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

QUANTUM STATES AND CLASSICAL COMPUTATION: JOINT QUEST FOR THE INFORMATION SECURITY

Vladyslav C. Usenko

Department of Optics, Palacký University,
Olomouc, Czech Republic

Masaryk University in Brno, 2011

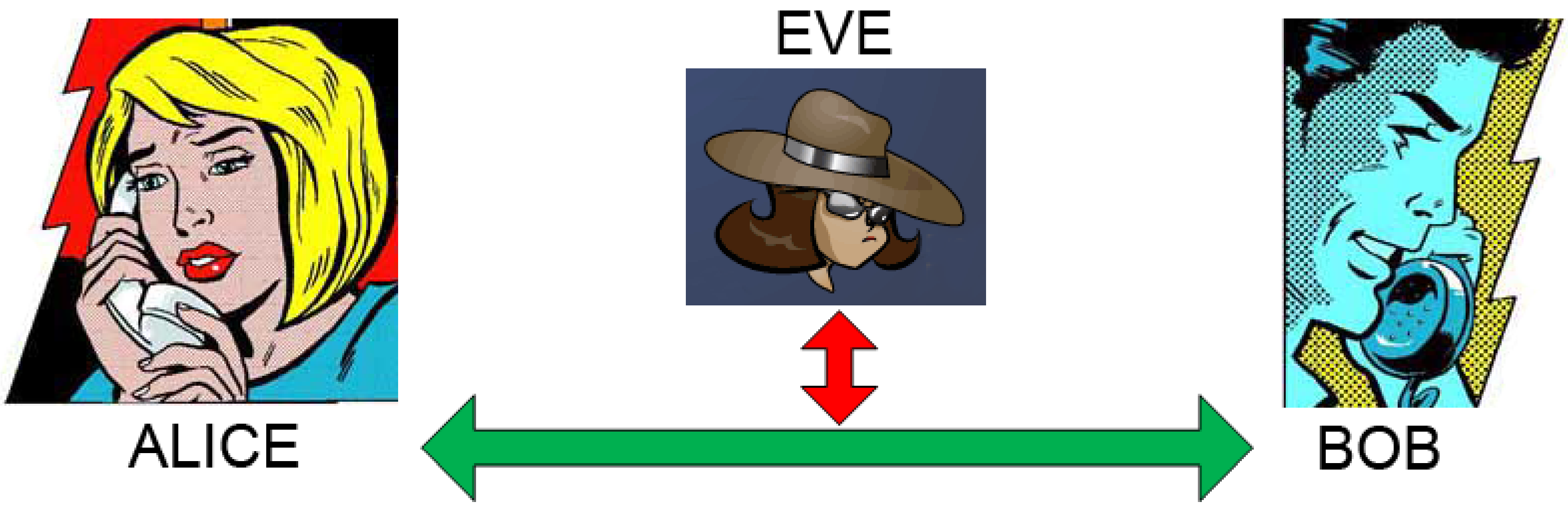
Outline

- Quantum vs classical cryptography, motivation
- Discrete-variable quantum key distribution
- Continuous-variable quantum key distribution
- Security analysis
- Resources: classical, quantum, computational
- Summary

Quantum cryptography

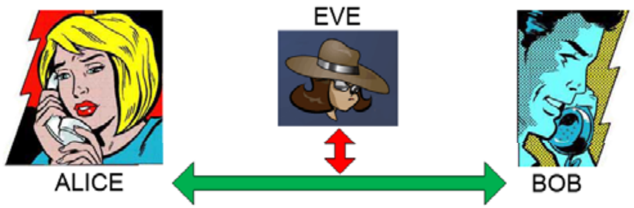
Practical motivation: necessity in secure communication between two trusted parties (**Alice** and **Bob**)

Quantum cryptography



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

Quantum cryptography

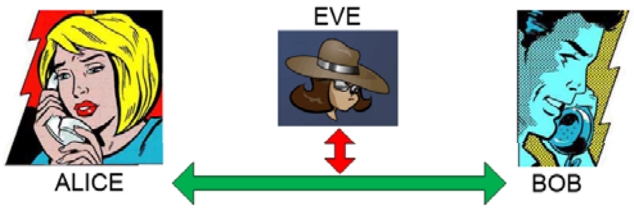


CLASSICAL CRYPTOGRAPHY

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

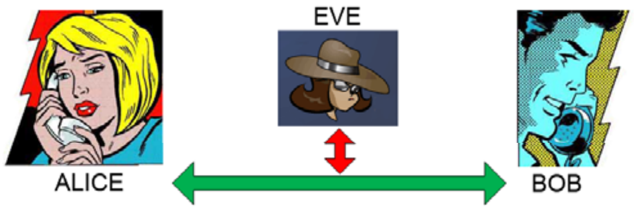
Asymmetrical schemes (RSA, DSA); symmetrical (DES, AES, RC4, MD5), mixed.

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: 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

- 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**:

QBER vs BER. Block codes etc. to correct the errors.
Simple example: XOR two bits, check the result, keep one or none.

- **Privacy amplification**:

Reduces the possible Eve's information on the key.
Simple example: replace two bits with their XOR. Probability for Eve to know the result is reduced.
E.g.: Eve knows bits with 60% probability, then she knows XOR with

$$0.6^2 + 0.4^2 = 52\%.$$

[Ch.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, 1995, "Generalized privacy amplification", IEEE Trans. Information th., 41, 1915-1923.]

Quantum key distribution: BB84

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

Information-theoretical analysis

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

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

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

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:

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

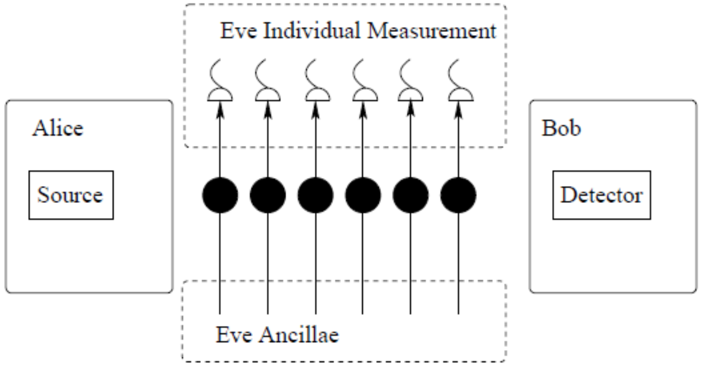
i.e. Alice (or Bob) needs to have more information than Eve!

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

Quantum key distribution: security

Individual attacks. Key rate:

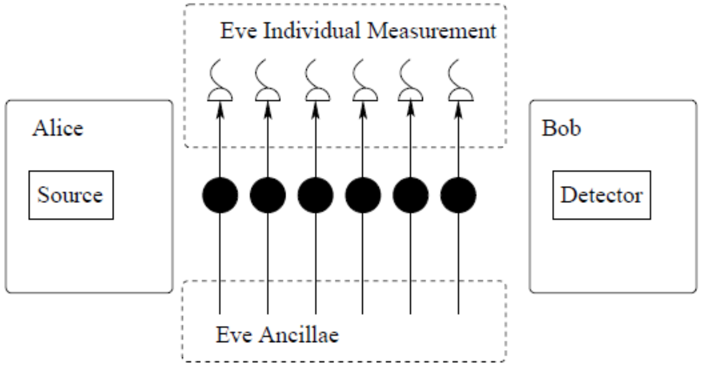
$$I_i = I_{AB} - I_{BE}$$



Quantum key distribution: security

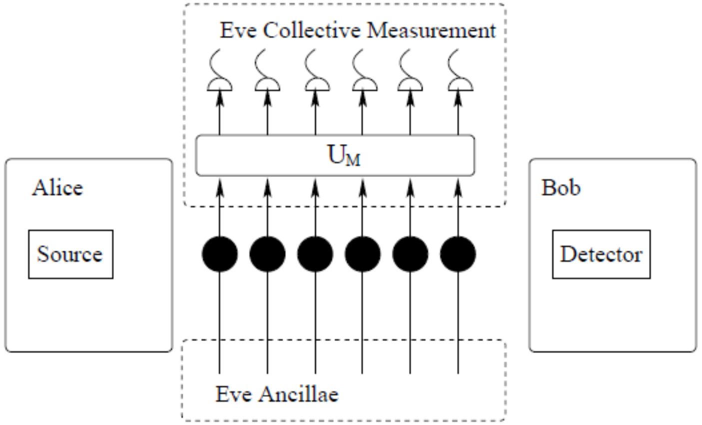
Individual attacks. Key rate:

$$I_i = I_{AB} - I_{BE}$$



Collective attacks:

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



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

$$\chi = S(\bar{\rho}) - \sum_{i=0}^{1} p_i S(\rho_i), \quad \bar{\rho} = \sum_{i=0}^{1} p_i \rho_i, \quad S(\rho) = -Tr\, \rho \log \rho$$

R. Renner,N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005)
R. Garcia-Patron, Ph.D. Thesis, Université Libre de Bruxelles (2007)

Error correction efficiency

Key rate upon imperfect error correction:

$$I = \int_0^{\infty} d\beta_x p_c(\beta_x)[1 - f(e)\mathrm{H}^{\mathrm{bin}}(e) - \chi(\beta_x)]$$

where

$$H^{\mathrm{bin}}(\mathrm{e}) = -\, e \log_2(e) - (1-e)\log_2(1-e).$$

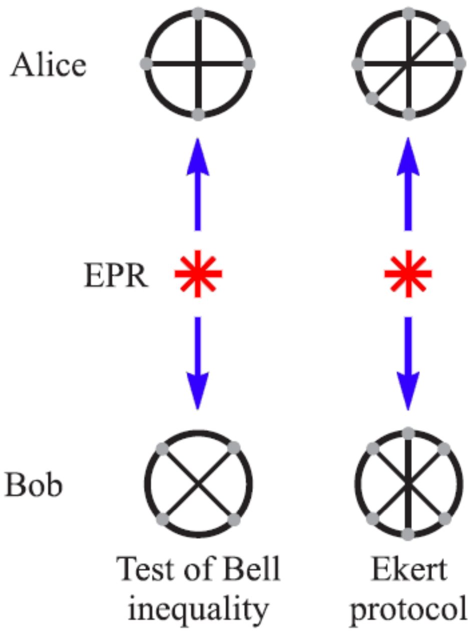
efficiency of CASCADE:

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.32

M. Heid and N. Lütkenhaus, Phys. Rev. A 73, 052316 (2006)

Quantum key distribution: E91

Instead of the preparation-and-measurement, Alice and Bob have entangled source in the middle:

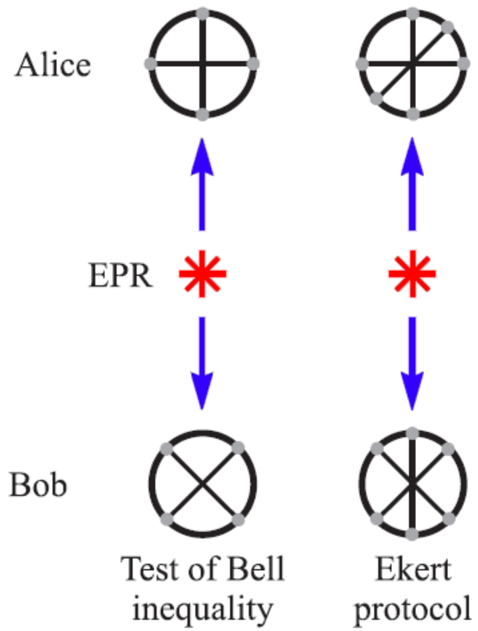


- Alice and Bob measure a particle each
- Key is generated in the process of measurement!
- Next stages – same as in BB84
  (key sifting, error correction, privacy amplification)

[A.K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991)]

Quantum key distribution: E91

Instead of the preparation-and-measurement, Alice and Bob have entangled source in the middle:

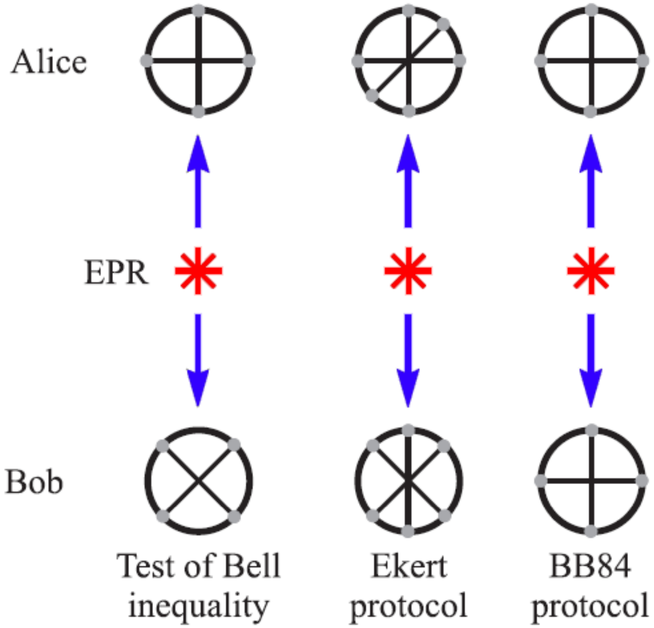


Security is based on Bell inequalities violation check (whether the state remains nonclassical)

[A.K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991)]

Quantum key distribution: E91

Instead of the preparation-and-measurement, Alice and Bob have entangled source in the middle:



Can be used for BB84 protocol.

The EPR-based and prepare-and-measure schemes are equivalent.

[A.K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991)]

Quantum key distribution: state-of-art

Commercial realizations:

MagiQ

id Quantique

~100 km, ~1 kbps

Problem: absence of single-photon sources, high detectors “dark count” rates

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

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

Fock states: $|n_k\rangle$ 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: $$H = \sum_k \hbar\omega_k (a_k^\dagger a_k + \tfrac{1}{2})$$

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

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

<u>Coherent states</u> - 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:

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

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

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

<u>Phase-space representation.</u>

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

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. $W(\xi) = \frac{1}{(2\pi)^N} \int d^{2N}\zeta e^{i\xi^T \Omega\zeta} \chi_\rho(\zeta)$

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: $\gamma + i\Omega \geq 0$

$$\Omega = \bigoplus_{i=1}^{N} \left[\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right]$$ - symplectic form

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

Continuous-variable states

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

$$\Delta x < 1$$

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

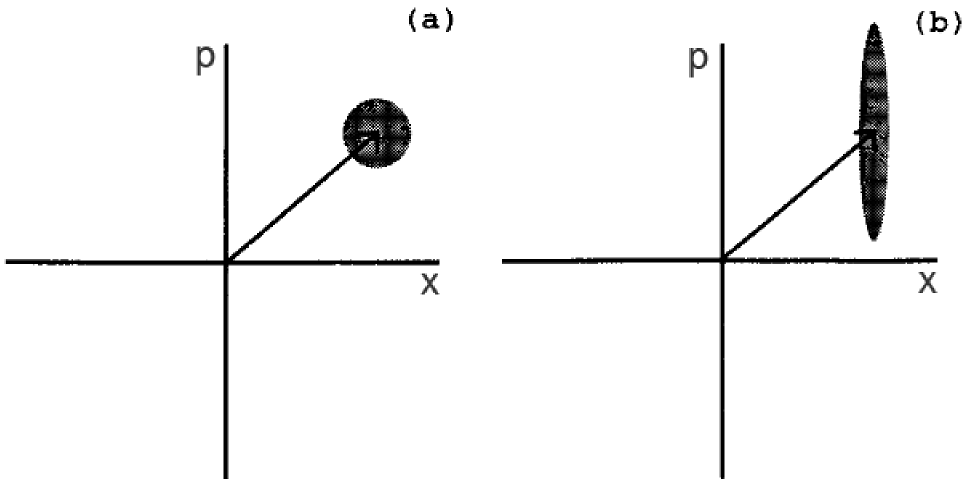
Continuous-variable states

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

$$\Delta x < 1$$

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

on the phase space:



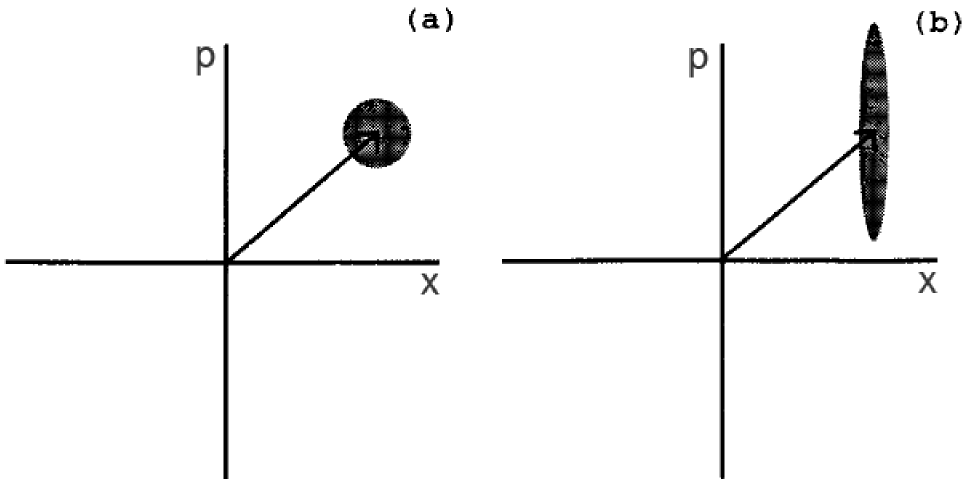
Continuous-variable states

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

$$\Delta x < 1$$

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

on the phase space:

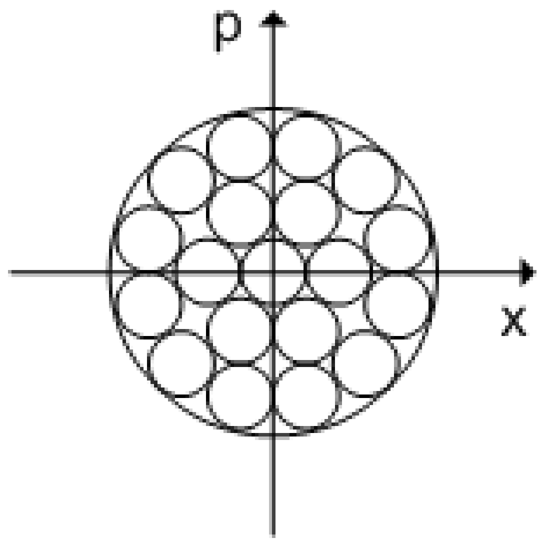


Achievements: **-10 dB** (*Vahlbruch et. al., PRL 100, 033602, 2008*)

CV Quantum Key Distribution

Coherent states protocol: laser beam quadrature modulation, homodyne detection (*F.Grosshans, P. Grangier, Phys Rev Lett, 88, 057092 (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, obtaining **a** or **b**
- Bases reconciliation
- Error correction, privacy amplification

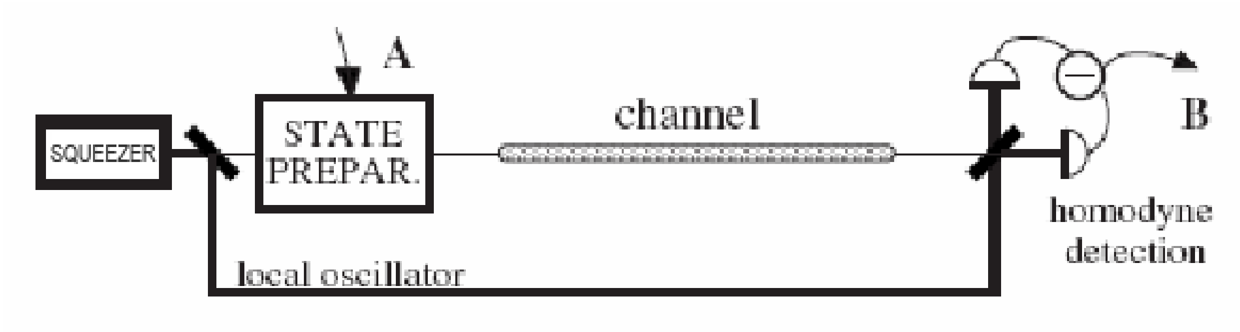


Achievements: 25 km, 2 kbps

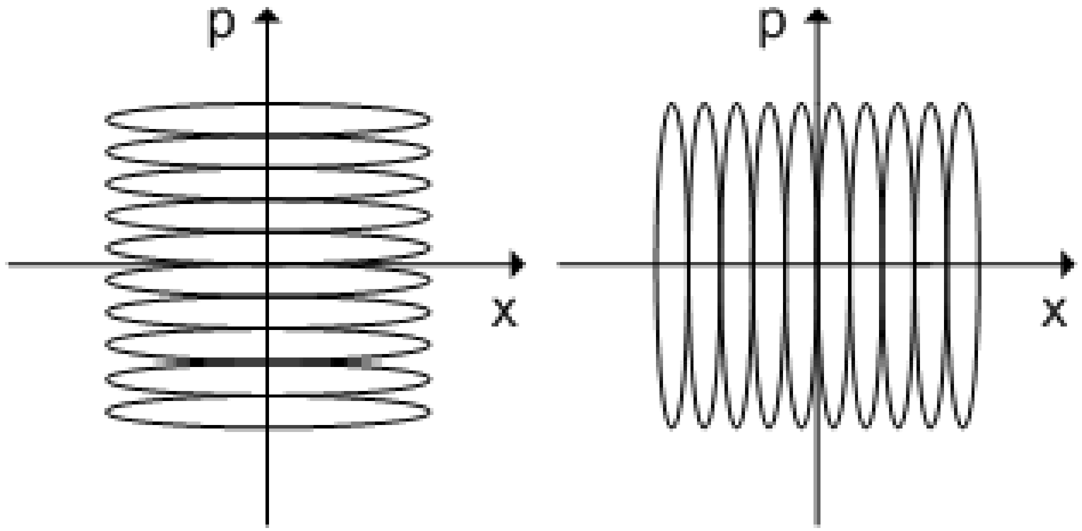
J. Lodewyck et al., PRA 76, 042305 (2007)

CV Quantum Key Distribution

Squeezed-states protocol: squeezed states quadrature modulation, homodyne detection (*N. J. Cerf, M. Levy, and G. Van Assche, Phys Rev A 63, 052311 (2001)*)

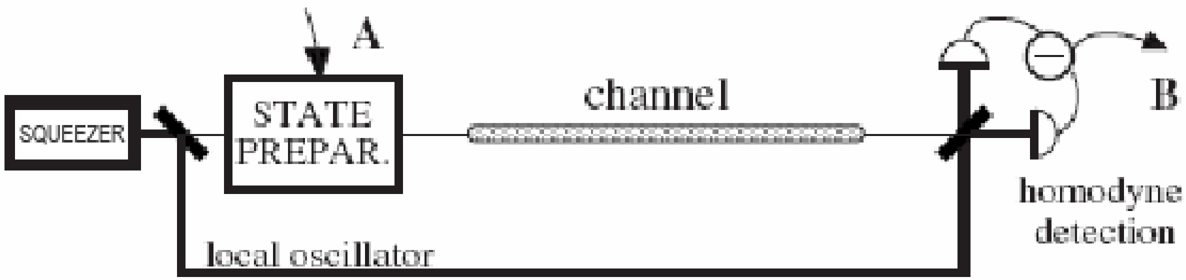


•Alice generates a Gaussian random variable **a**
•Alice prepares a squeezed state, displaced by **a** in squeezed direction
•Bob measures a quadrature
•Bases reconciliation
•Error correction, privacy amplification



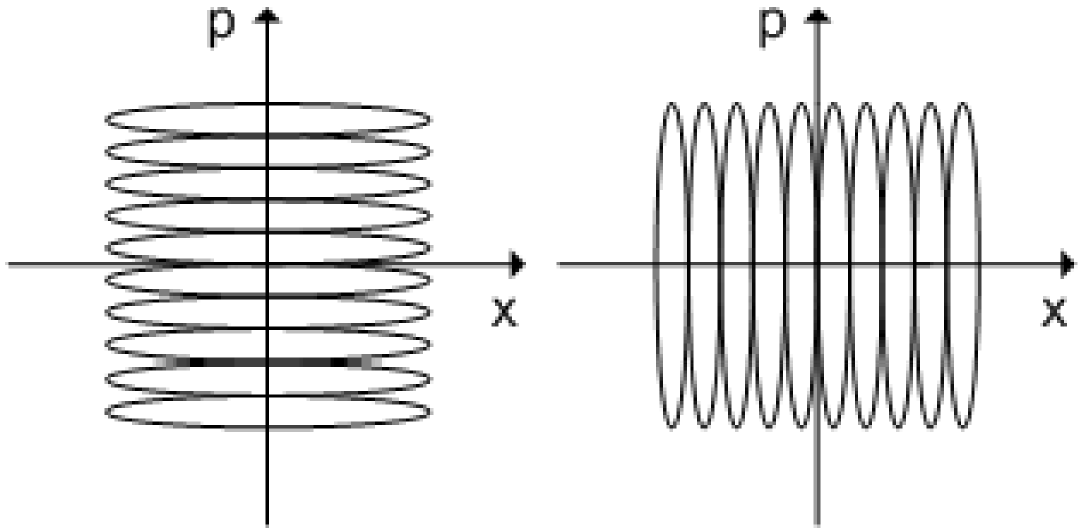
CV Quantum Key Distribution

Squeezed-states protocol: squeezed states quadrature modulation, homodyne detection (*N. J. Cerf, M. Levy, and G. Van Assche, Phys Rev A 63, 052311 (2001)*)

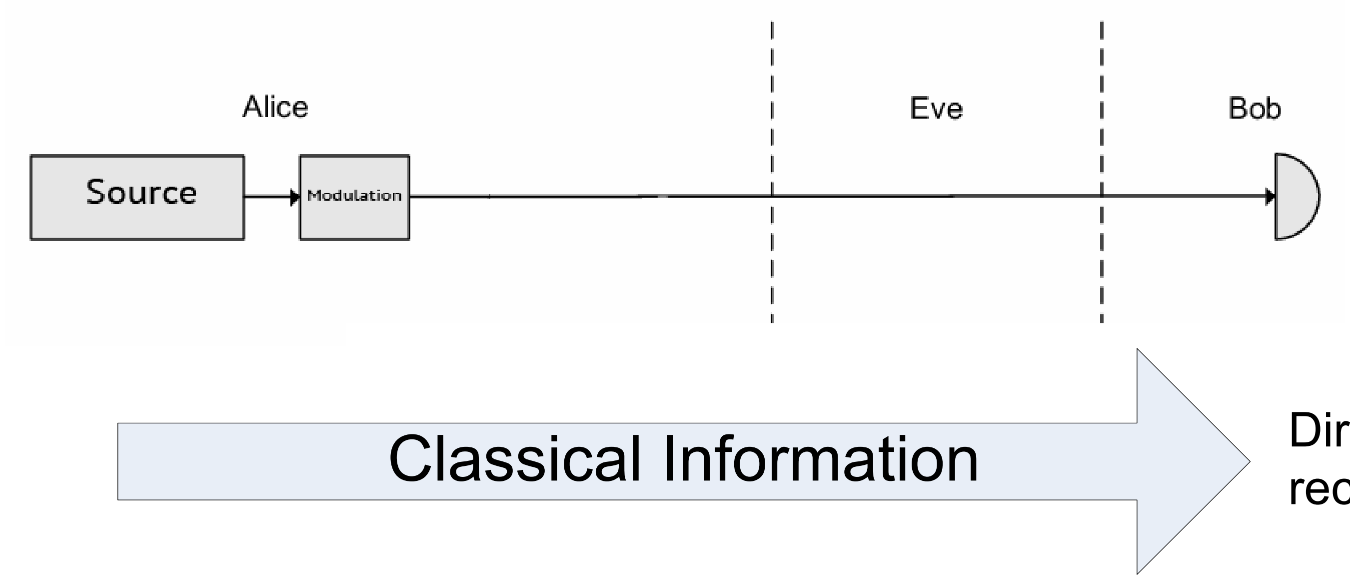


Was not practically implemented,

investigated mainly for high squeezing

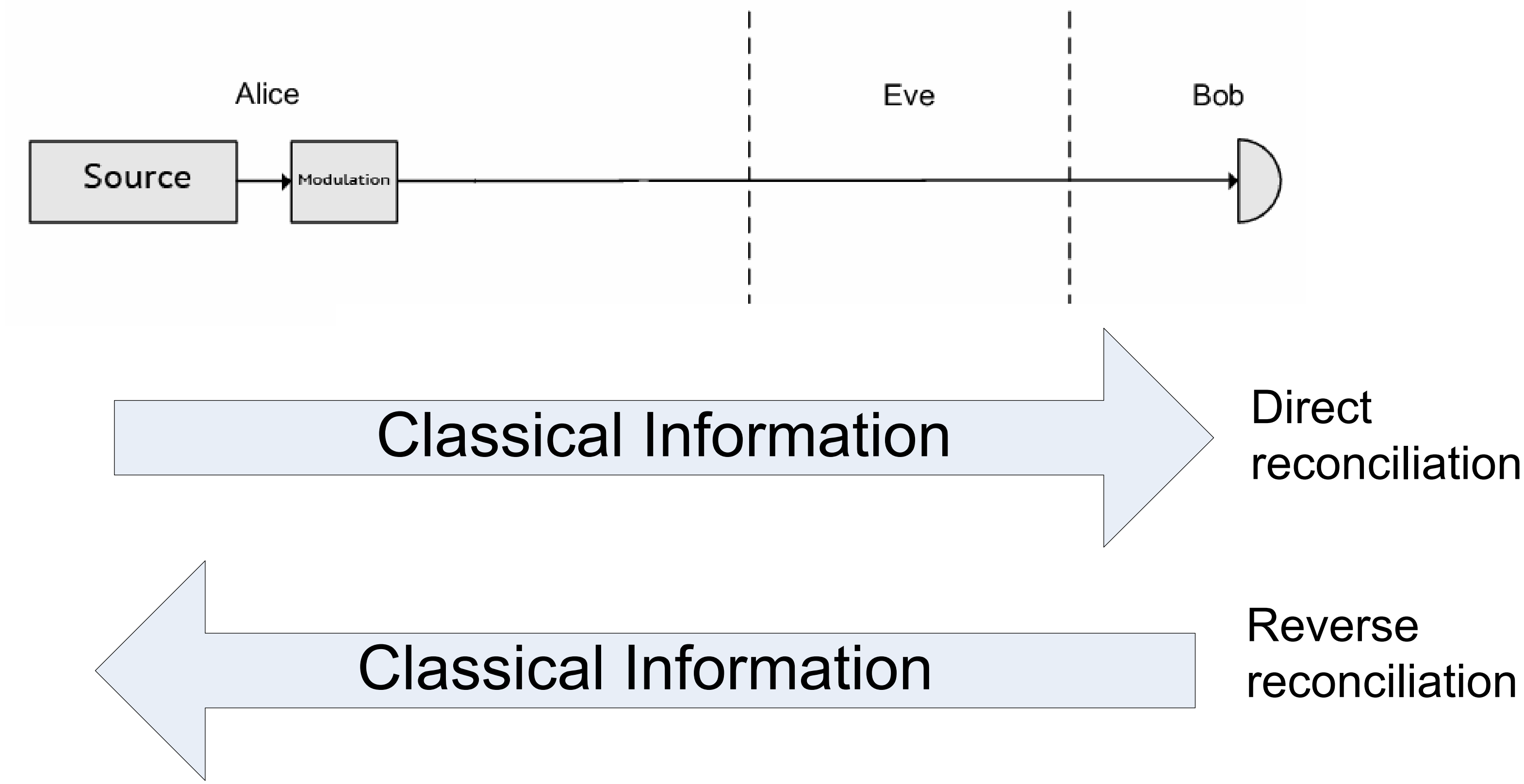


CV Quantum Key Distribution



Direct reconciliation

CV Quantum Key Distribution



CV Quantum Key Distribution

Is unsecure for > 50% channel loss

Classical Information →

Direct reconciliation

Tolerates any pure loss

← Classical Information

Reverse reconciliation

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 $f(\rho_{A_{1\ldots N}B_{1\ldots N}}) \leq f(\rho_{A_1 B_1}) + \ldots + f(\rho_{A_N B_N})$

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:

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

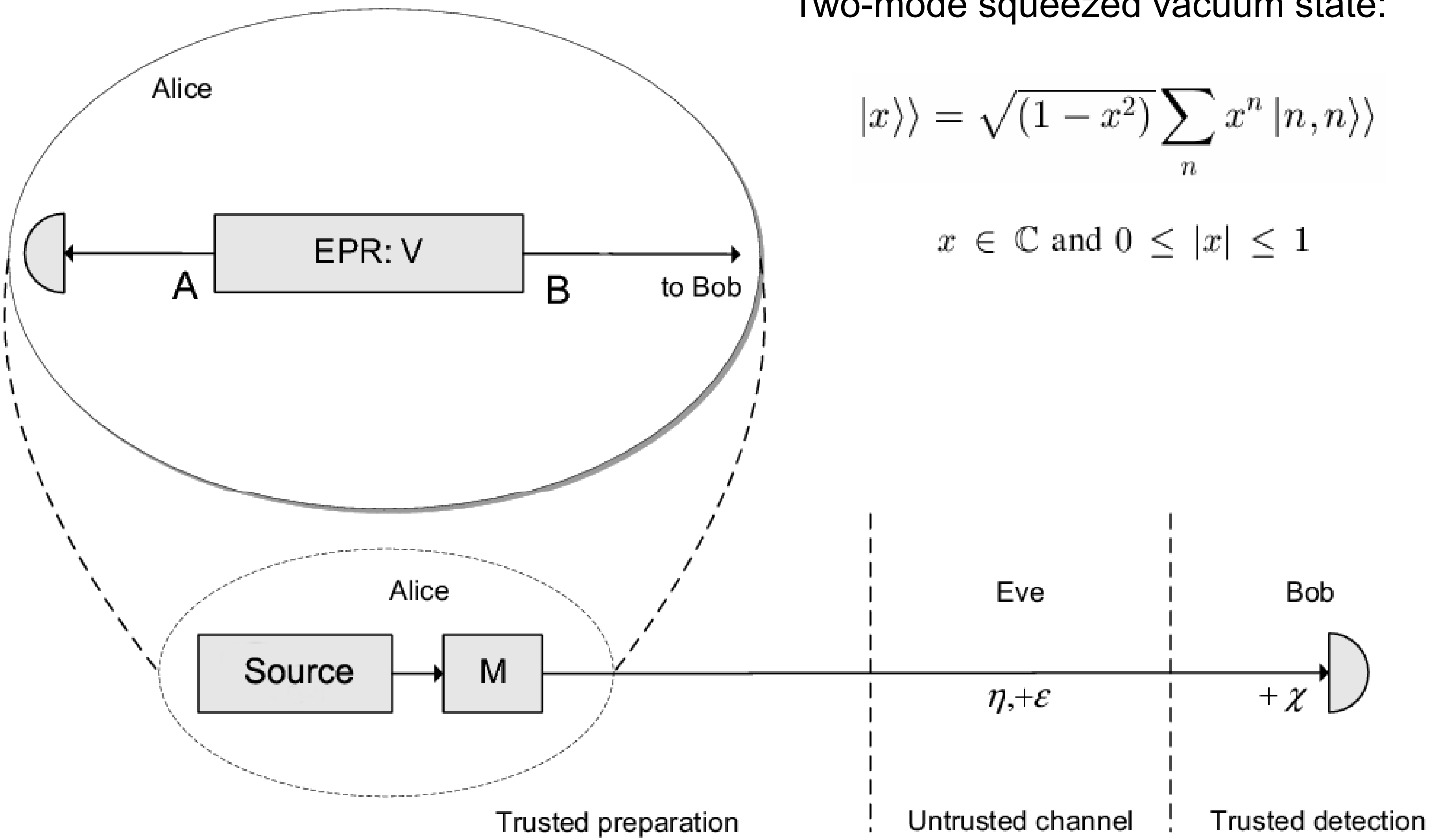
$$\gamma_A^{x_B} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T \qquad X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Framework: EPR-based set-up

Two-mode squeezed vacuum state:

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

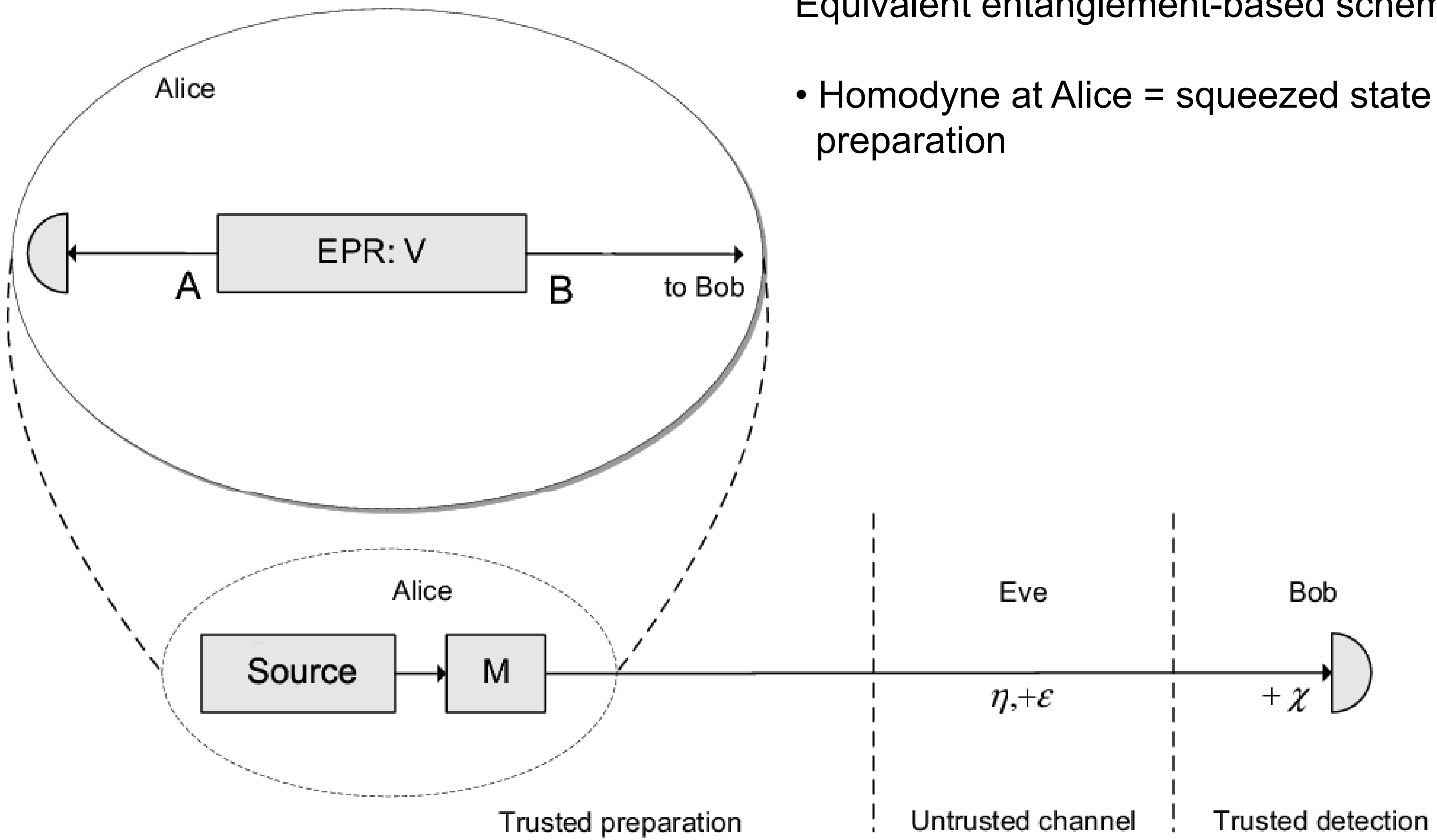
$$x \in \mathbb{C} \text{ and } 0 \leq |x| \leq 1$$



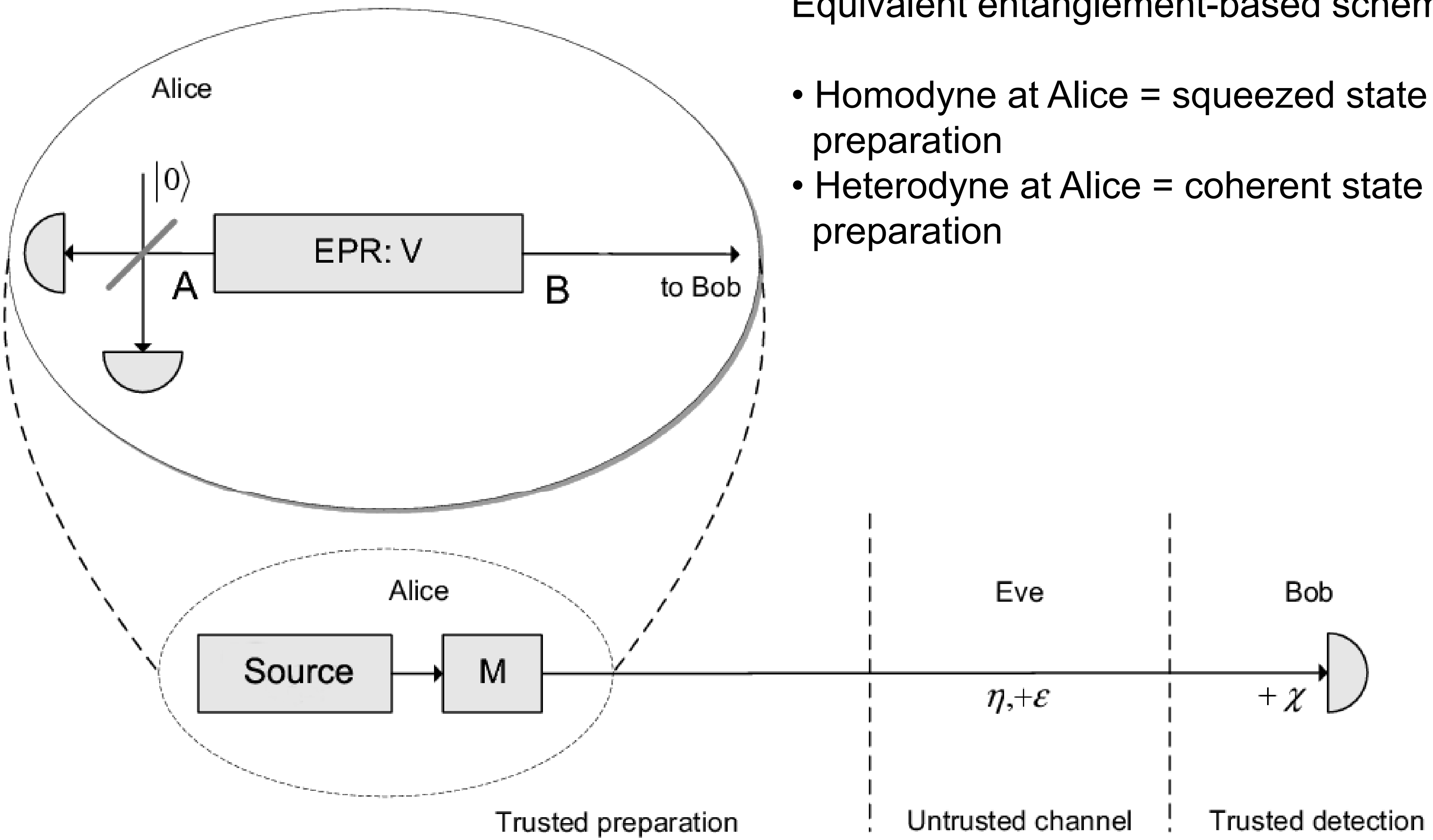
Framework: EPR-based set-up

Equivalent entanglement-based scheme:

- Homodyne at Alice = squeezed state preparation



Framework: EPR-based set-up



Equivalent entanglement-based scheme:

- Homodyne at Alice = squeezed state preparation
- Heterodyne at Alice = coherent state preparation

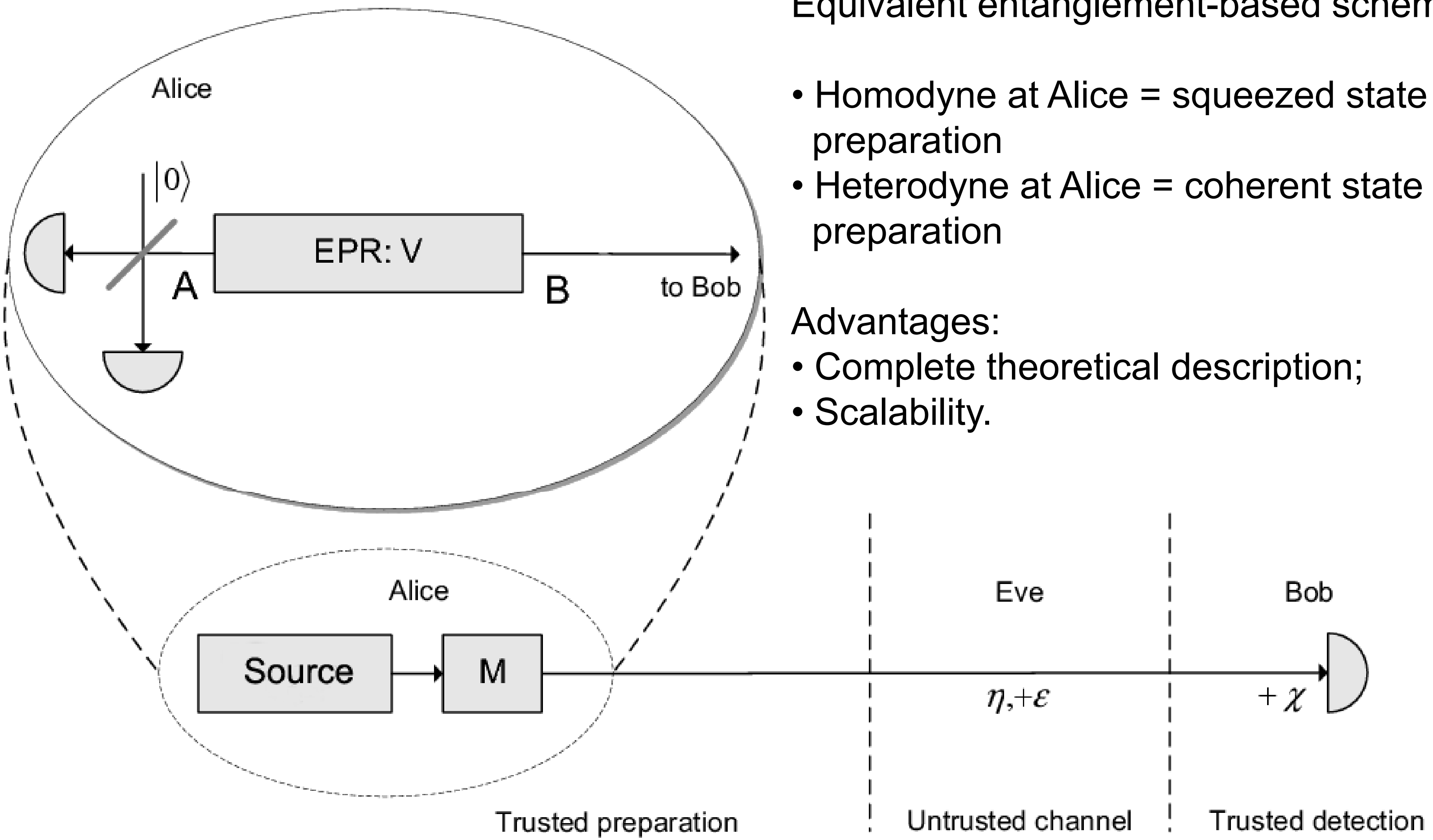
Framework: EPR-based set-up

Equivalent entanglement-based scheme:

- Homodyne at Alice = squeezed state preparation
- Heterodyne at Alice = coherent state preparation

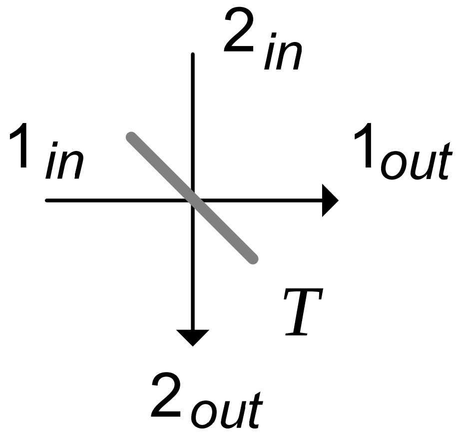
Advantages:

- Complete theoretical description;
- Scalability.



Framework: covariance matrices

Transformation on a beam splitter:



$$\begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \end{bmatrix}_{out} = \begin{bmatrix} \cos\gamma & \sin\gamma \\ -\sin\gamma & \cos\gamma \end{bmatrix} \begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \end{bmatrix}_{in}$$

$\sqrt{T} = \cos\gamma$ - transmittance; $\sin\gamma = \sqrt{1-T}$. - reflectance

$$\begin{bmatrix} \hat{r}_1 \\ \hat{r}_2 \end{bmatrix}_{out} = \begin{bmatrix} \cos\gamma\mathbb{I} & \sin\gamma\mathbb{I} \\ -\sin\gamma\mathbb{I} & \cos\gamma\mathbb{I} \end{bmatrix} \begin{bmatrix} \hat{r}_1 \\ \hat{r}_2 \end{bmatrix}_{in}$$

Framework: covariance matrices

EPR-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 attenuation and lossy channel:

$$\gamma_{ABC} = \begin{pmatrix} V\mathbb{I} & \sqrt{\eta T}\sqrt{V^2-1}\sigma_z & \sqrt{1-T}\sqrt{V^2-1}(-\sigma_z) \\ \sqrt{\eta T}\sqrt{V^2-1}\sigma_z & [\eta(TV+1-T)+(1-\eta)]\mathbb{I} & \sqrt{\eta T(1-T)}(1-V)\mathbb{I} \\ \sqrt{1-T}\sqrt{V^2-1}(-\sigma_z) & \sqrt{\eta T(1-T)}(1-V)\mathbb{I} & [(1-T)V+T]\mathbb{I} \end{pmatrix}$$

Framework: covariance matrices

EPR-source covariance matrix:

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

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

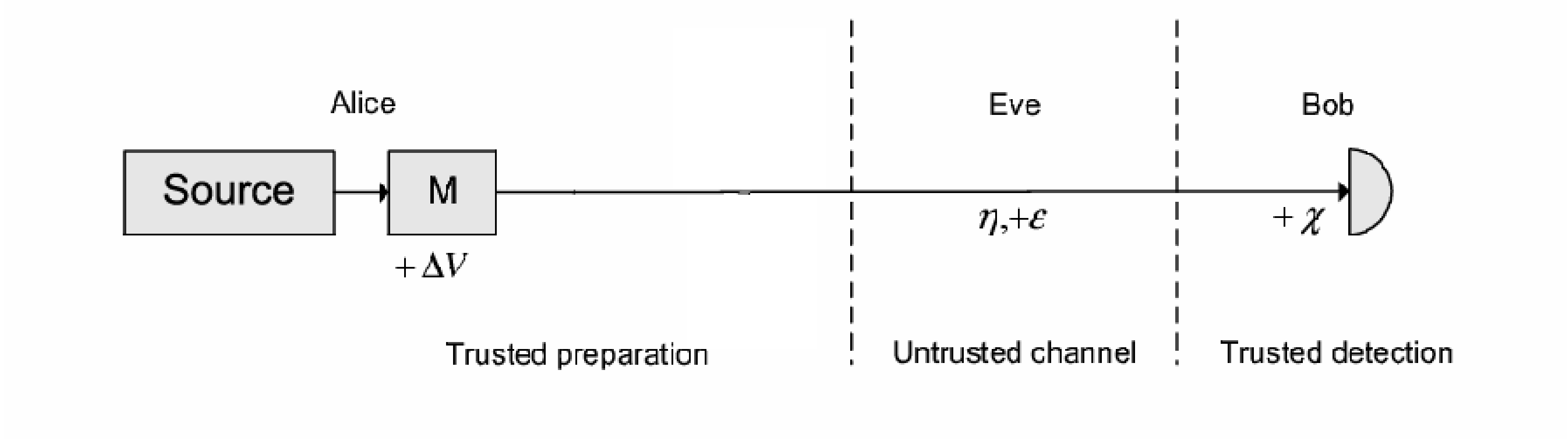
After attenuation and lossy channel:

$$\gamma_{ABC} = \begin{pmatrix} V\mathbb{I} & \sqrt{\eta T}\sqrt{V^2-1}\sigma_z & \sqrt{1-T}\sqrt{V^2-1}(-\sigma_z) \\ \sqrt{\eta T}\sqrt{V^2-1}\sigma_z & [\eta(TV+1-T)+(1-\eta)]\mathbb{I} & \sqrt{\eta T(1-T)}(1-V)\mathbb{I} \\ \sqrt{1-T}\sqrt{V^2-1}(-\sigma_z) & \sqrt{\eta T(1-T)}(1-V)\mathbb{I} & [(1-T)V+T]\mathbb{I} \end{pmatrix}$$

More modes – larger matrix. For 4-5 modes – generally analytically unsolvable

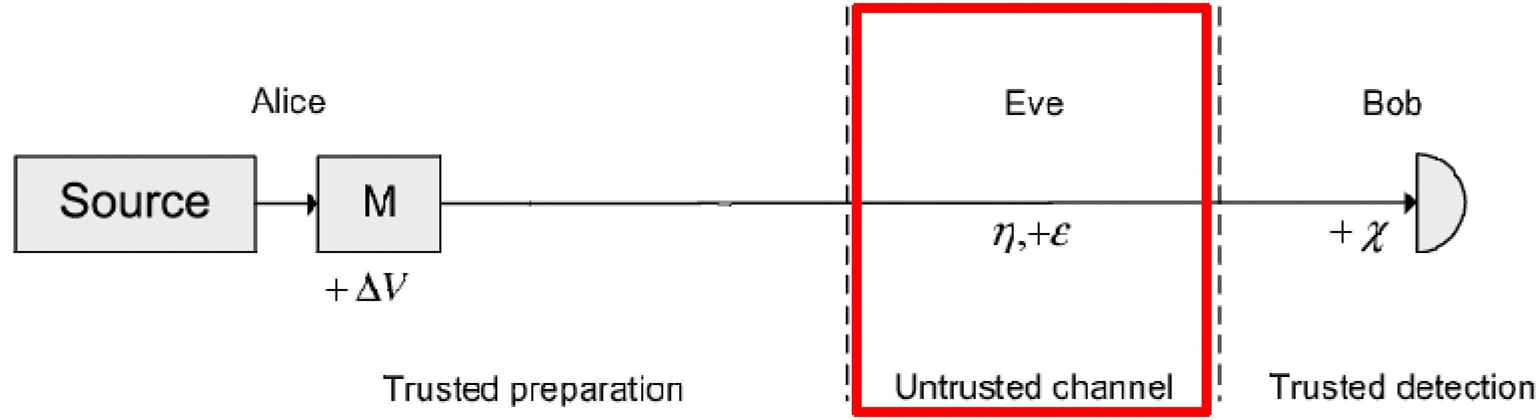
Influence of noise

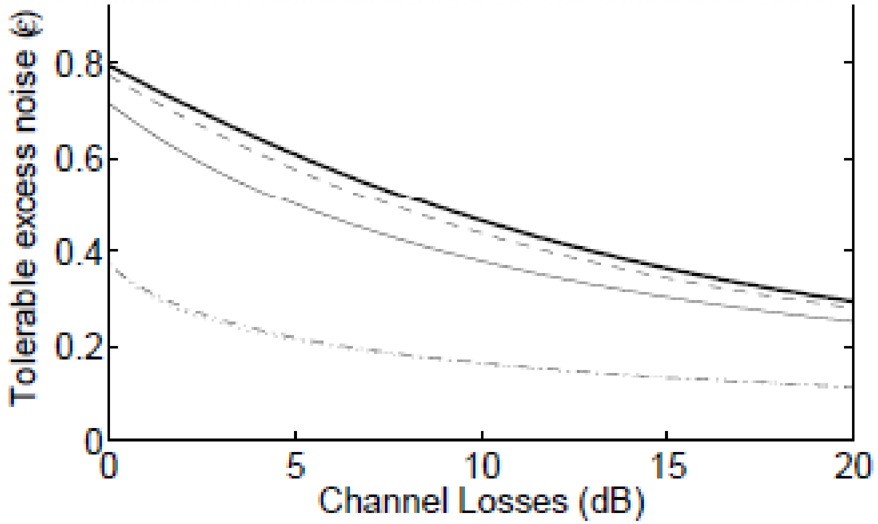
Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



Influence of noise

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



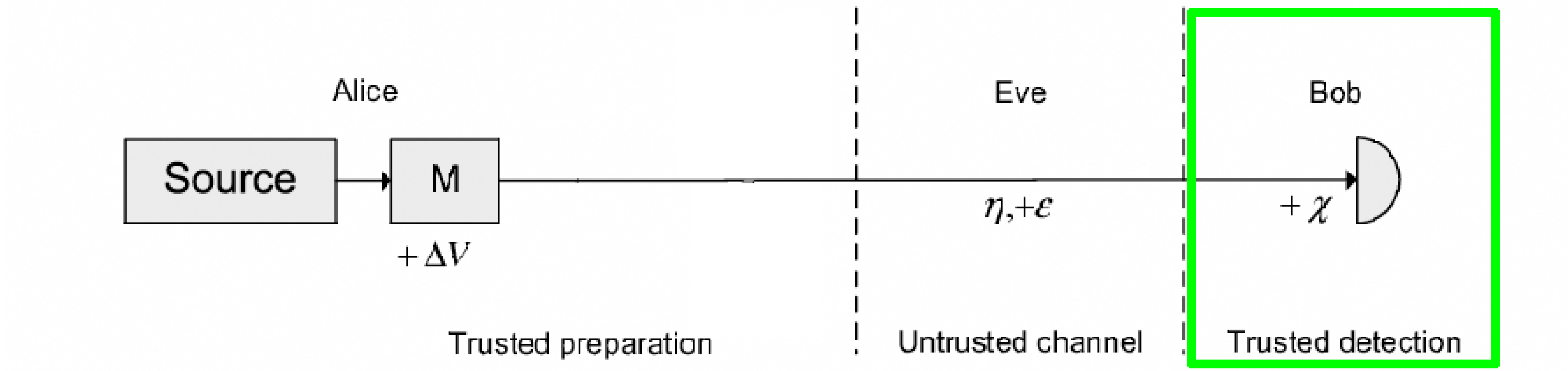


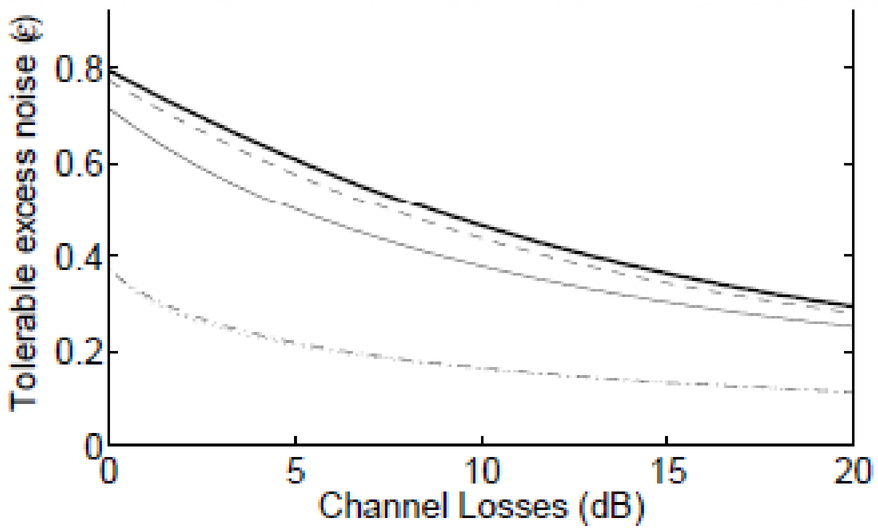
Untrusted noise limits security.

◀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)





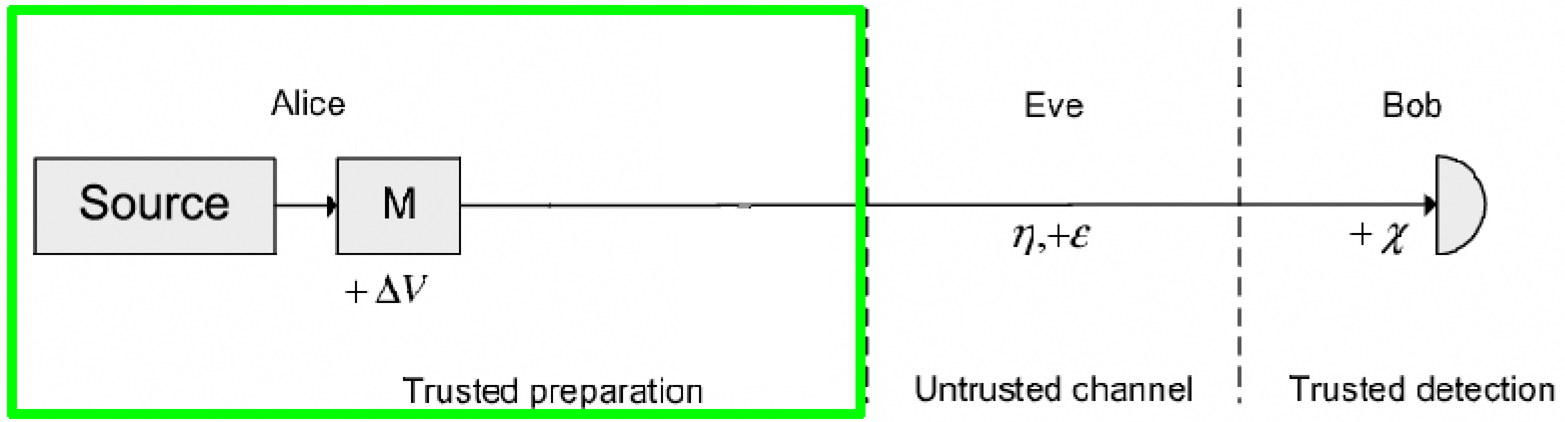
Trusted detection noise improves (!) security.

◀Typical dependence of maximum tolerable channel excess noise versus loss

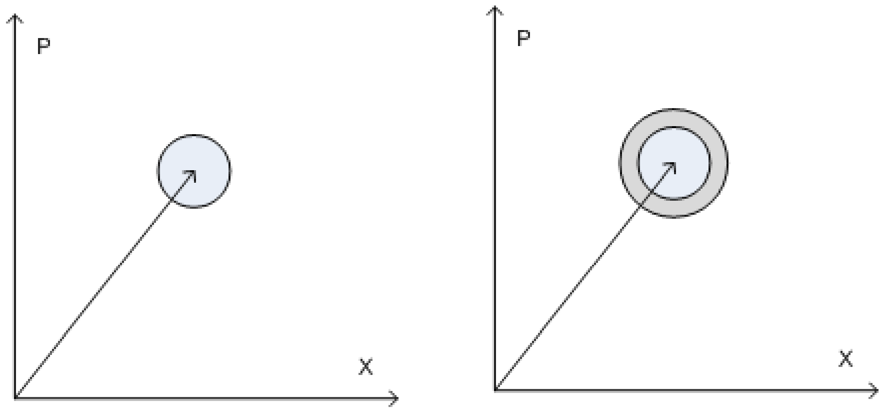
R. Garcia-Patron, N. Cerf, PRL 102 120501 (2009)

Influence of noise

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

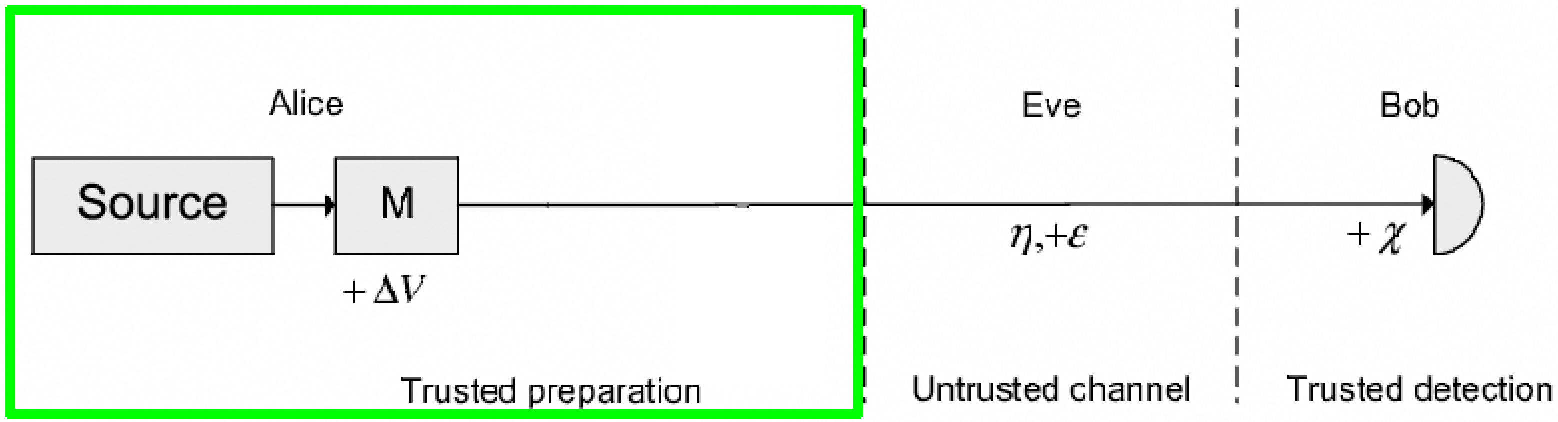


Trusted preparation noise. Coherent states: phase-insensitive excess noise



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

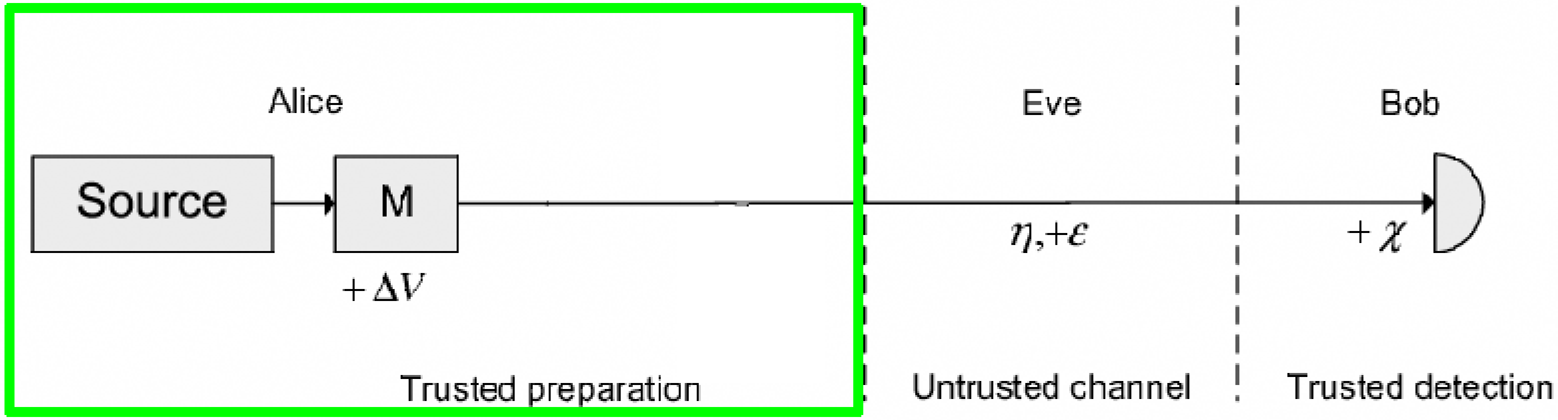
Is security breaking:

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

η - channel transmittance

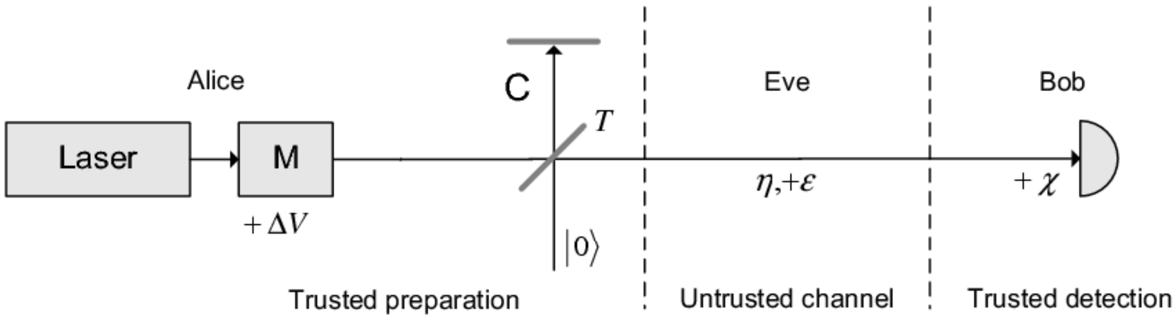
Influence of noise

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



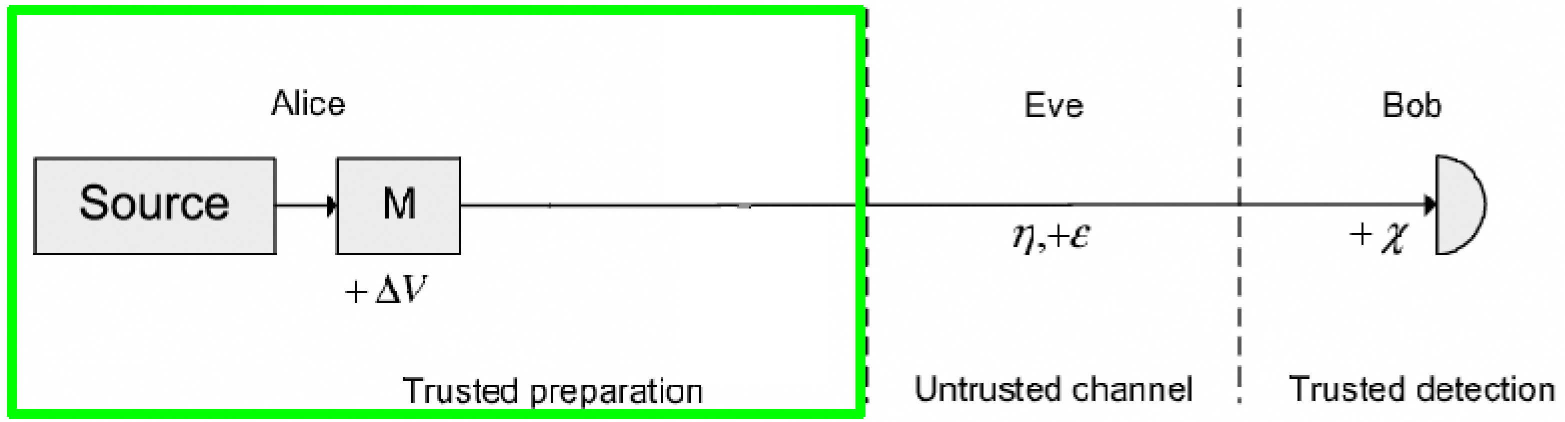
Trusted preparation noise. Coherent states: phase-insensitive excess noise

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

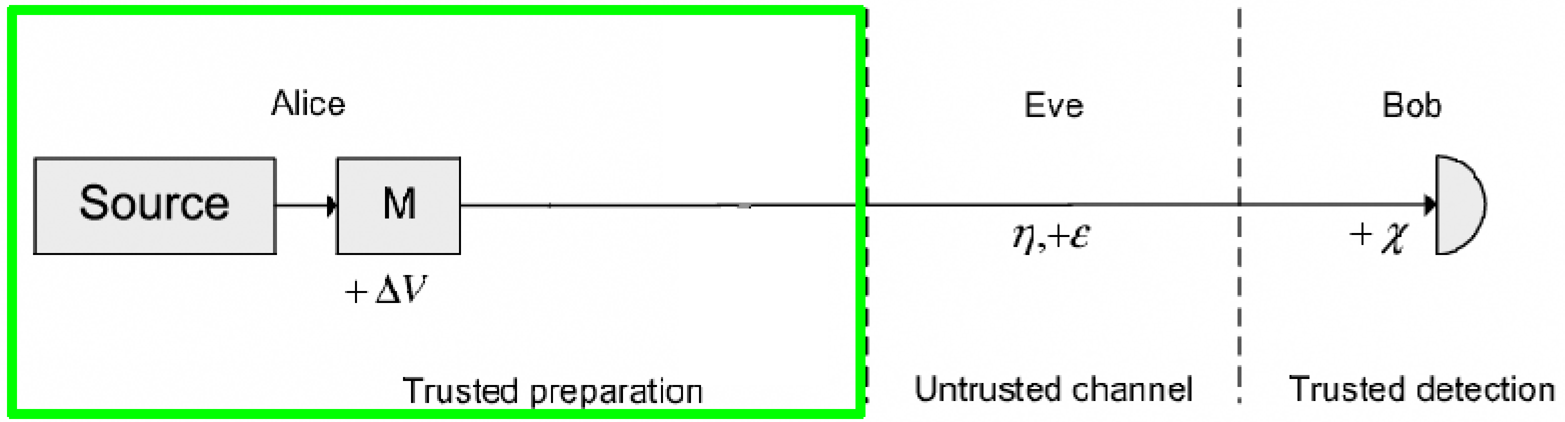
Purification restores security:

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

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

Influence of noise

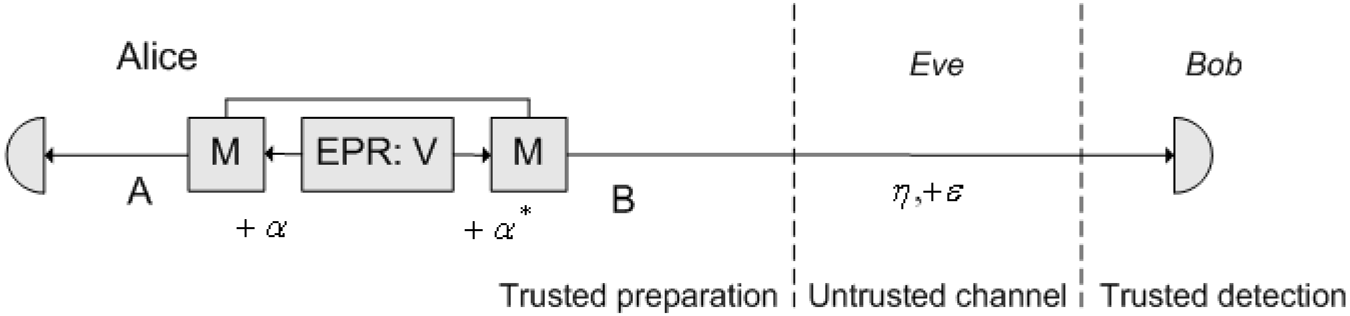
Distinguishing the noise types: **trusted** (preparation ΔV and detection χ noise) and **untrusted** (channel noise ε)



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

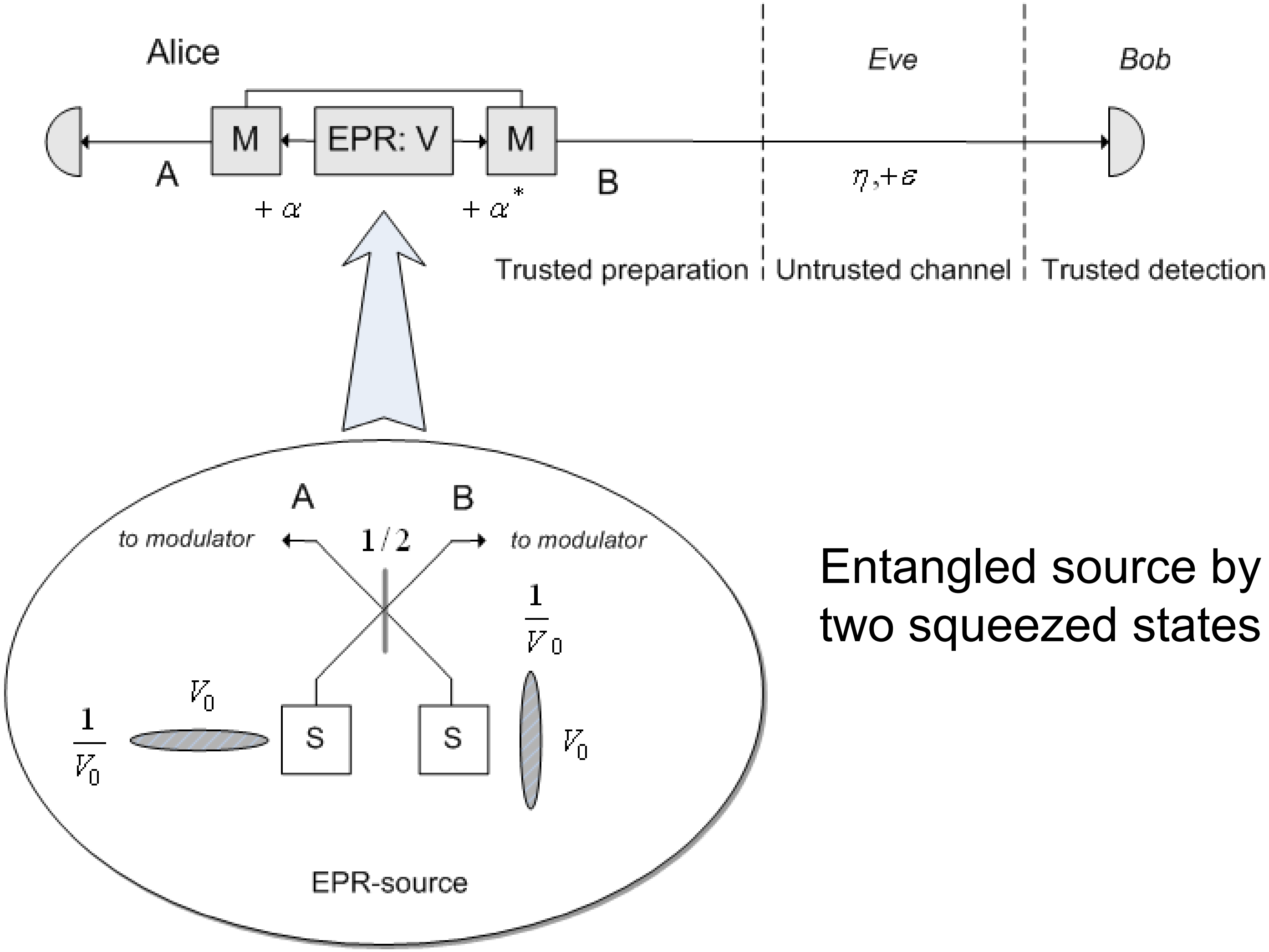
What if noise is correlated?

Additional classical correlations



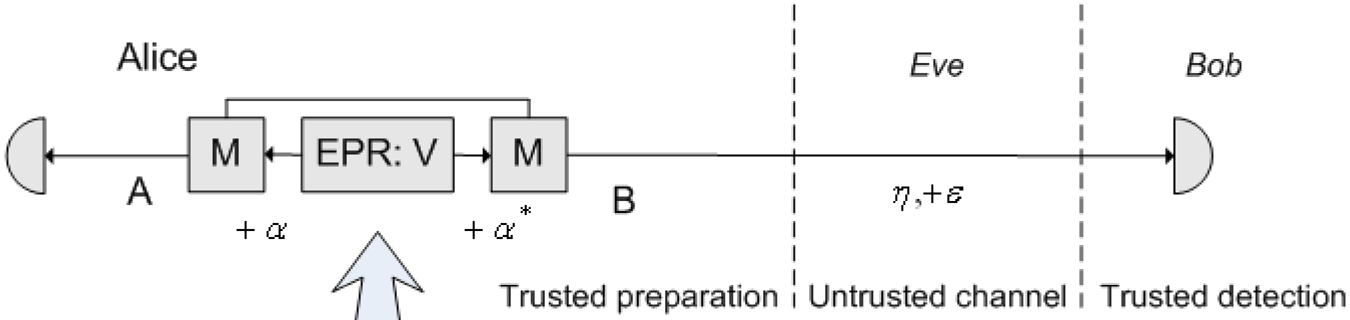
Turning noise to correlations: additional modulator

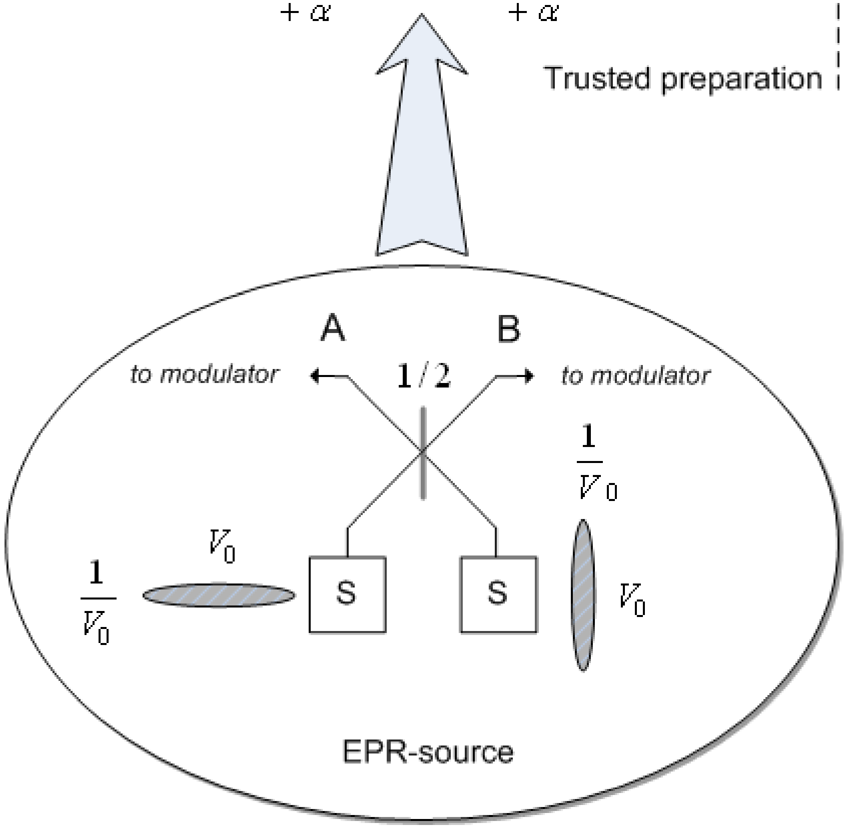
Additional classical correlations

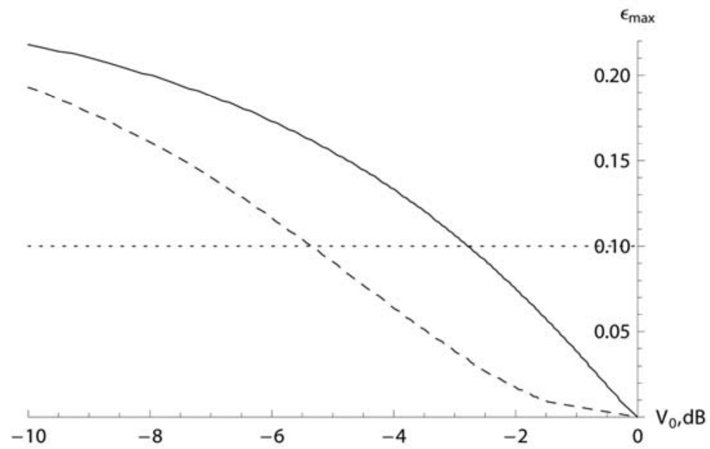


Entangled source by coupling of two squeezed states

Additional classical correlations

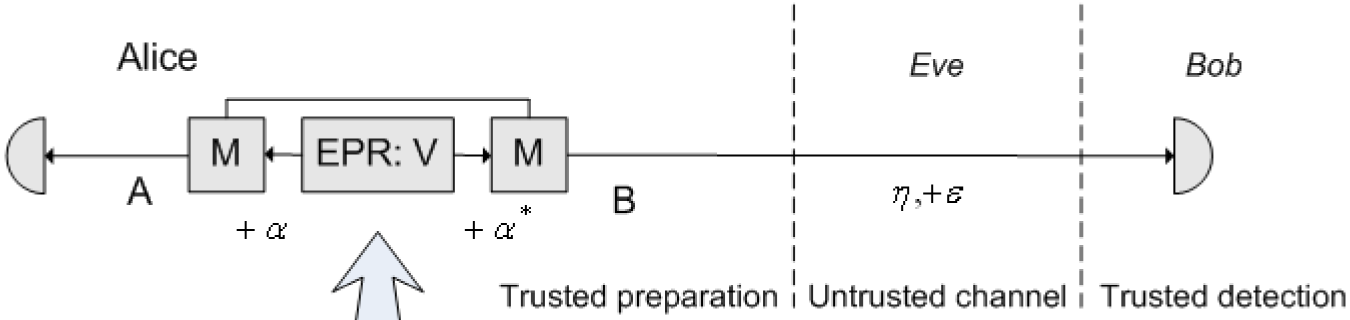


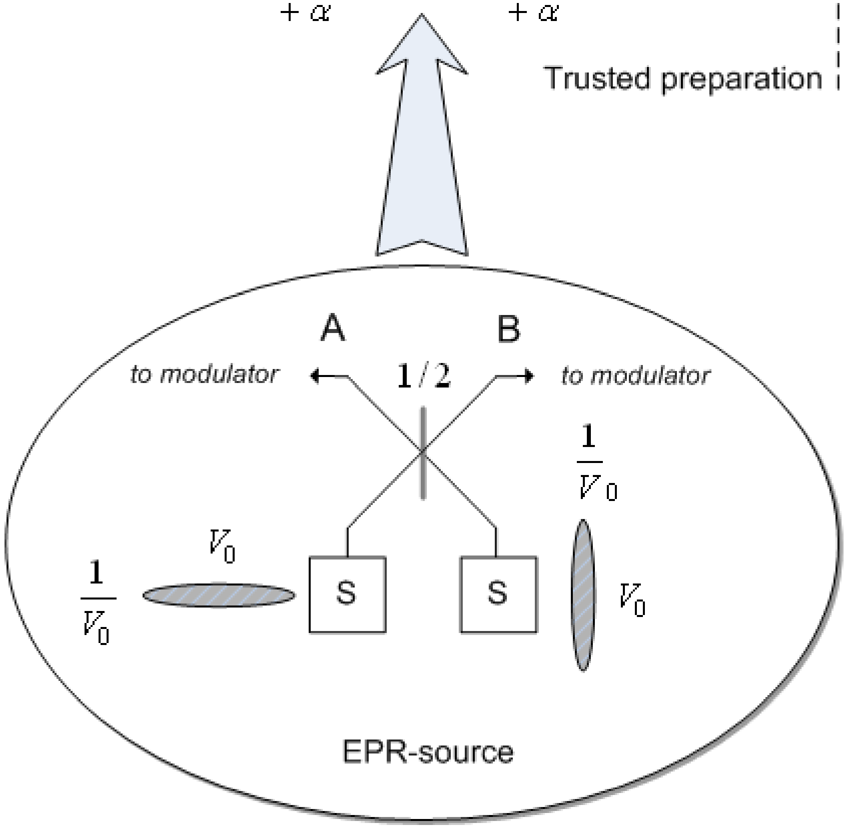


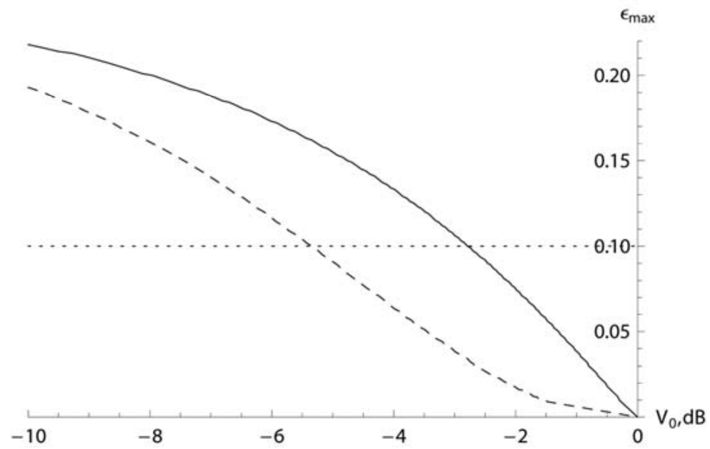


Additional modulation of squeezed states (i.e., additional classical correlations) makes scheme more robust to the channel excess noise.

Additional classical correlations

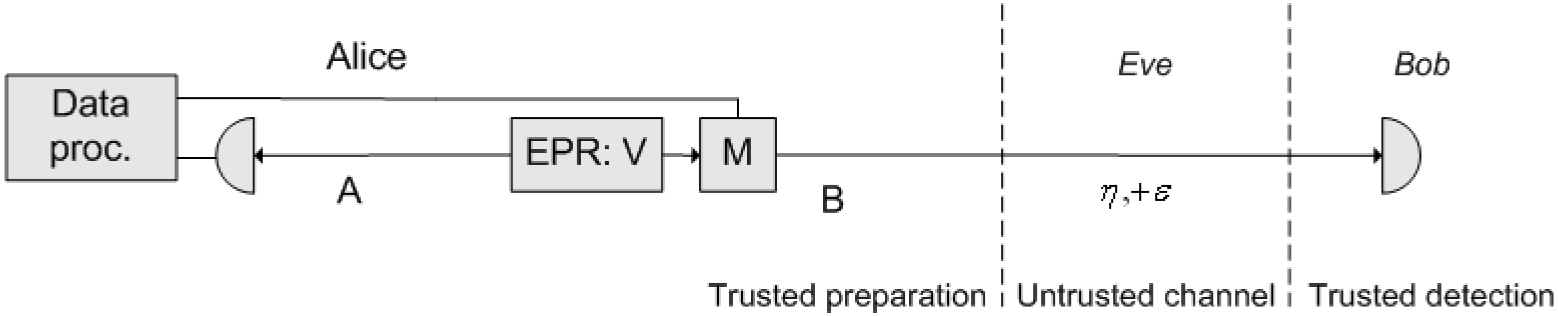






*[V. Usenko and R. Filip, New J. Phys., **13**, 113007, (2011) / arXiv:1111.2311]*

Super-optimized protocol



Alice applies gain factor to her data:

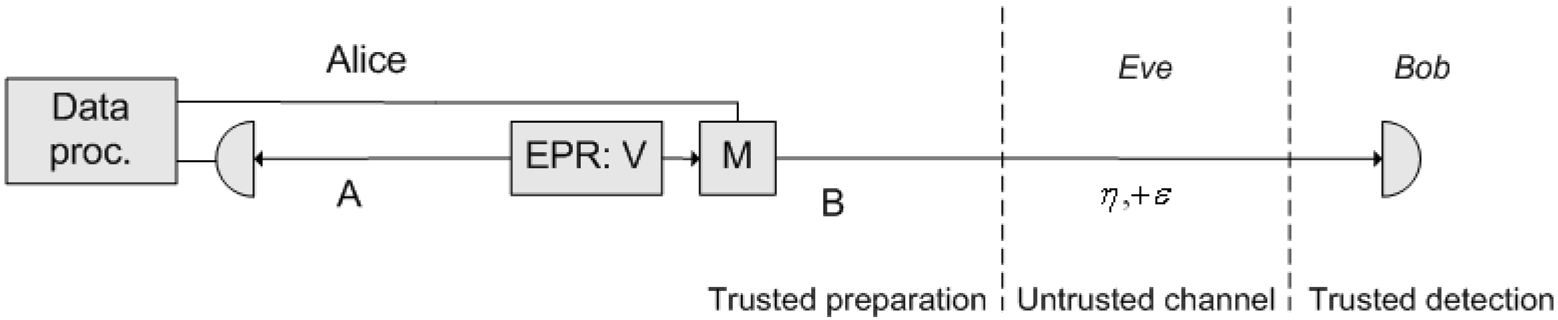
$$x'_A = g x_A + x_M$$

Covariance and correlation matrices:

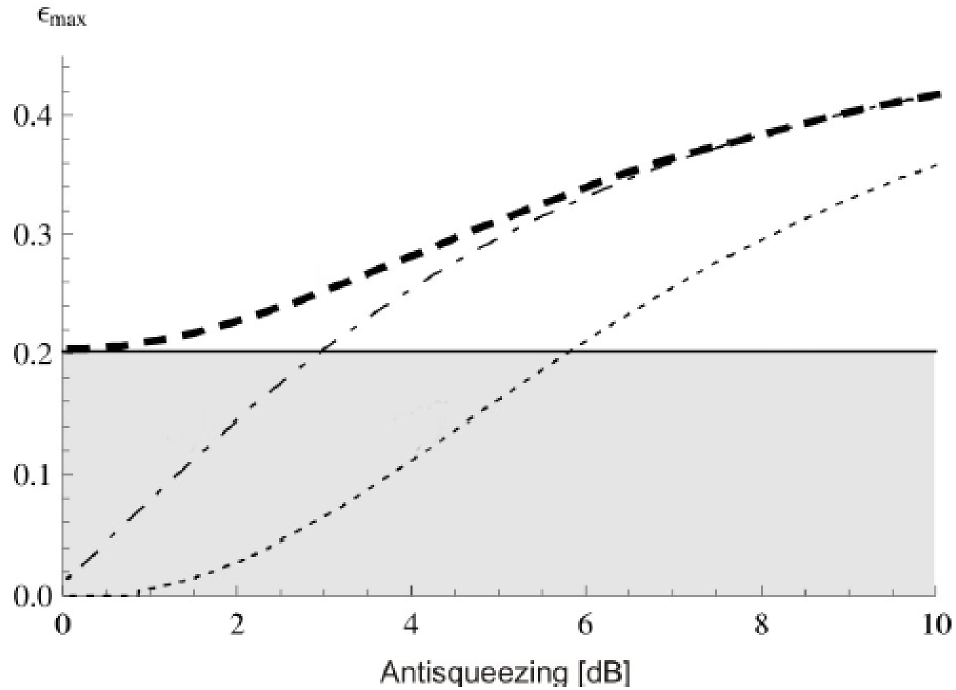
$$\gamma_A = \left[g^2 \frac{1}{2}\left(\frac{1+V_0^2}{V_0} + \Delta V_0\right) + \Delta V\right]\mathbb{I}$$

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

Super-optimized protocol

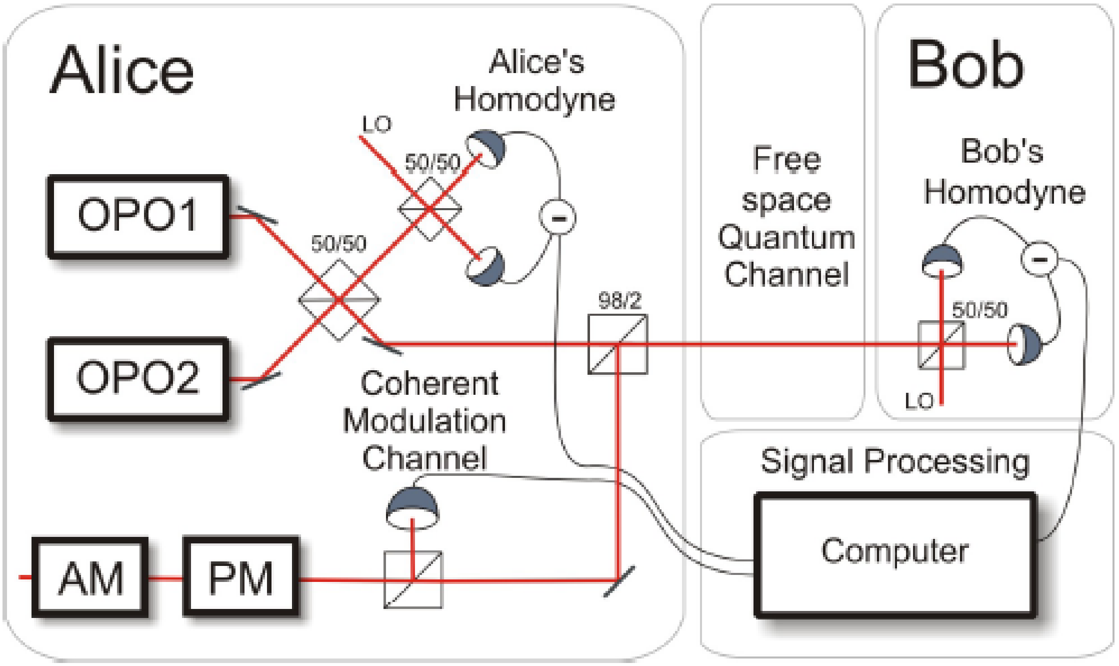


The protocol overcomes the coherent-state protocol upon any degree of squeezing



Proof-of-principle

Performed at the Denmark Technical University, Lyngby (NLQO group, Prof. Ulrik Andersen)



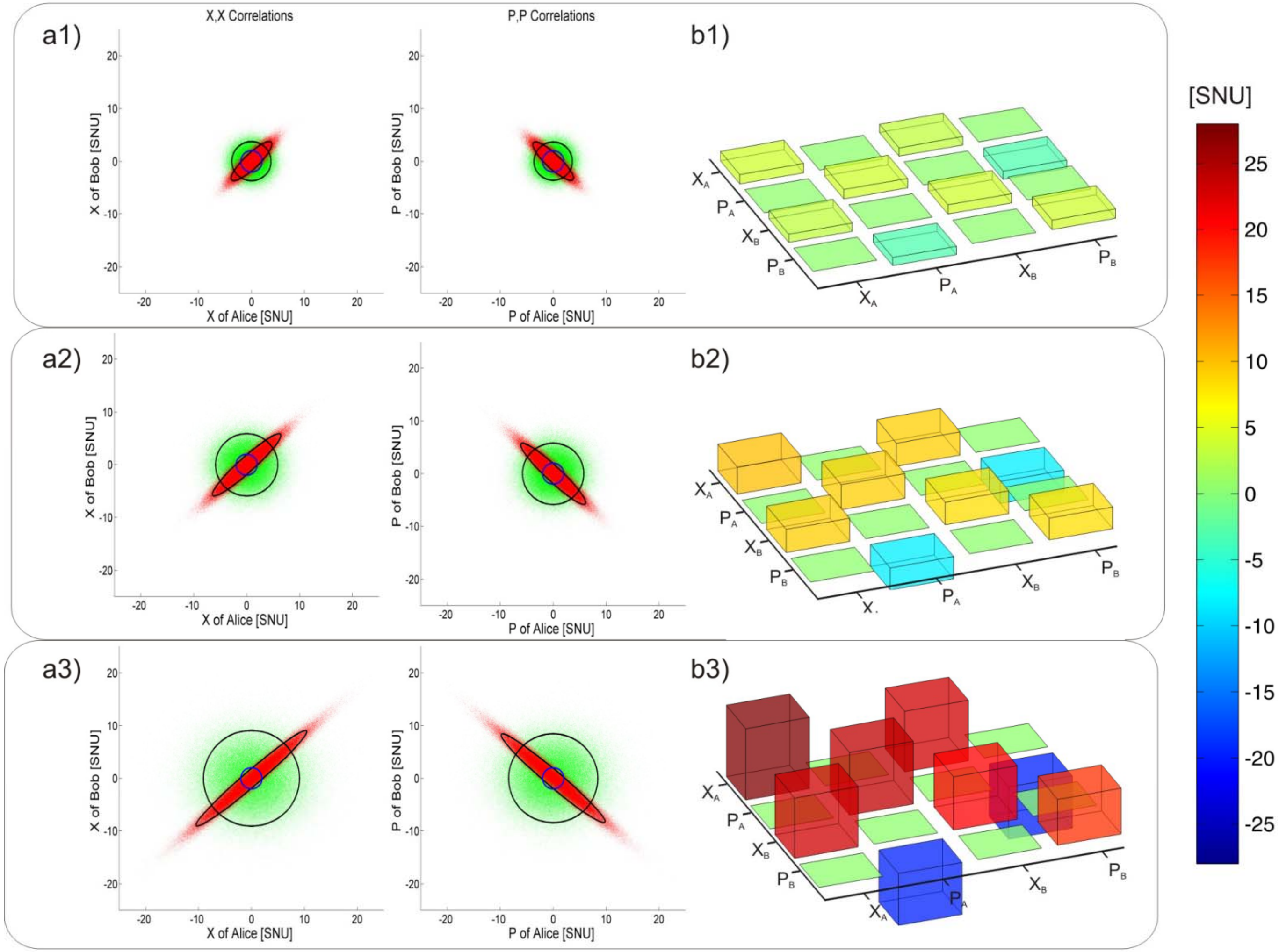
Sketch of the set-up

Proof-of-principle

No modulation

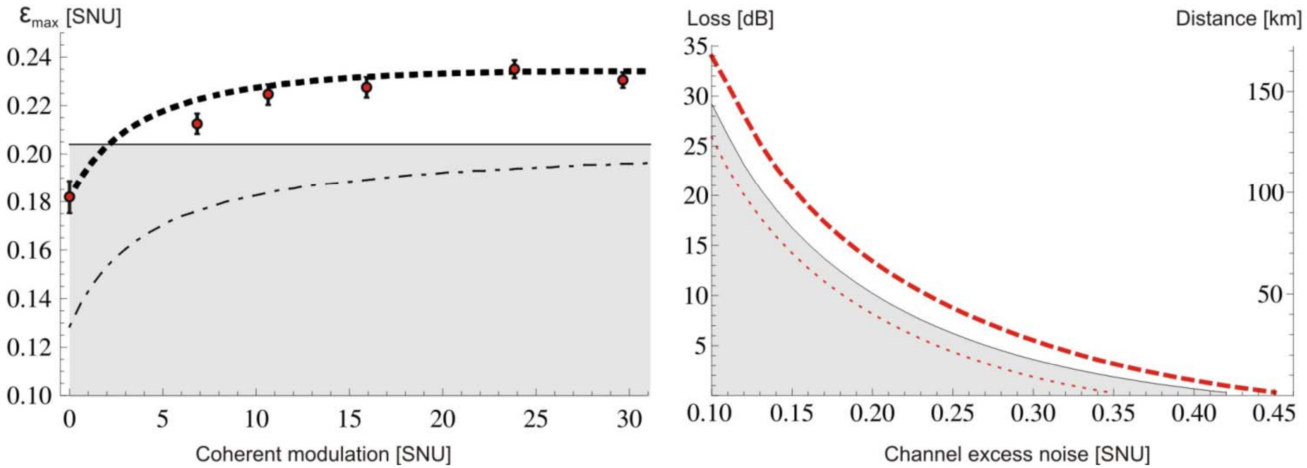
3.6 SNU

23.8 SNU



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

Proof-of-principle



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, arXiv:1110.5522

Resources in CV QKD

- Classical modulation is helpful
- Coherent states are enough

What is what in CV QKD?
What is the role of 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 (binarization, error correction)

Generally depends on SNR and algorithms.

Post-processing efficiency

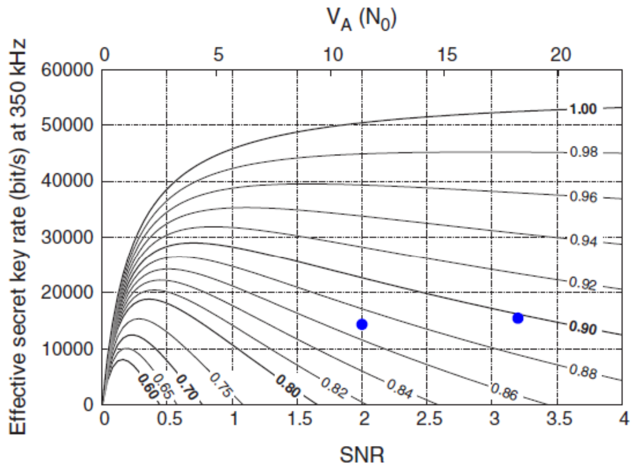
Lower bound on secure key rate (collective attacks) upon realistic reconciliation:

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

$\beta \in [0,1]$ - post-processing efficiency (binarization, error correction)

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*).



Post-processing efficiency

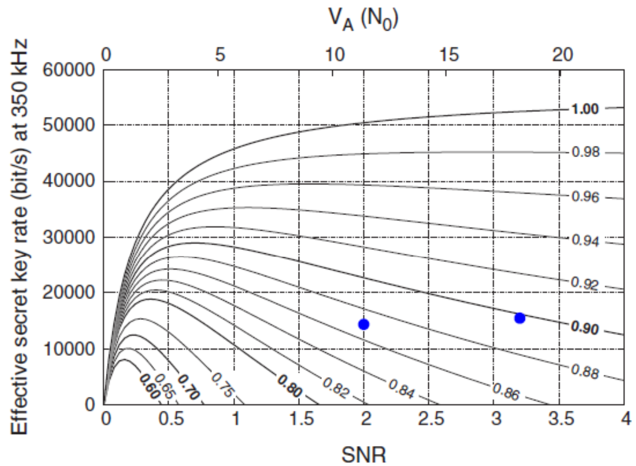
Lower bound on secure key rate (collective attacks) upon realistic reconciliation:

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

$\beta \in [0,1]$ - post-processing efficiency (binarization, error correction)

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*).



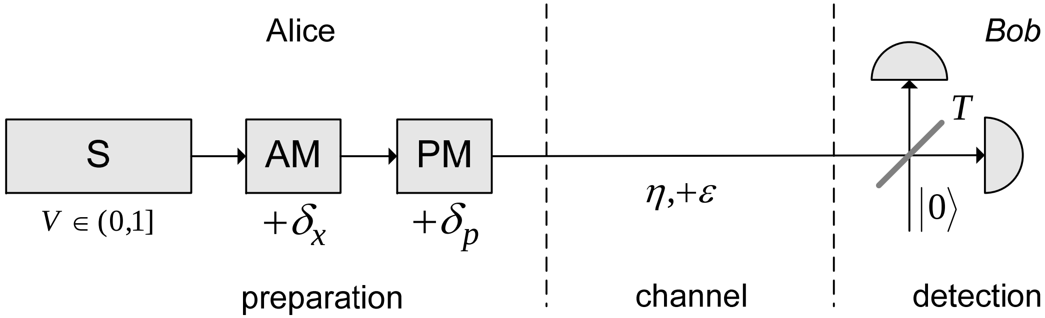
Together with mutual information – a classical resource.

<u>**Resources** (uniquely distinguishable in CV QKD)**:**</u>

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

Post-processing efficiency

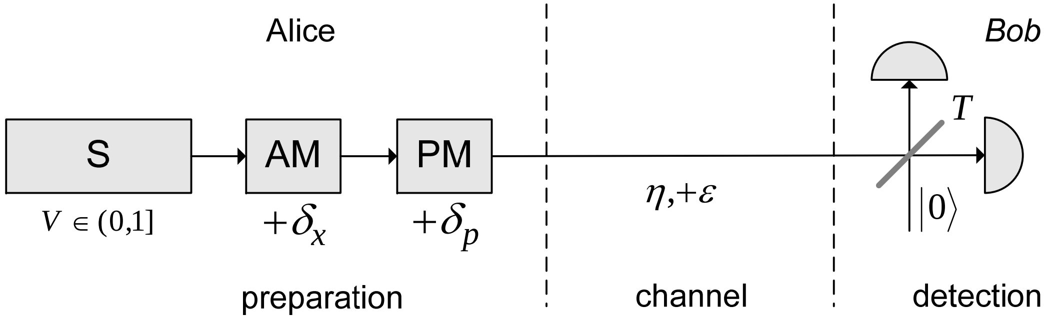
Generalized Gaussian P&M scheme:



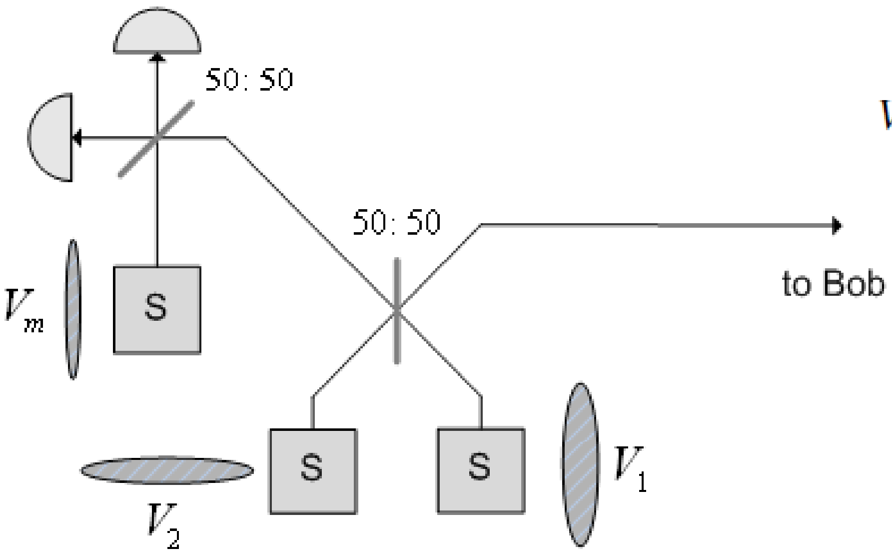
Not equivalent to a generic entanglement-based scheme.

Post-processing efficiency

Generalized Gaussian P&M scheme:



Equivalent to the modified scheme:



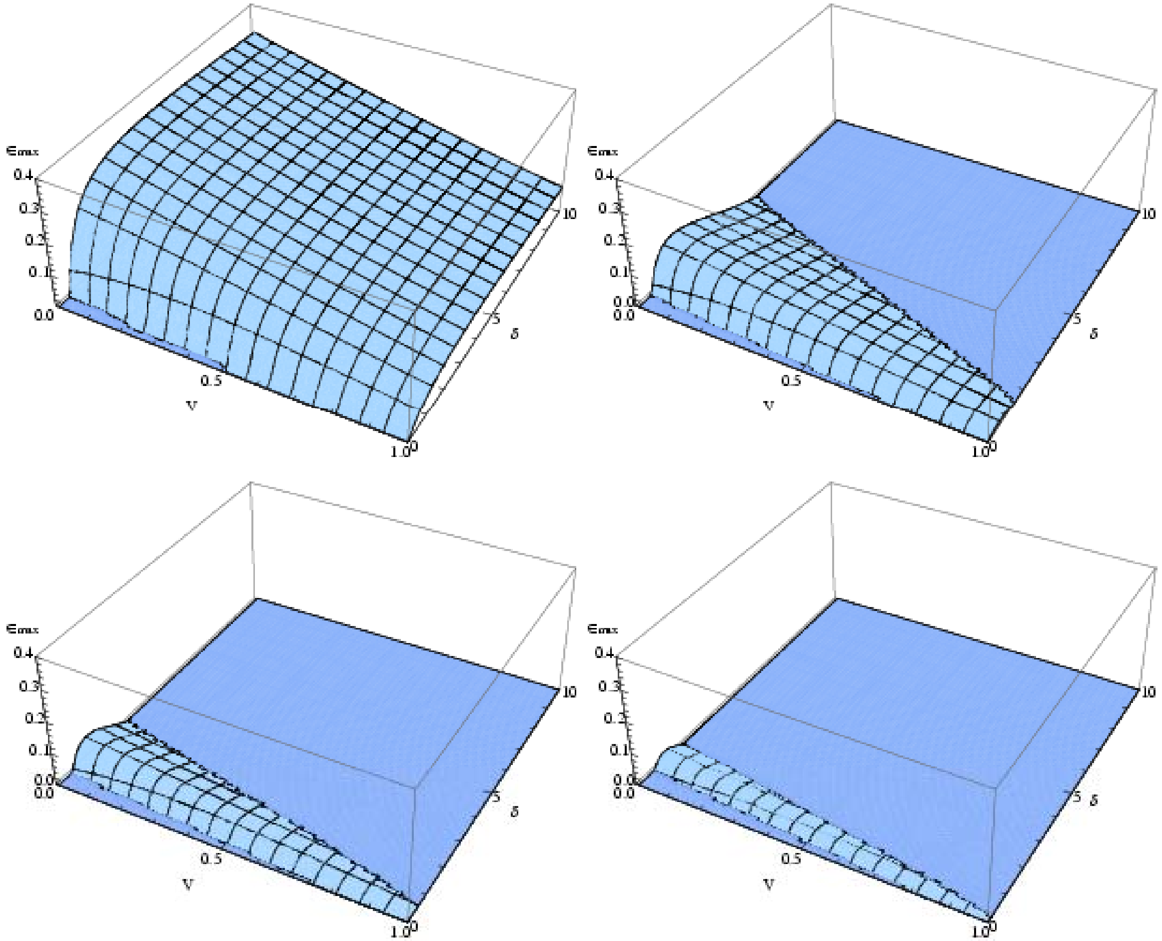
$$V_{1,2} = V + \sigma_x \pm \sqrt{\frac{(V + \sigma_x)(\sigma_x + V\sigma_p(V + \sigma_x))}{1 + V\sigma_p}}$$

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

Limited post-processing

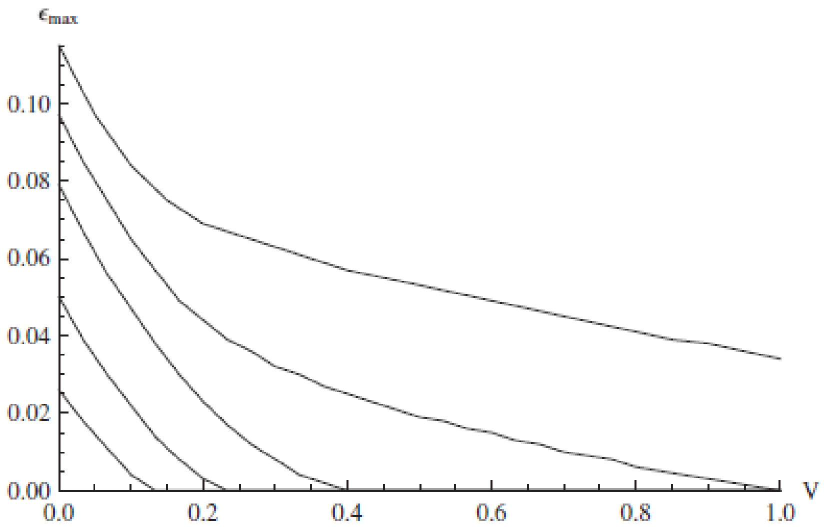
$\beta = 0.95$ $\beta = 0.6$

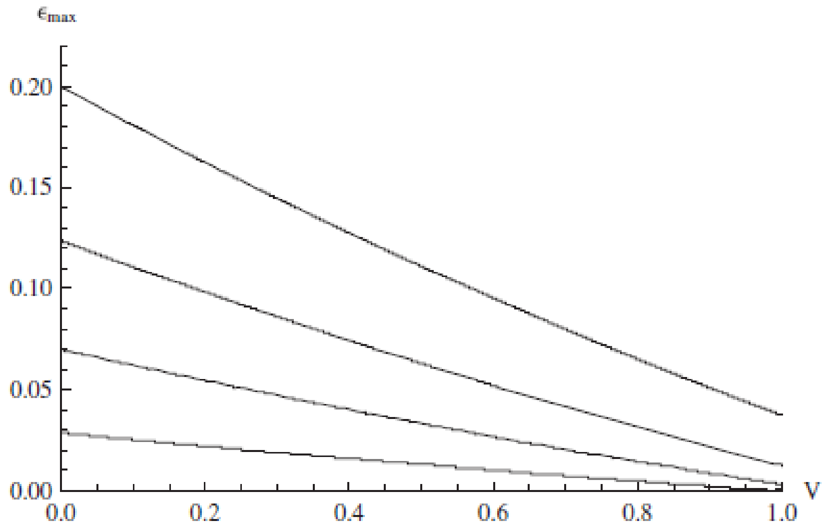
$\beta = 0.4$ $\beta = 0.2$



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

Limited post-processing



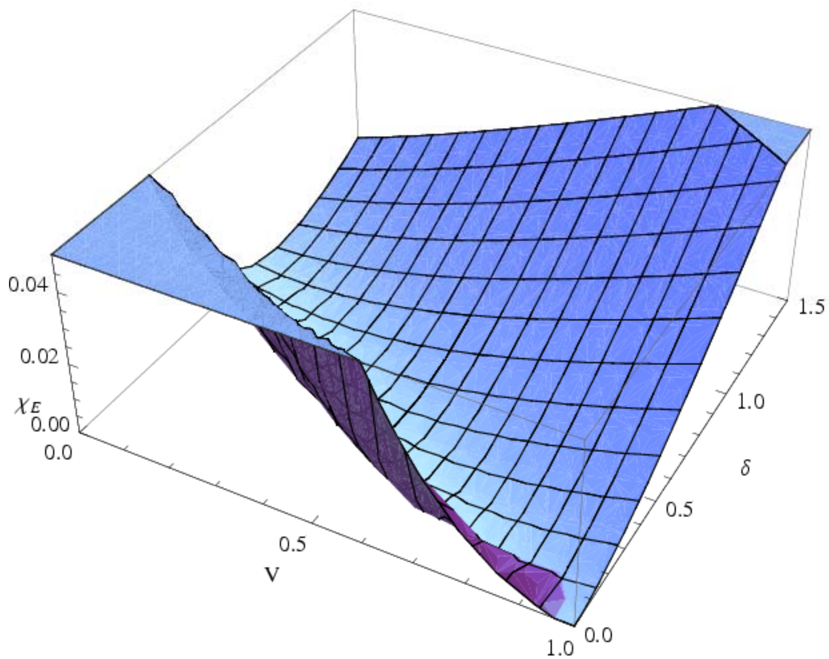


Noise threshold profile versus signal state variance (from squeezed to coherent state) upon optimized modulation. Left: direct reconciliation, right: reverse

Strongly limited post-processing

$$\beta \ll 1$$

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



Upper bound on Eve’s information (Holevo quantity)

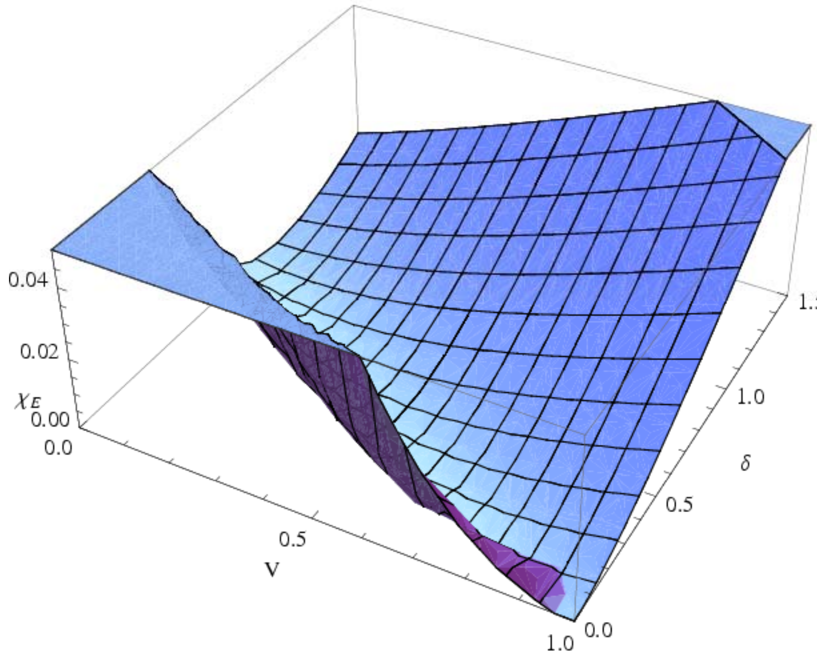
Minimization is achieved upon complete decoupling (zero correlation). Squeezing allows stronger modulation, while coherent states allow no modulation if Holevo quantity needs to be minimized.

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

Strongly limited post-processing

$$\beta \ll 1$$

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



Maximal secure modulation:

$$\sigma_{max} = 1 - V$$

Upper bound on Eve's information (Holevo quantity)

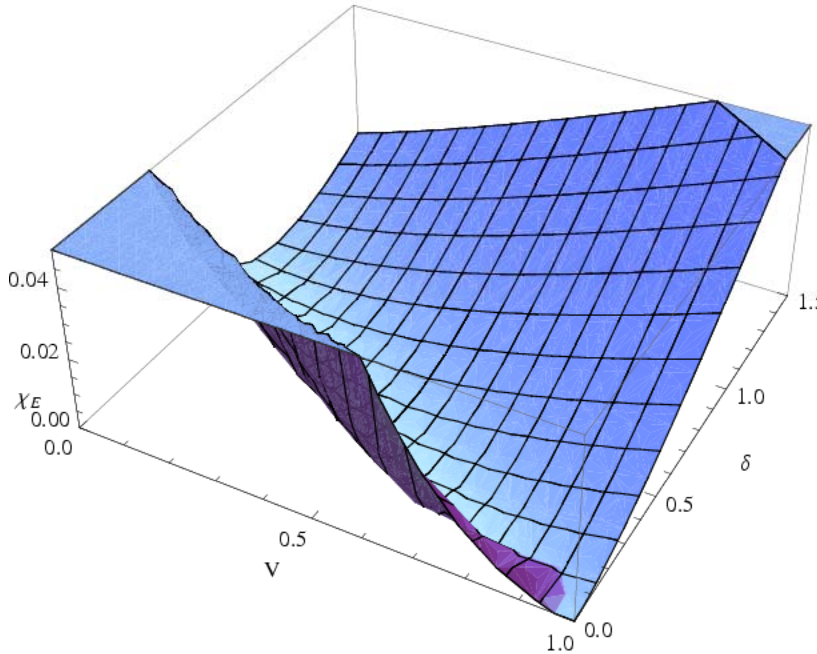
Minimization is achieved upon complete decoupling (zero correlation). Squeezing allows stronger modulation, while coherent states allow no modulation if Holevo quantity needs to be minimized.

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

Strongly limited post-processing

$$\beta \ll 1$$

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



Maximal secure modulation:

$$\sigma_{max} = 1 - V$$

For infinite squeezing:

$$V \to 0$$

$$\frac{1}{1+\sqrt{\beta}} < \sigma < \frac{1}{1-\sqrt{\beta}}$$

Upper bound on Eve's information (Holevo quantity)

Minimization is achieved upon complete decoupling (zero correlation). Squeezing allows stronger modulation, while coherent states allow no modulation if Holevo quantity needs to be minimized.

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

Summary

- Preparation noise is security-breaking for CV QKD protocols, although being trusted. The states can be purified to restore security;

- Additional correlated modulation improves security region of a squeezed CV QKD protocol;

- Super-optimized protocol uses advantage of both coherent and squeezed protocols, gaining from any degree of squeezing;

- If post-processing efficiency is limited, nonclassicality is required to provide security of CV QKD. Protocols then enter nonclassical regime, when coherence is not enough.

- Nonclassical resource (squeezing) can partly substitute the classical (computational) resource.