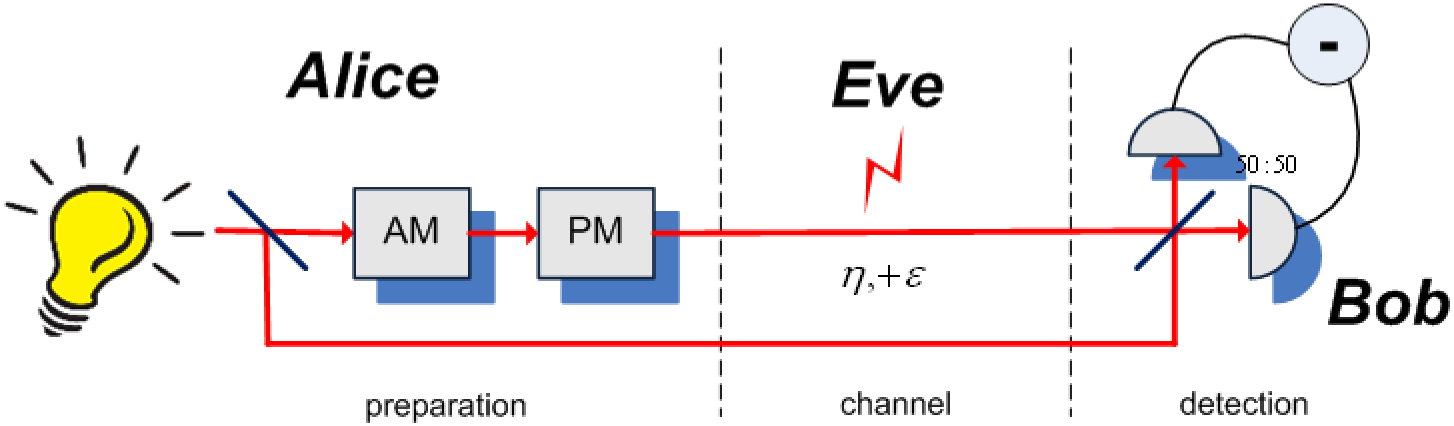
Generalized preparation

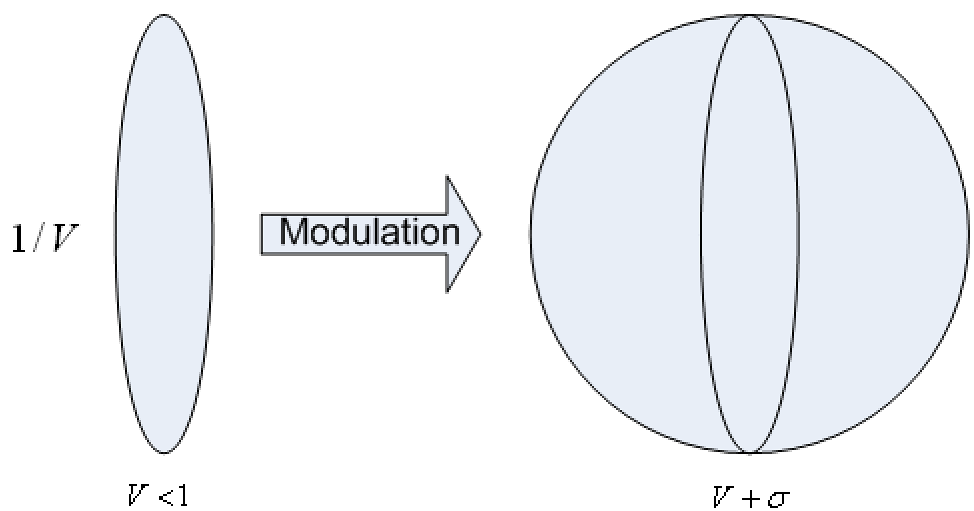




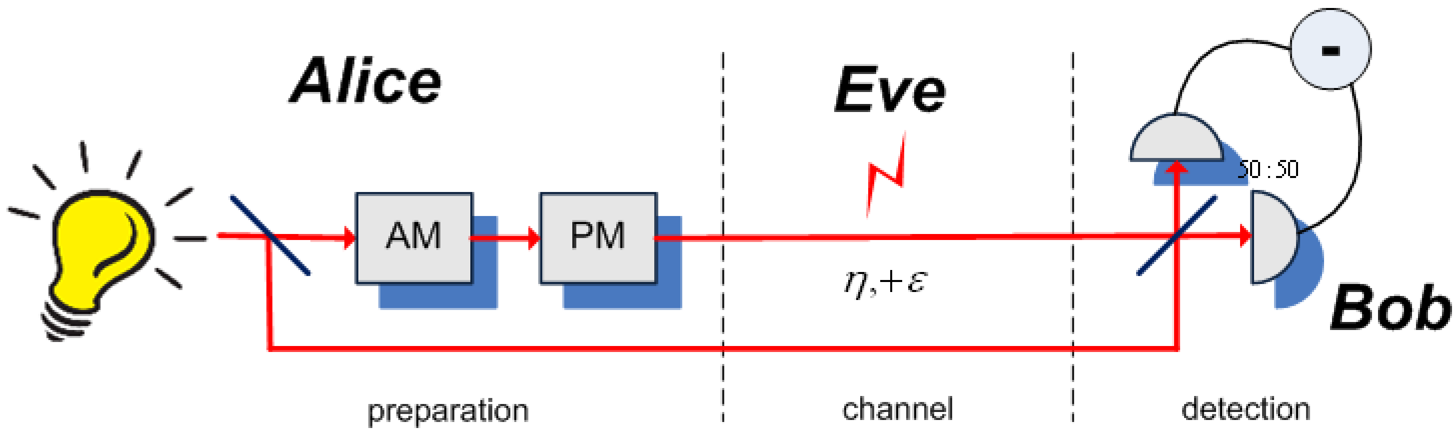
Source state

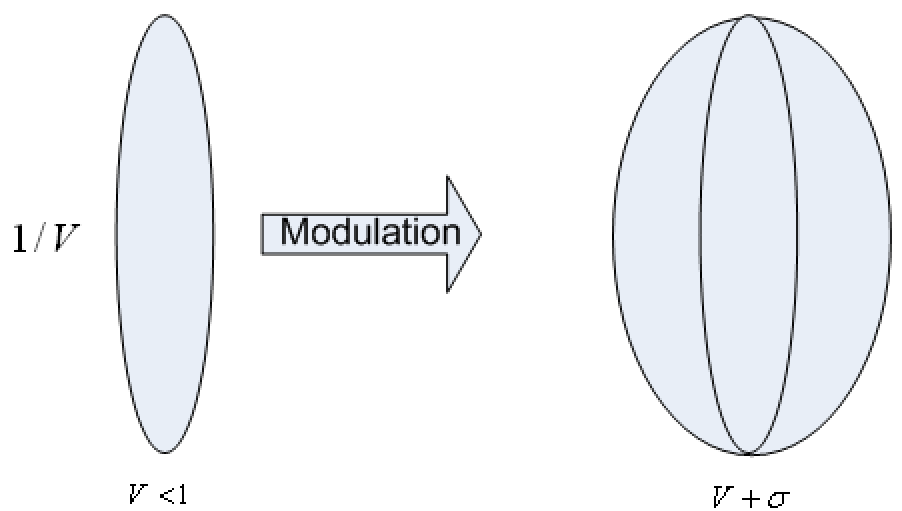
Generalized preparation



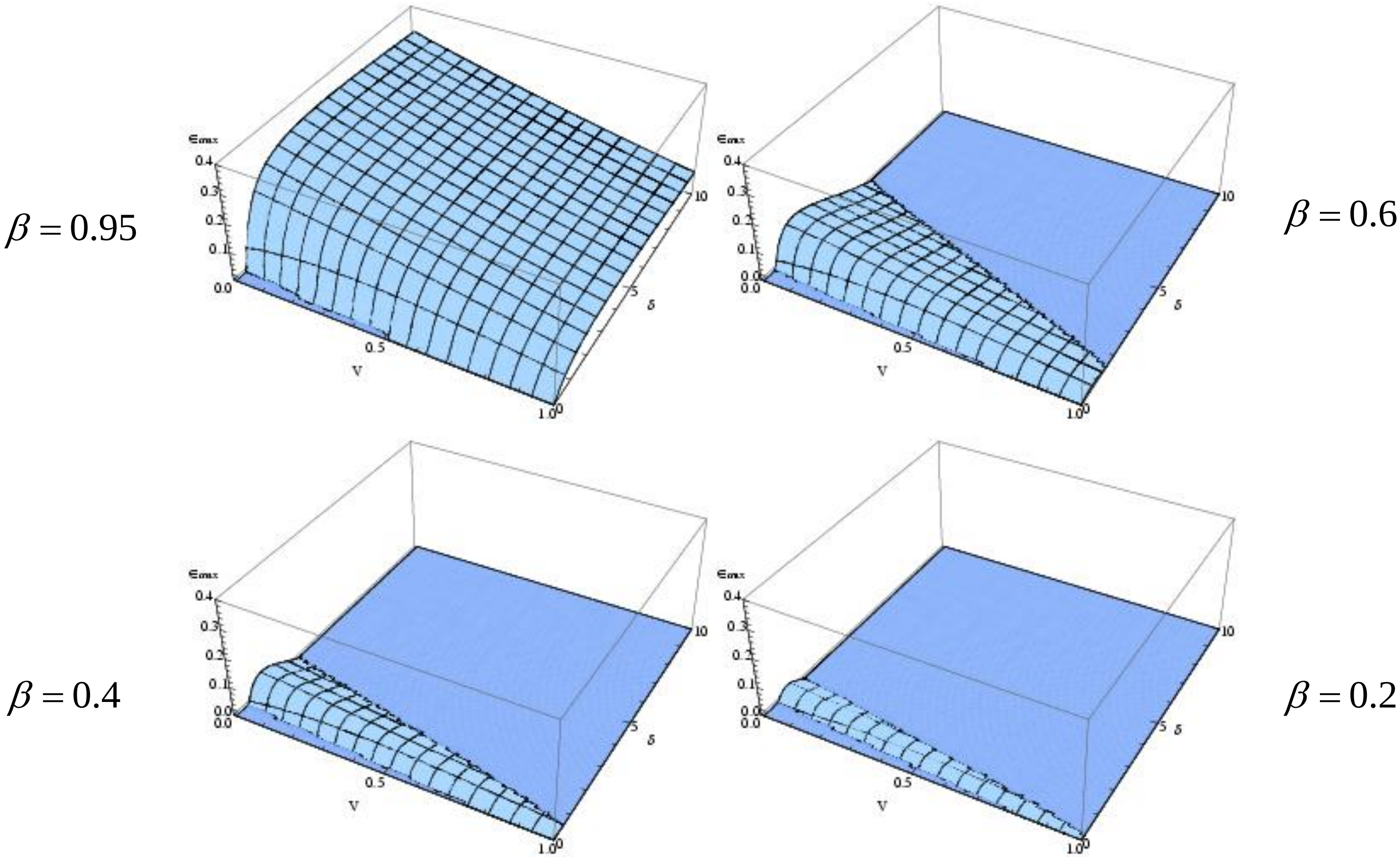


Generalized preparation



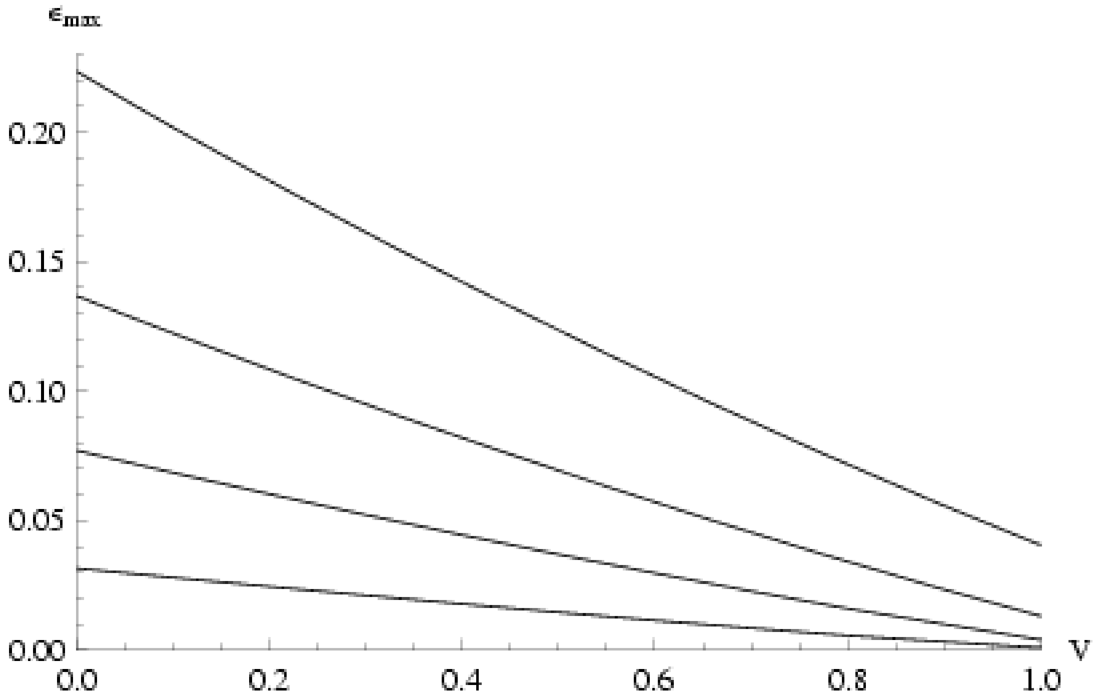


Limited post-processing



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)

$$\beta \ll 1$$

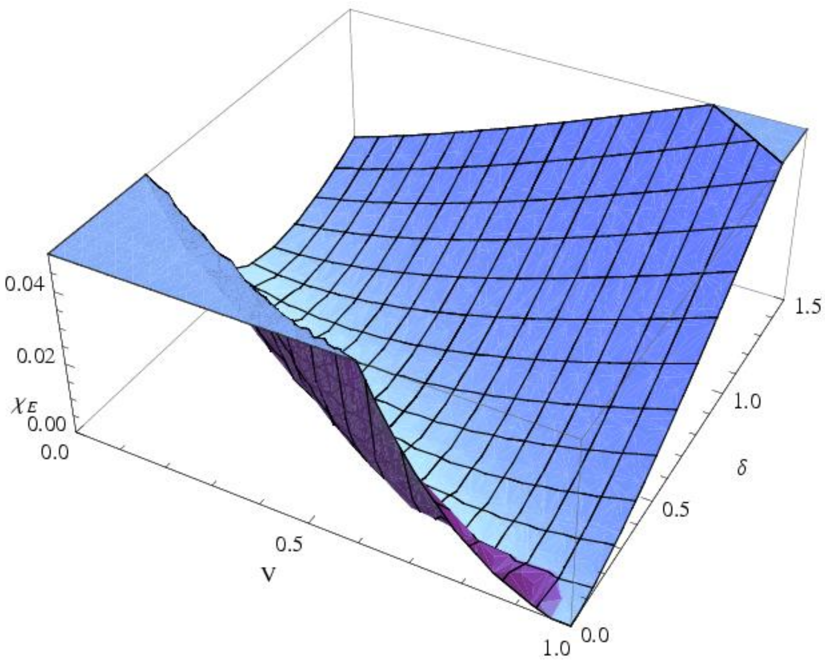
$\eta \ll 1$ $\quad I_{AB} = \sigma\eta/\log 4 + O[\eta]^2$ - independent of squeezing

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

Ineffective post-processing

$$\beta \ll 1$$

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

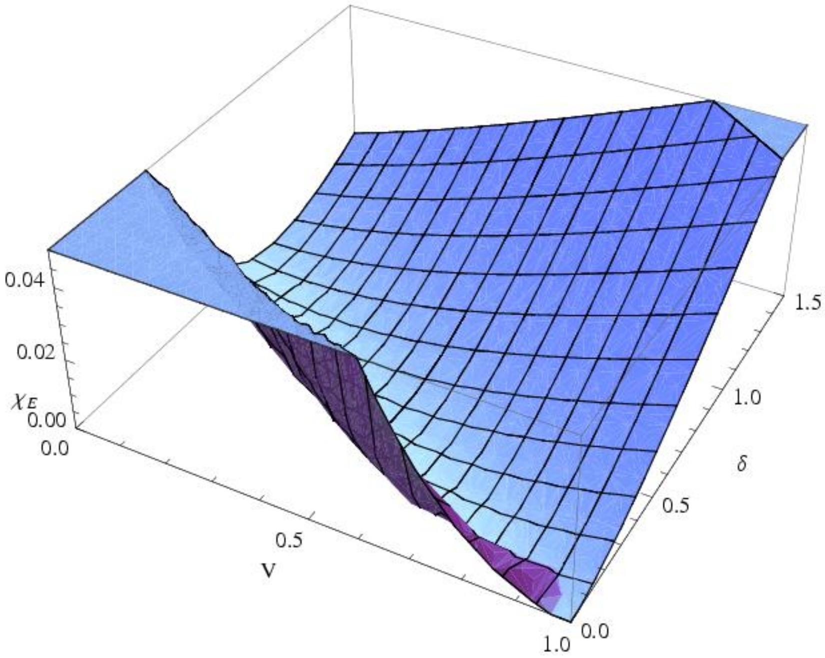


Upper bound on Eve's information (Holevo quantity)

Ineffective post-processing

$$\beta \ll 1$$

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



Holevo quantity turns to 0 upon pure channel loss when

$$V + \sigma = 1$$

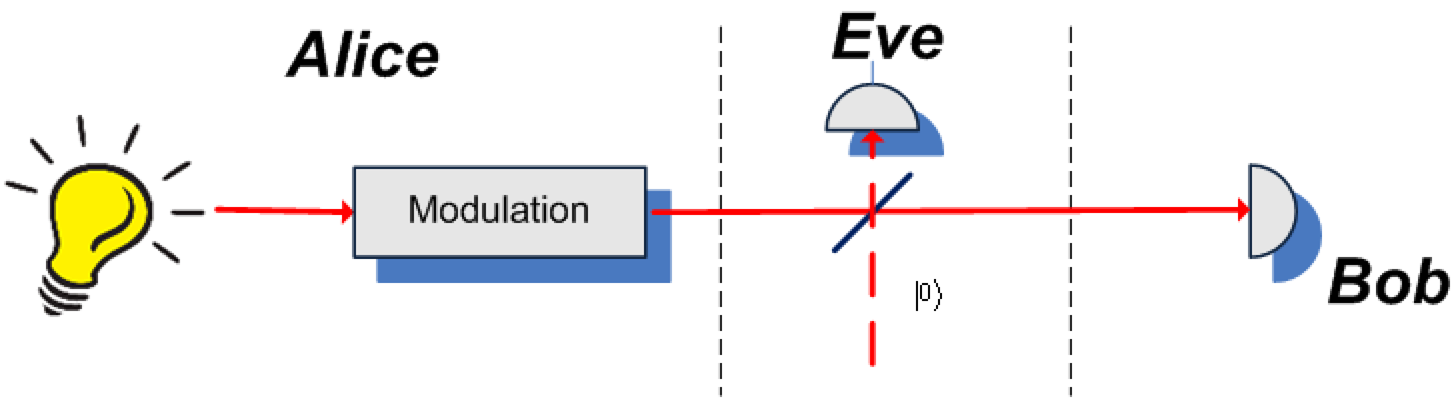
i.e. modulation must be

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

Canceling information leakage

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

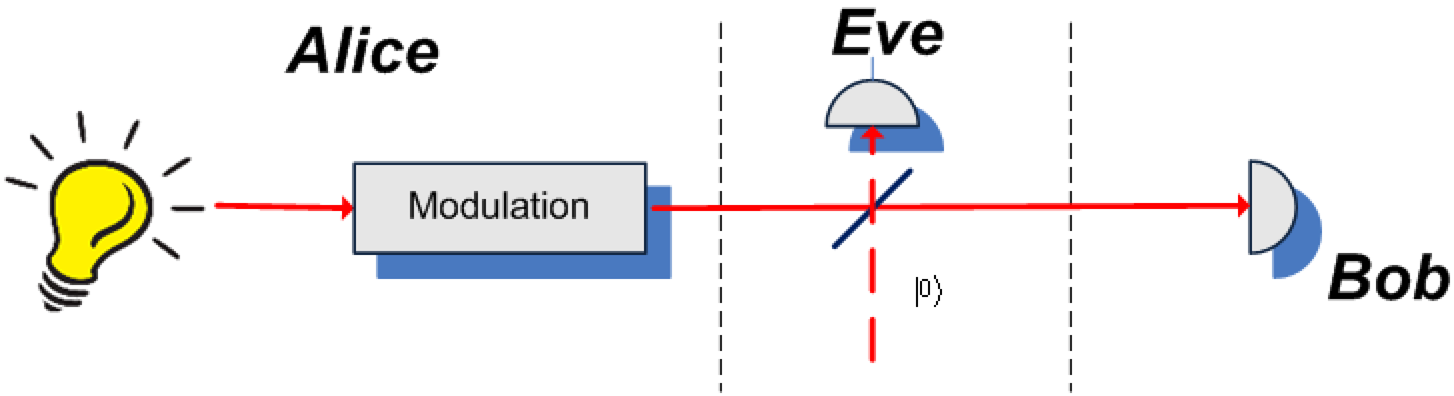
Pure channel loss:



Canceling information leakage

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

Pure channel loss:

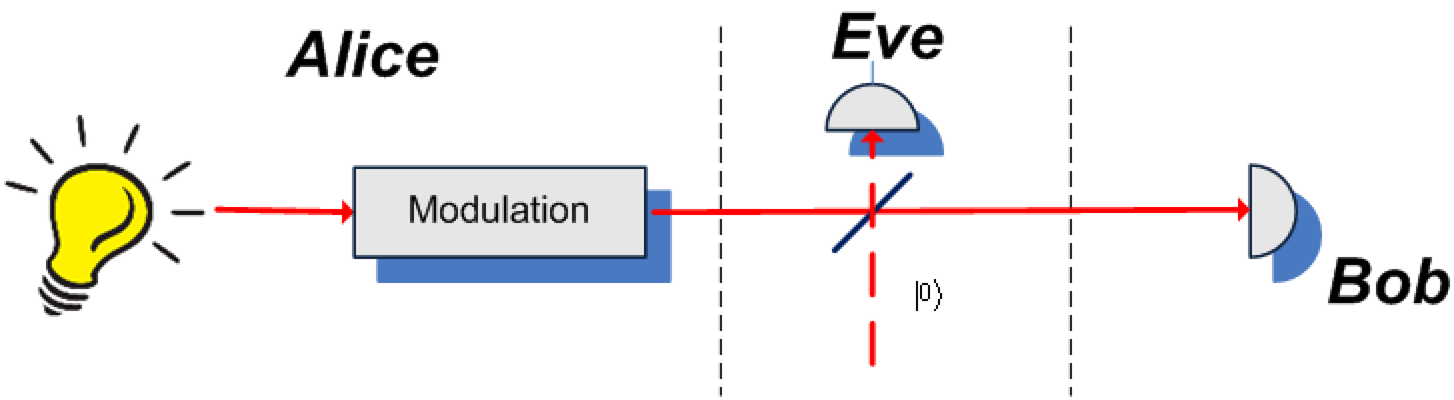


Correlation $C_{BE} \propto V_S - V_E = (V + \sigma) - 1 = 0$

Canceling information leakage

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

Pure channel loss:



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

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

Summary

• CV QKD is based on the solid Gaussian security proofs and is free from the single-photon assumptions of DV QKD;

• Optimal combination of resources improves CV QKD protocols;

• Nonclassical resource (squeezing) can partly substitute the classical (computational) resource;

• By properly adjusting modulation applied to squeezed states we can cancel or minimize the information leakage.

CV QKD: current challenges

- Side-channels (trusted-side leakage), decoupling of Eve;
- Fluctuating & non-Markovian environment
- Device independence;
- Finite-size effects, channel estimation.

Acknowledgements

Collaborators:

Radim Filip, Laszlo Ruppert, Ivan Derkach (UPOL, Olomouc);

Ulrik Andersen (DTU, Lyngby);

Christoph Marquardt, Bettina Heim, Christian Peuntinger (MPI, Erlangen)

Thank you for attention!

usenko@optics.upol.cz