TOWARDS MULTIMODE CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

Vladyslav C. Usenko, Laszlo Ruppert, Radim Filip

Department of Optics, Palacký University,
Olomouc, Czech Republic

SPIE Security+Defense 2014, Amsterdam

Outline

- Continuous-variable quantum key distribution
- Multimode homodyne detection
- Knowledge of detection structure
- Mode selection by homodyne detector
- Symmetrization of source modes
- Security stabilization by multimode states
- Summary

QKD

ALICE

Share a secret key between
Alice and Bob to use in one-time pad
(Vernam, 1919; Shannon, 1949)

BOB

Continuous variable realization – attempt to go beyond the single photon statistics

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: $[x, p] = 2i$

Continuous-variable states

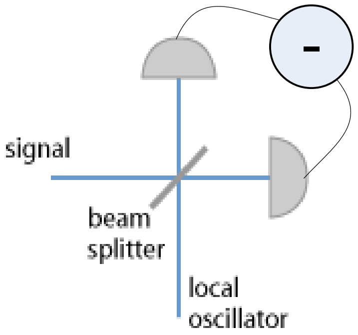
Field quadratures: analogue of the position and momentum operators of a particle:

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

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

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

Homodyne measurement:



Continuous-variable states

Gaussian states:

characteristic function / Wigner function is Gaussian

Covariance matrix:
Explicitly describes Gaussian states

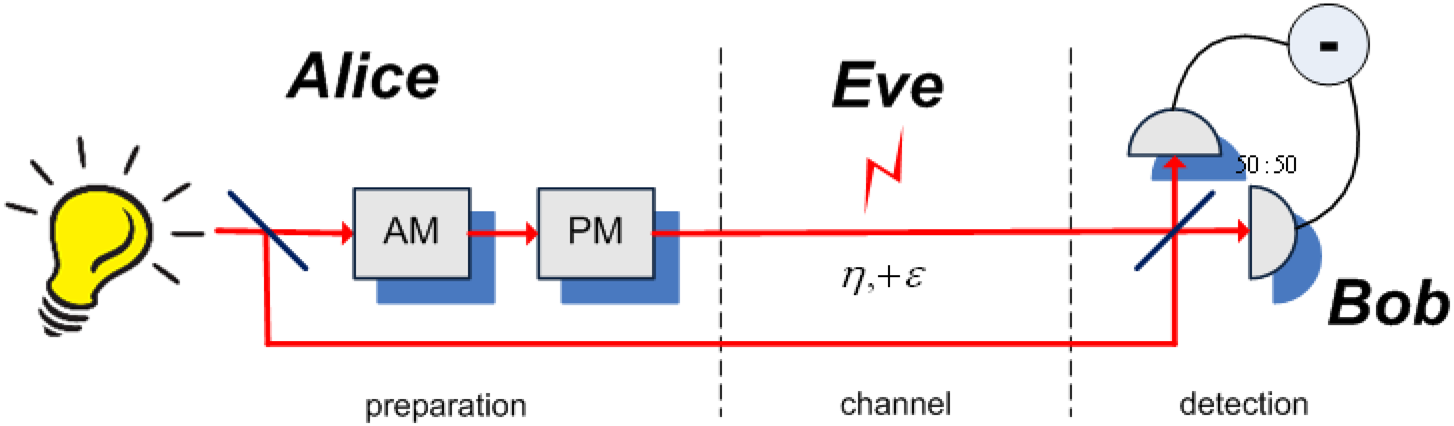
$$\boxed{\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle}$$

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

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

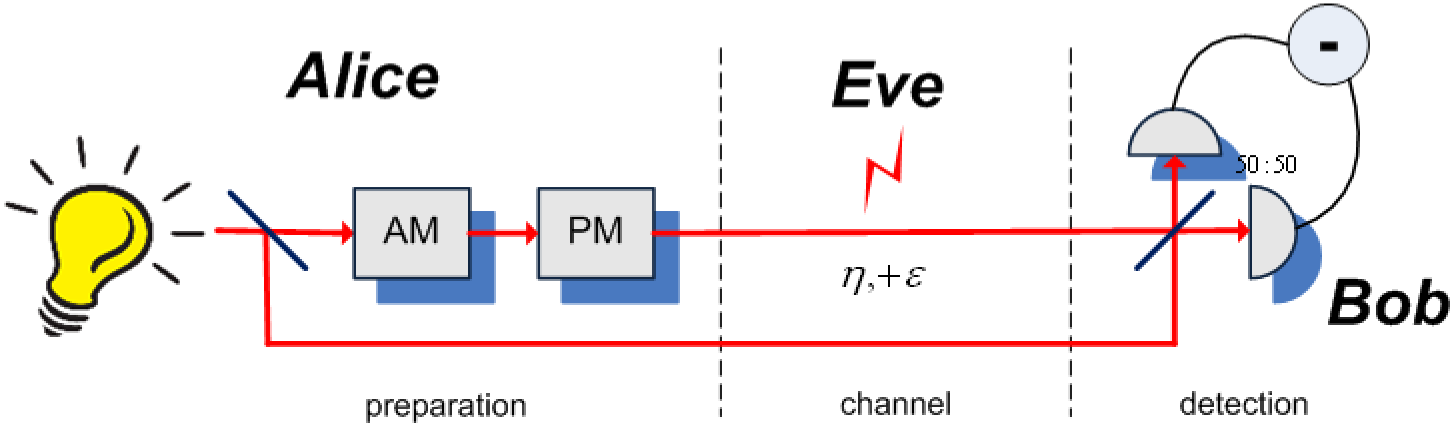
Bosonic commutation relations: $[\hat{r}_k, \hat{r}_l] = i\Omega_{kl}$

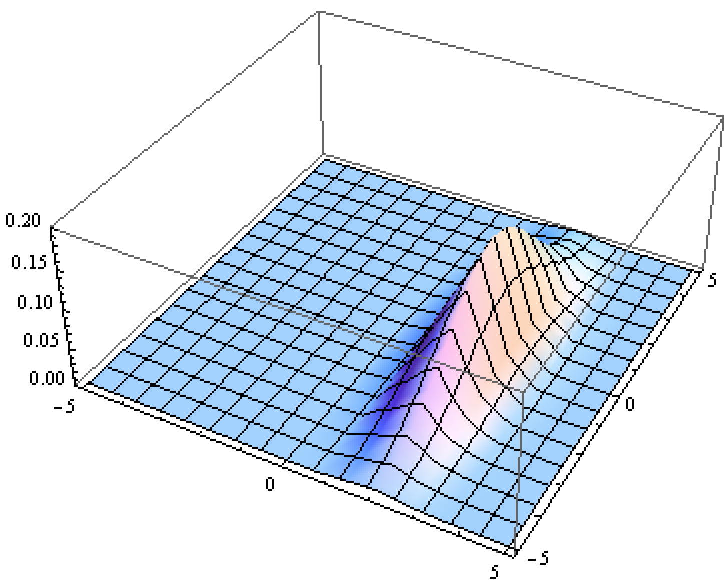
CV Quantum Key Distribution



T. C. Ralph, PRA 61, 0103303 (1999)

CV Quantum Key Distribution

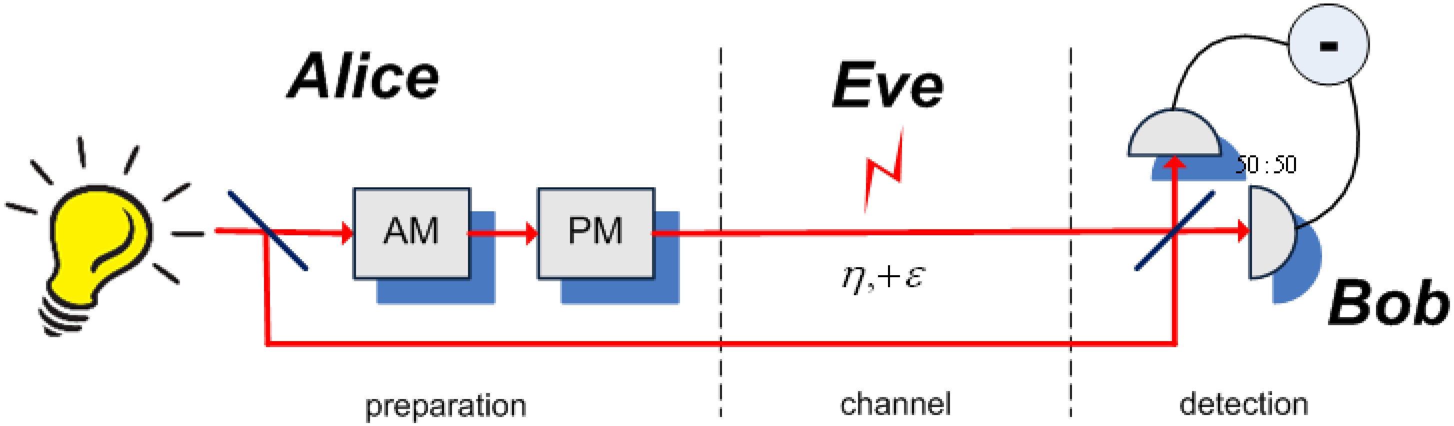


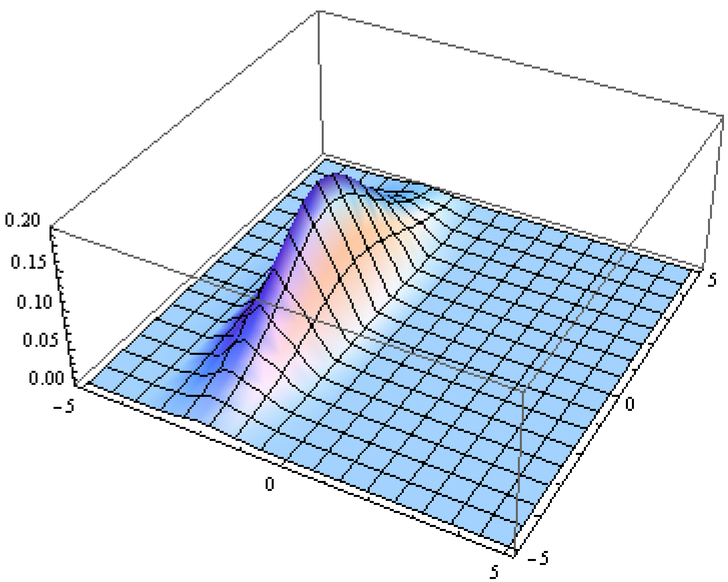


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

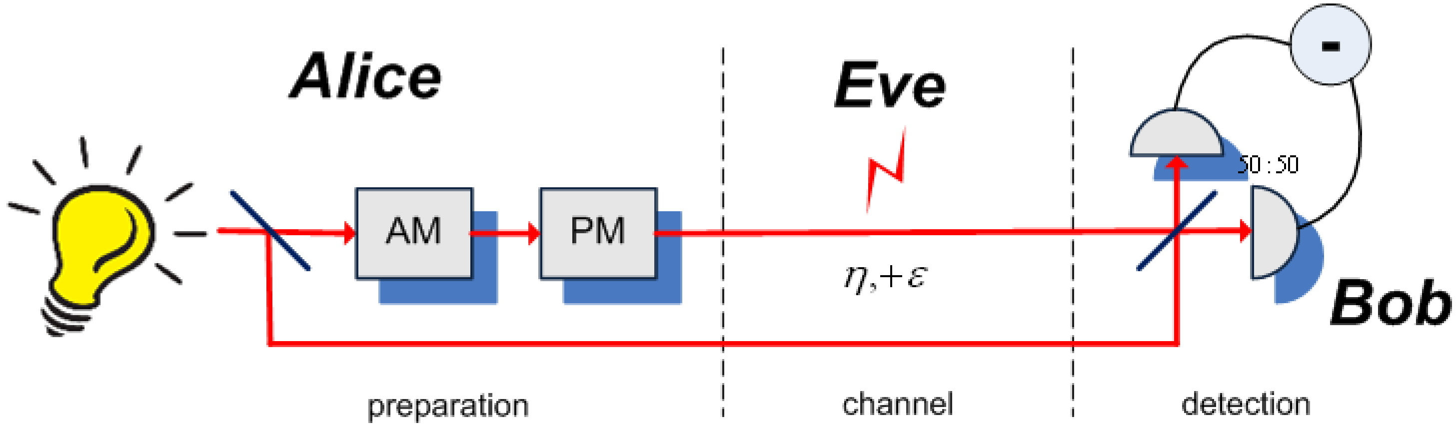


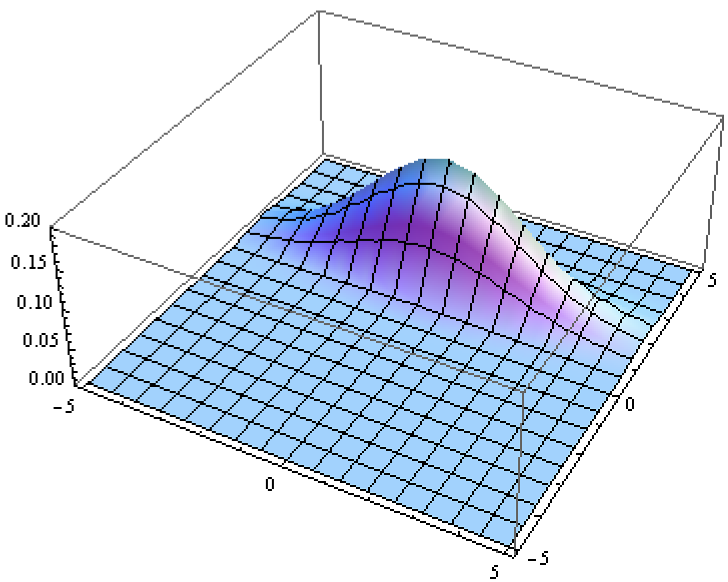


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

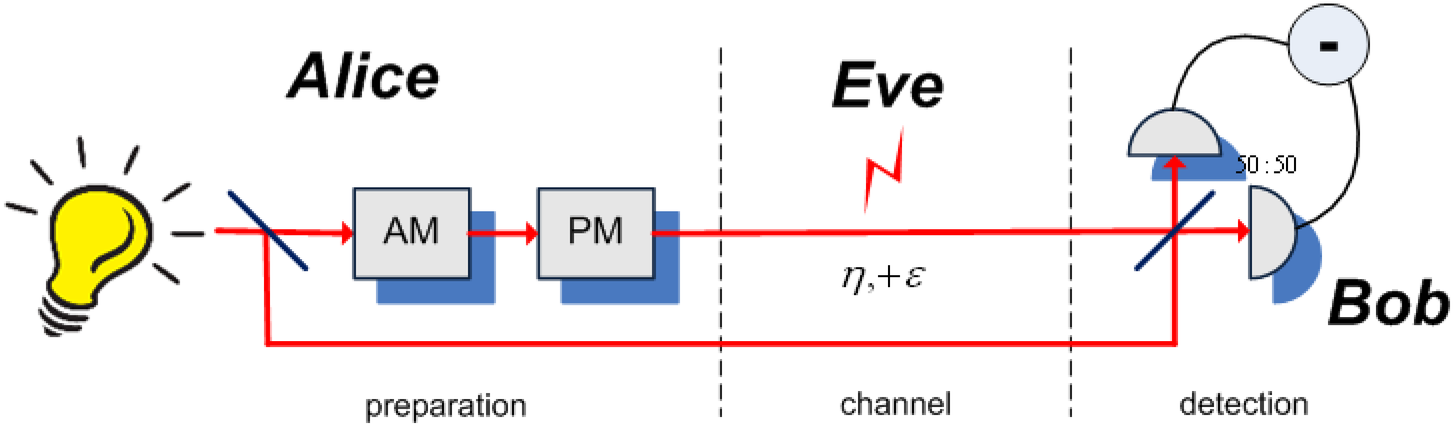


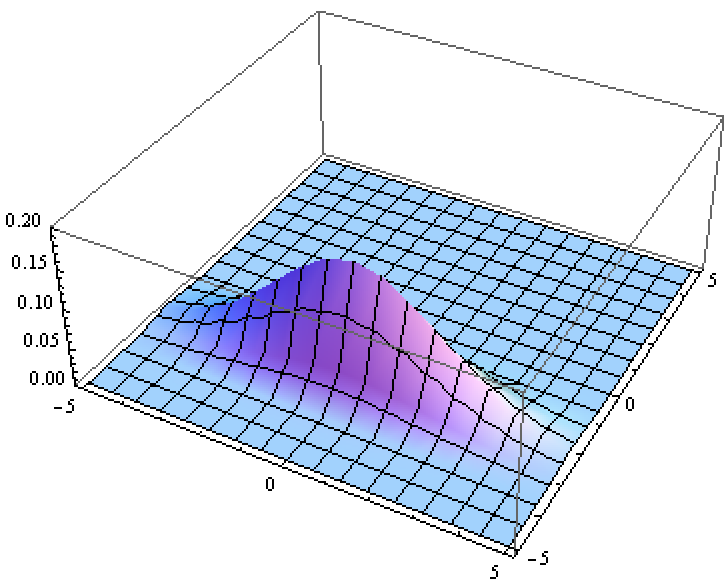


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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

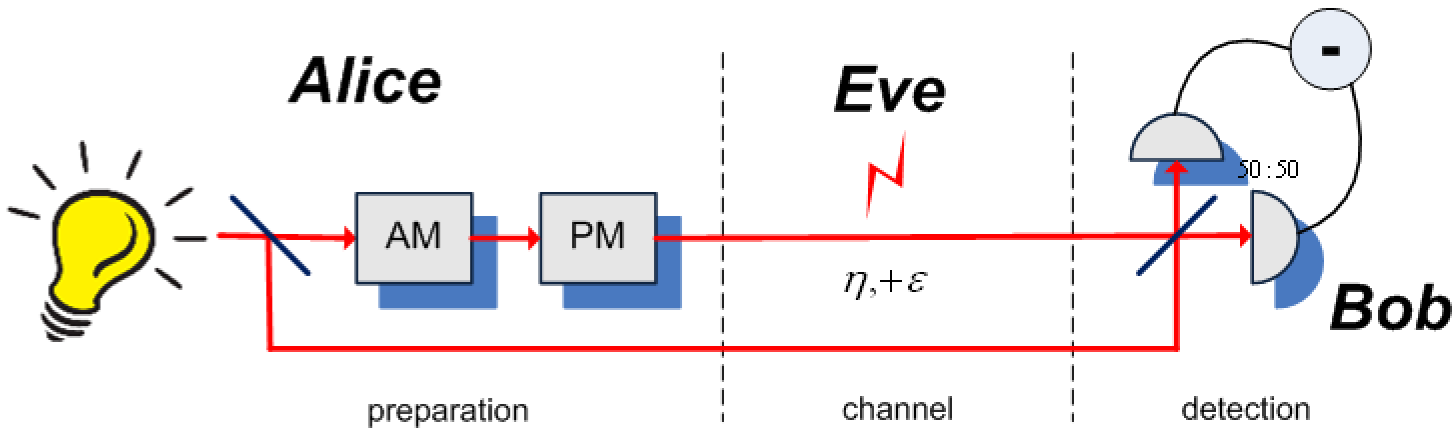


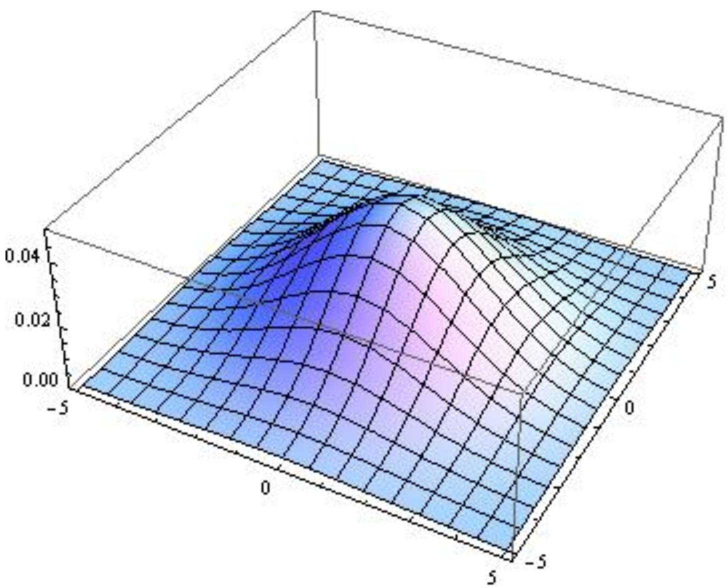


Squeezed states-based protocol:
Squeezed source, modulation
N. J. Cerf, M. Levy, and G. Van Assche, PRA 63, 052311 (2001)

- 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



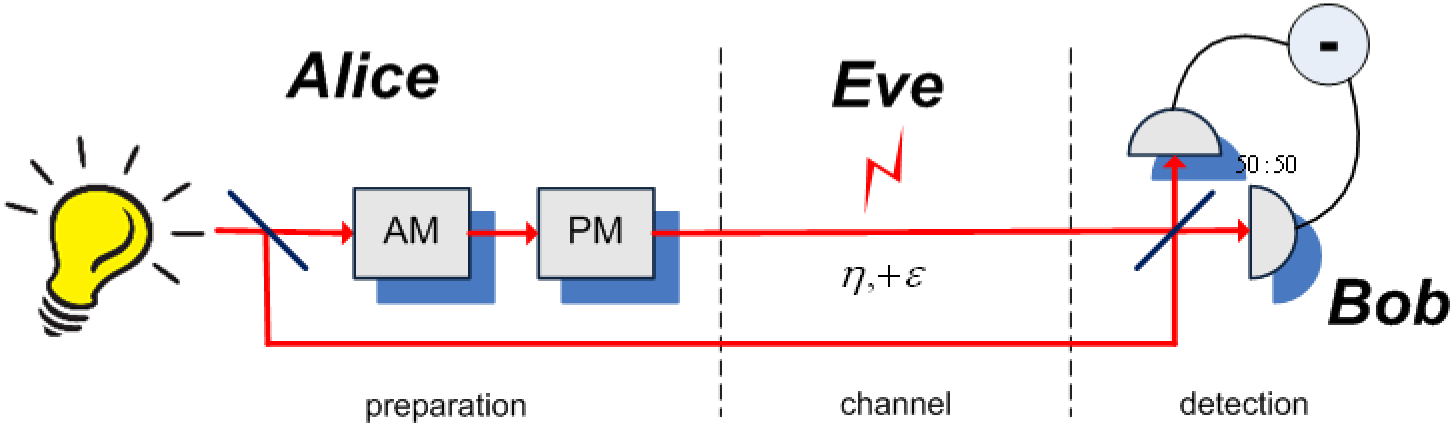


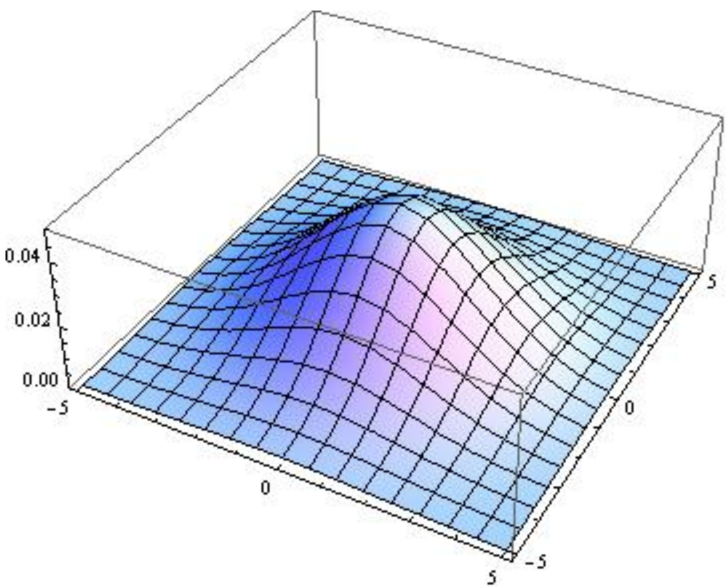
Mixture

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

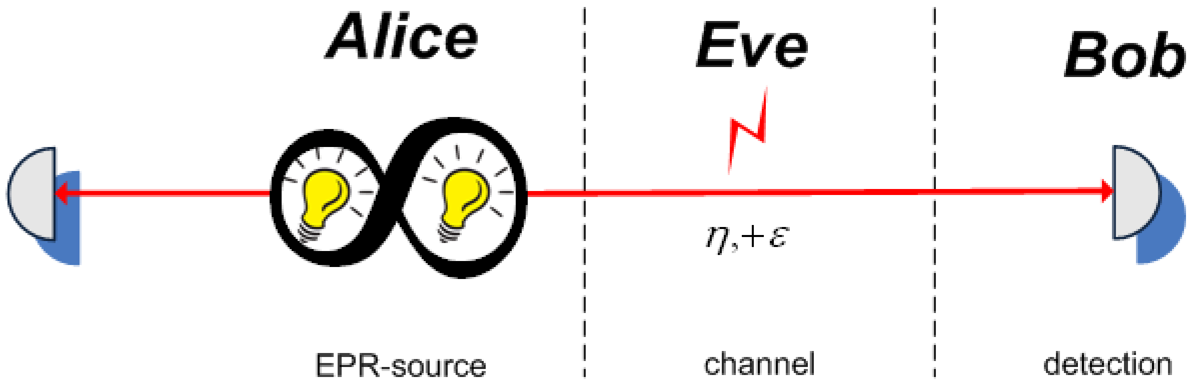


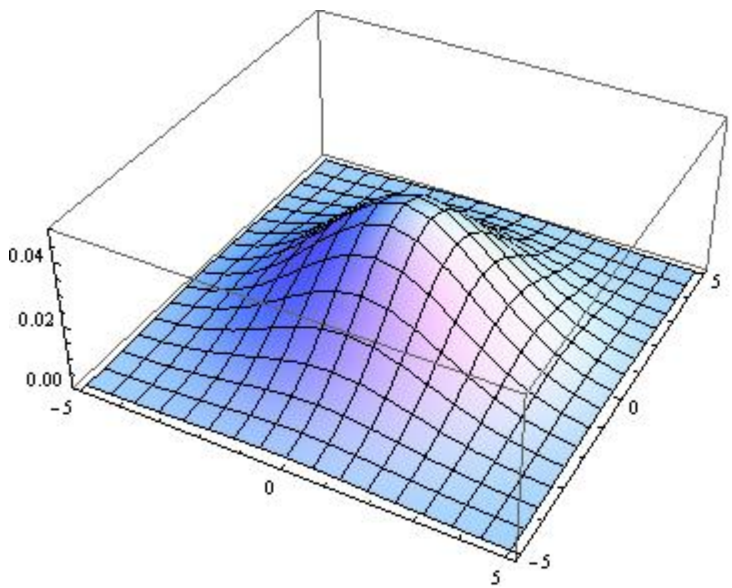


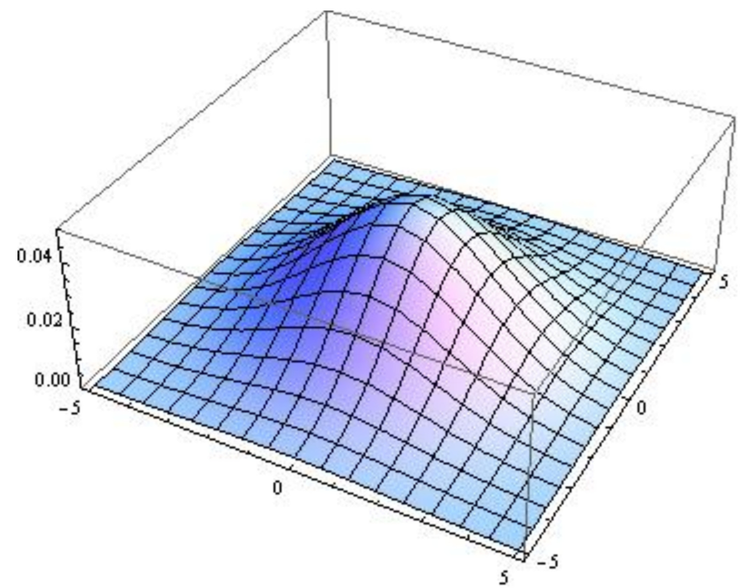
Mixture

Alternatively: 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 QKD: entangled-based

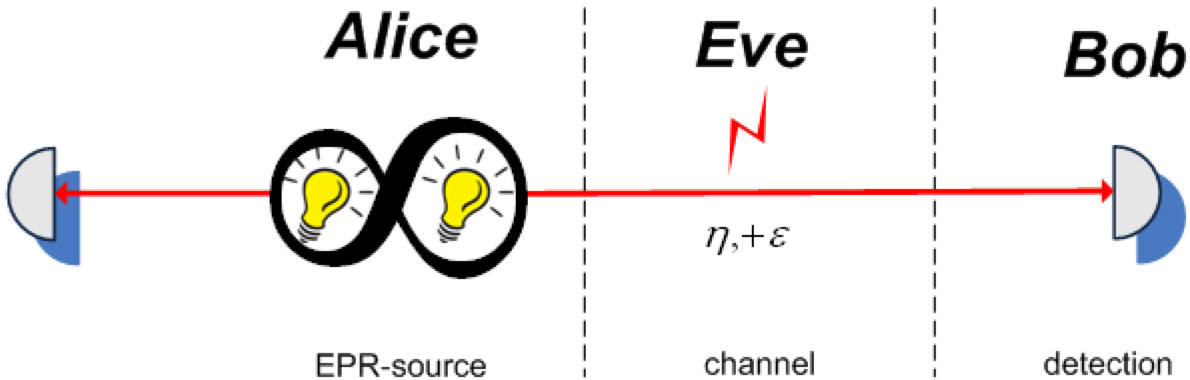




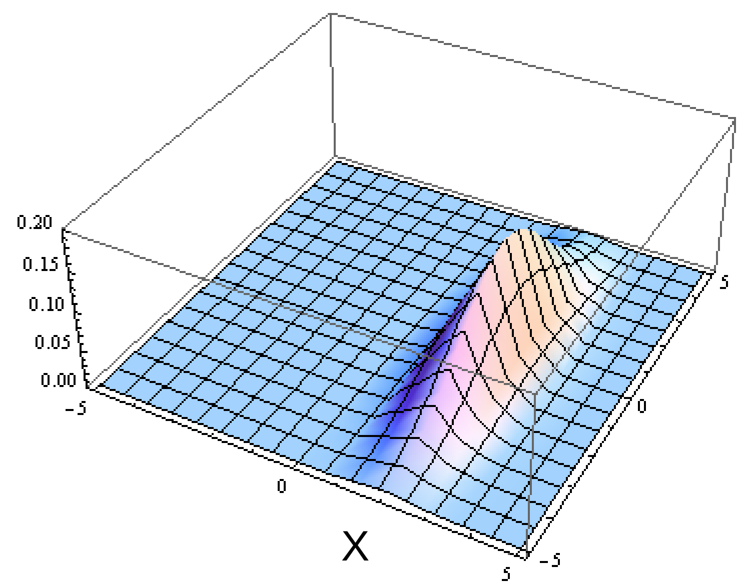


Two-mode squeezed vacuum: Before measurement

CV QKD: entangled-based



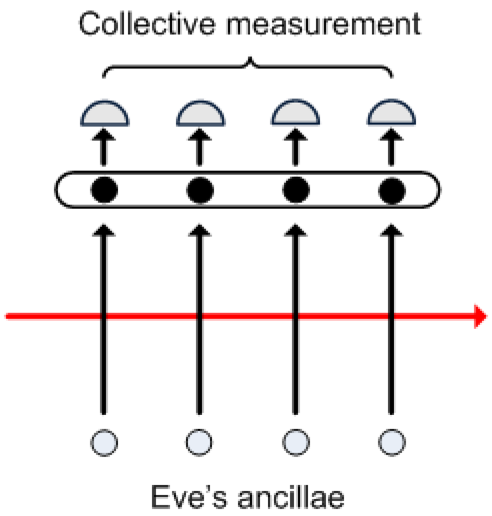
X



Two-mode squeezed vacuum: after homodyne measurement

CV QKD: security

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



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

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

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

CV QKD: security

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

Gaussian modulation / Gaussian entangled states:

• Gaussian states extremality [M. M. Wolf, G. Giedke,and J. I. Cirac, PRL 96, 080502 (2006)]

• Gaussian attacks optimality [R. Garcia-Patron and N. J. Cerf, PRL 97, 190503 (2006); M. Navascues, F. Grosshans, and A. Acin, PRL 97, 190502 (2006)]

• Covariance matrix description is enough

CV QKD: security

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

computation: $S(\gamma) = \sum_{i=1}^{N} G\left(\frac{\nu_i - 1}{2}\right)$, $G(x) = (x+1)\log_2(x+1) - x\log_2 x$

ν_i - symplectic eigenvalues of the covariance matrix γ_E,

similarly for conditional state:

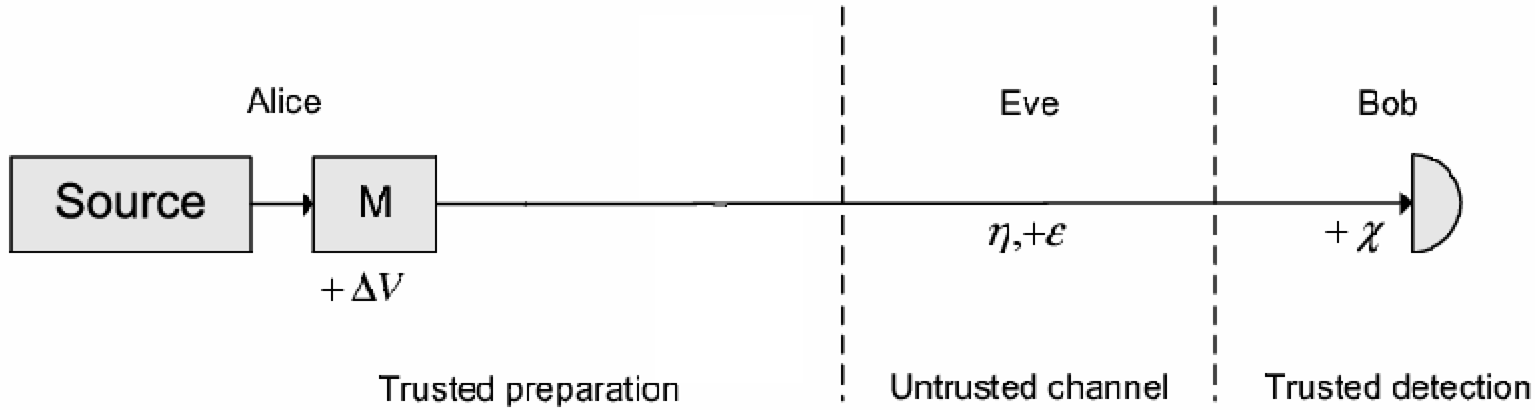
$$\gamma_E^{x_B} = \gamma_E - \sigma_{BE}(X\gamma_B X)^{MP}\sigma_{BE}^T$$

In the presence of channel noise purification by Eve is assumed:

$$S(\gamma_E) = S(\gamma_{AB}) \qquad S(\gamma_{E|B}) = S(\gamma_{A|B})$$

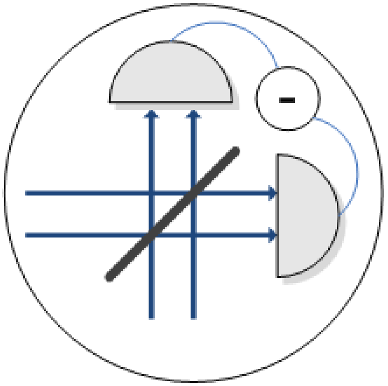
Practical issues

Noise (source, channel, detection), channel transmittance



- Source noise: VU, Filip, Phys. Rev. A **81**, 022318 (2010)
- Role of squeezing: VU, Filip, New J. Phys. **13**, 113007 (2011)
- Resource engineering: Lassen, VU, Madsen, Filip, Andersen, Nature Communications **3**, 1083 (2012)
- Fluctuating channels: VU, Heim, Peuntinger, Wittmann, Marquardt, Leuchs, Filip, New J. Phys. **14**, 093048 (2012)

Multimode homodyne detection



N-mode local oscillator $|\alpha_i| \exp(i\theta),\ i = 1, \ldots, N$

Ideal balanced detection $i_{-}^{(N)} = \sum_{i=1}^{N} |g_i \alpha_i| \tilde{X}_i(\theta)$

with $\tilde{X}_i(\theta) = a_i \exp(i\theta) + a_i^{\dagger} \exp(-i\theta)$

Detection calibration: measurement of $V_0^{(N)} = \sum_{n=1}^{N} |g_i \alpha_i|^2.$

After normalization of photo-current:

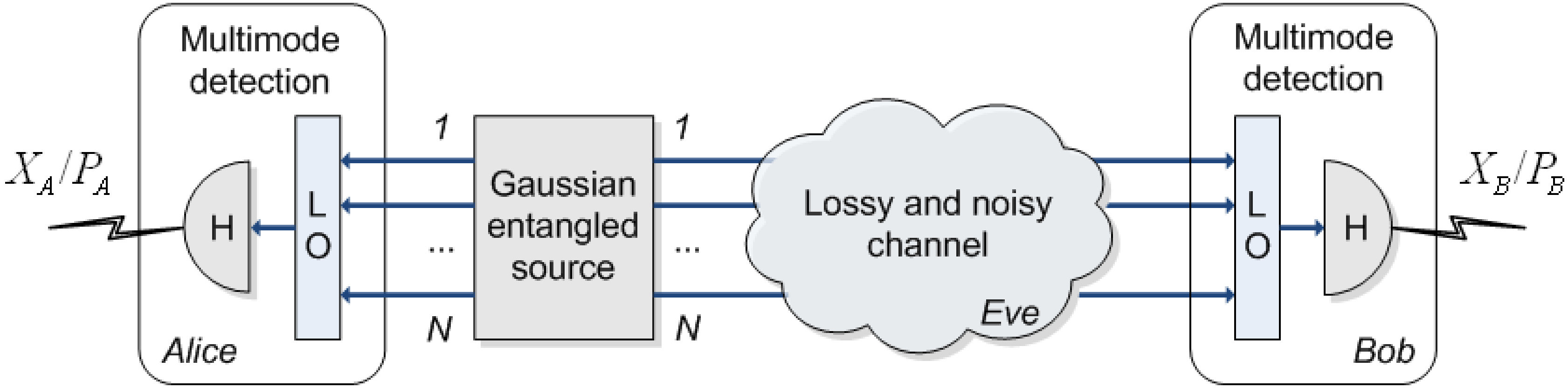
$$X^{(N)}(\theta) = \frac{\sum_{n=1}^{N} G_i \tilde{X}_i(\theta)}{\sqrt{\sum_{n=1}^{N} G_i^2}}$$

Normalization coefficients $\lambda_i = G_i / \sqrt{\sum_{n=1}^{N} G_i^2}$ satisfy $\sum_{i=1}^{N} \lambda_i^2 = 1$

Thus, **multimode homodyne = linear optical network and single-mode homodyne**

If $G_i = G$, then N-mode vacuum is $V_0^{(N)} = N G^2$ and $\boxed{X^{(N)}(\theta) = \frac{\sum_{i=1}^{N} \tilde{X}_i(\theta)}{\sqrt{N}}}$

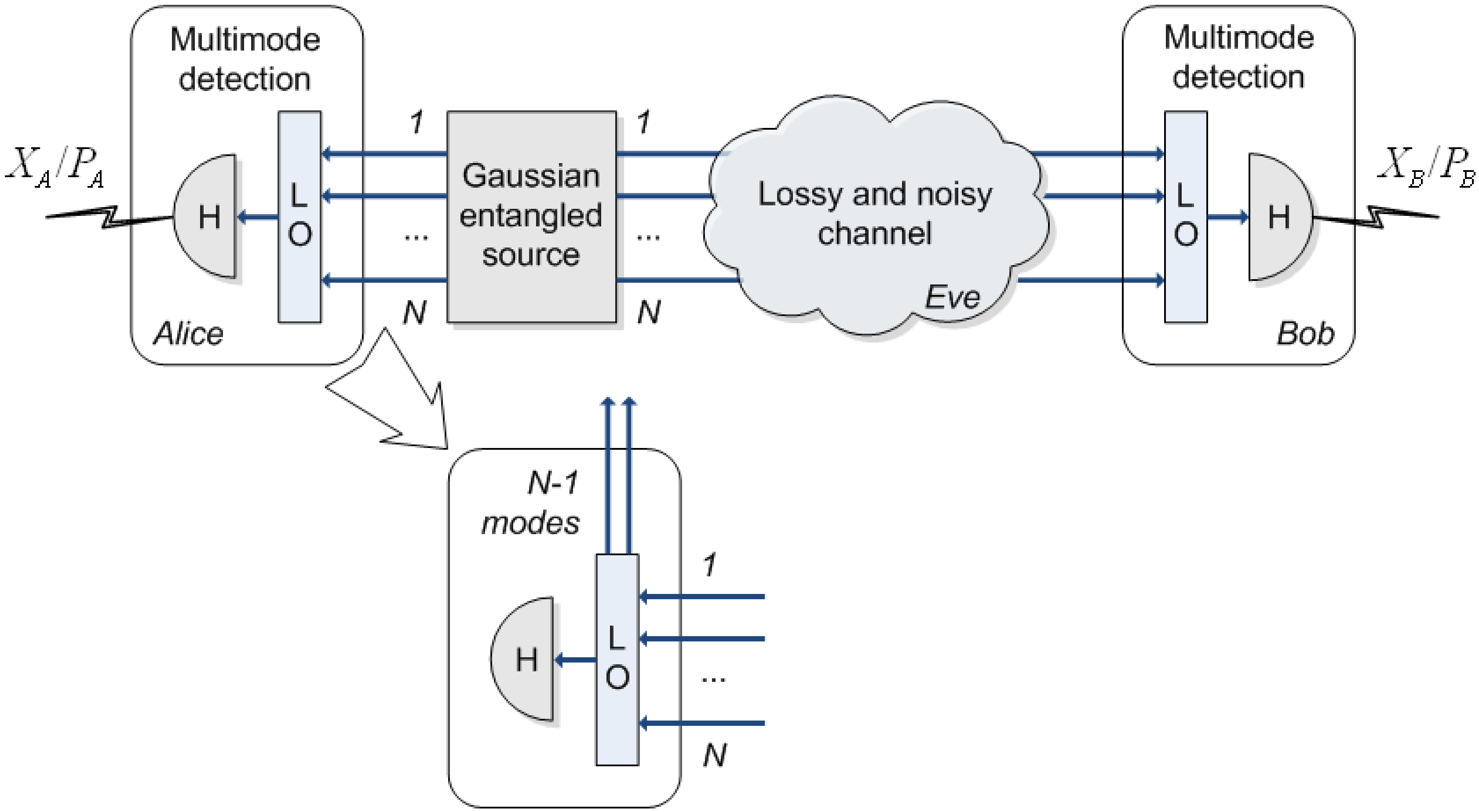
QKD with multimode states/detectors



Assumptions:

- No crosstalk between the modes
- No mode mismatch
- Detectors are identical in both the beams
- Channel is the same for all the modes
- **Multimode structure is completely known to Eve**

Untrusted multimode detectors

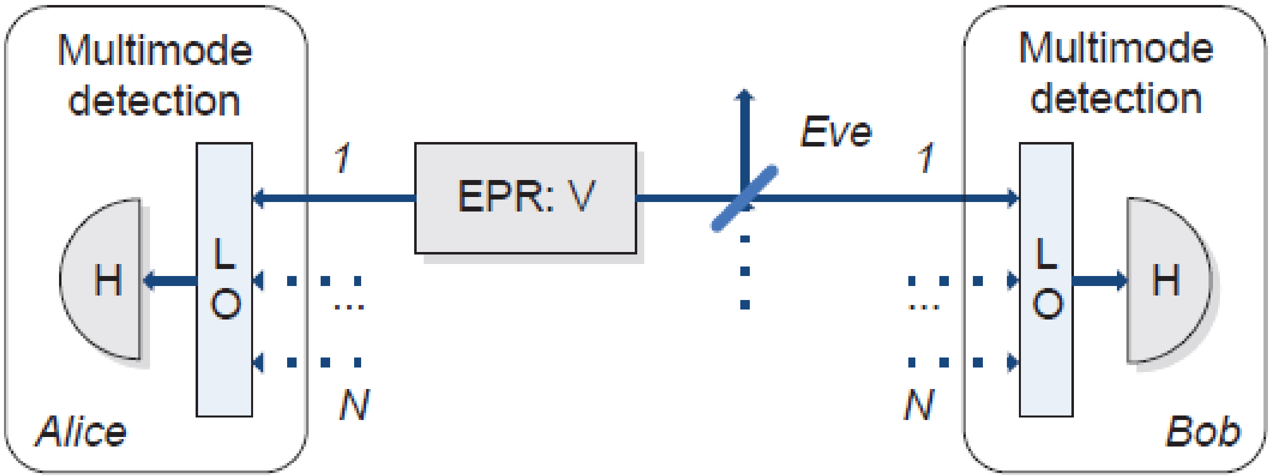


Output modes of the LO coupling before detection are available to Eve.

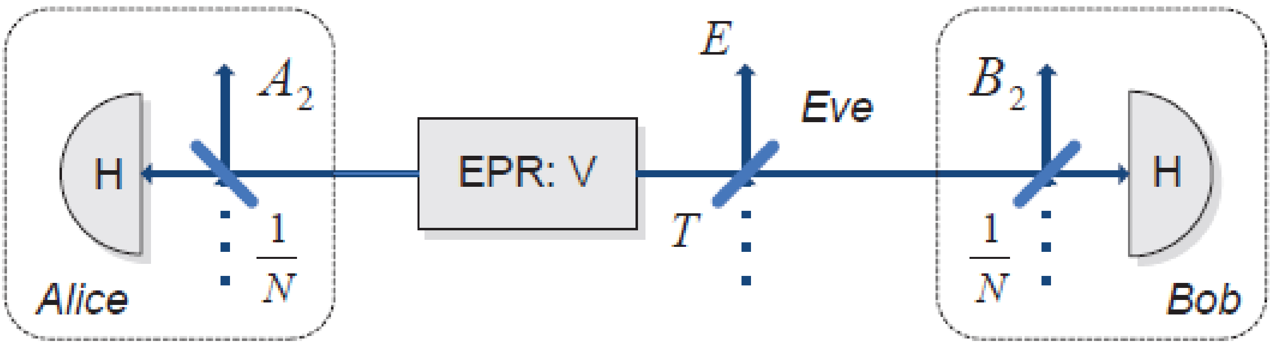
Multimode covariance matrix becomes weighted sum of single-modes ones:

$$\gamma_{AB}^{(N)} = \sum_{i=1}^{N} \lambda_i^2 \gamma_{AB,i}$$

Untrusted multimode detectors



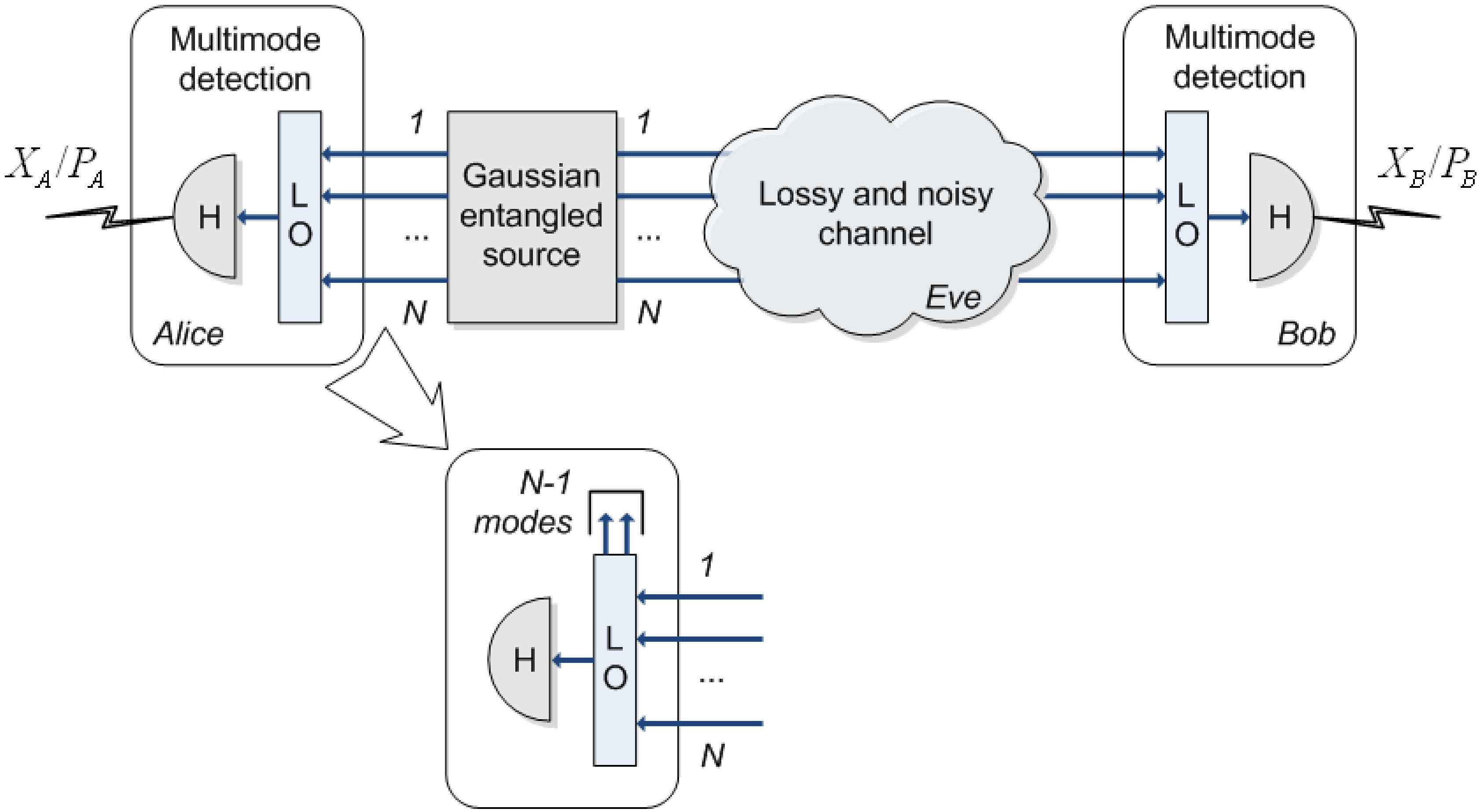
All modes, but one are in the vacuum state -> equivalent to symmetrical side-channels with untrusted outputs:



Security is lost already at perfect channel and N=2 !

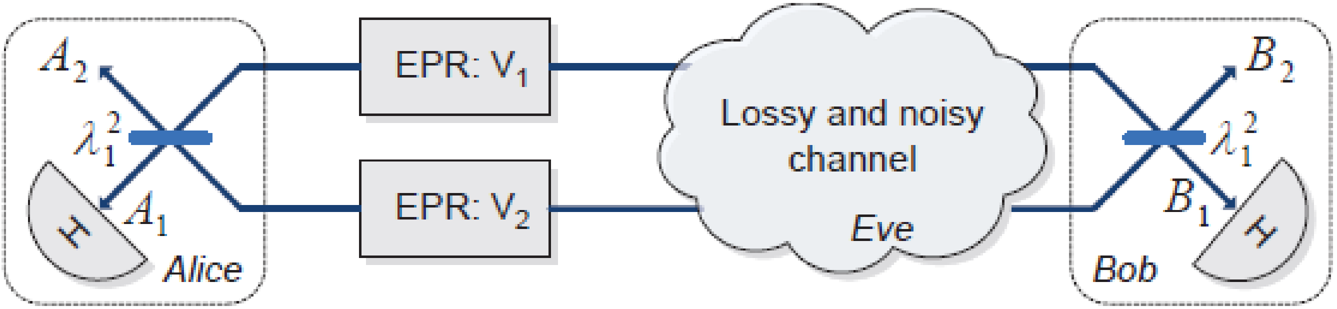
(while entanglement is preserved)

Trusted multimode detectors



If trusted parties know the mode structure, they can tighten bound on Eve's information.

Trusted multimode detectors



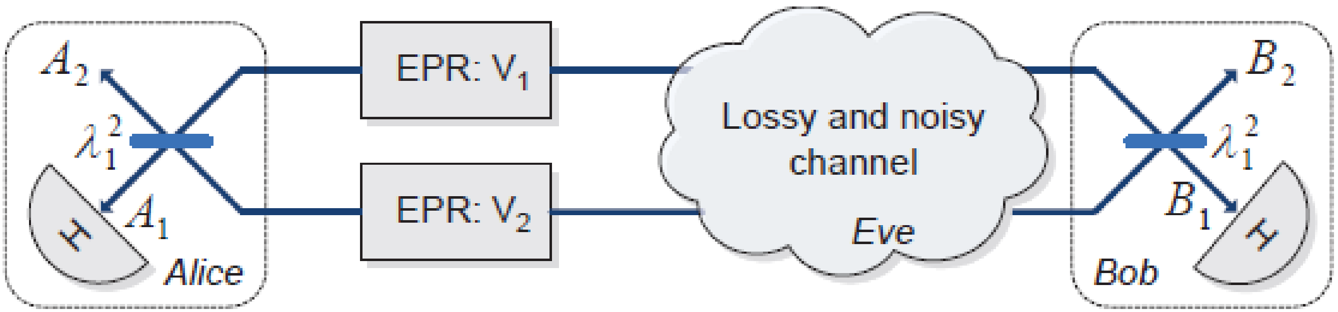
Purification of 2-mode scheme.

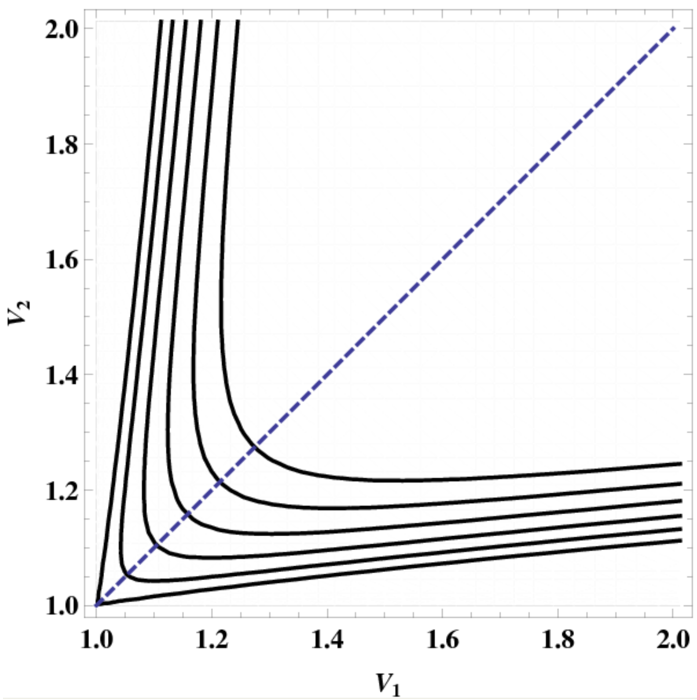
In particular, security can be restored for any number of unoccupied modes.

For unlimited state variance: $K^{(2)} = \frac{1}{2}\log\left[(1-T/2)/(1-T)\right]$

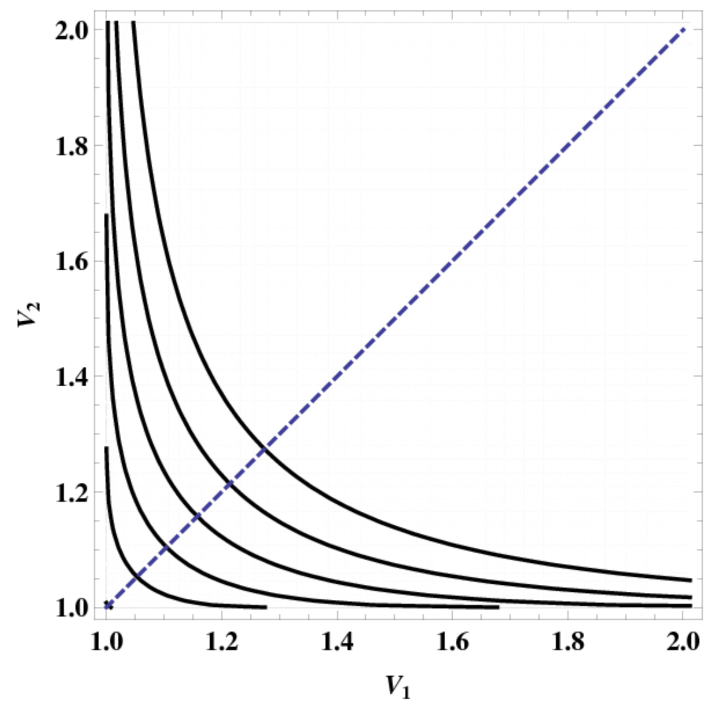
is always positive, though less than $K^{(1)} = \log\left[1/(1-T)\right]$

Unbalanced multimode sources



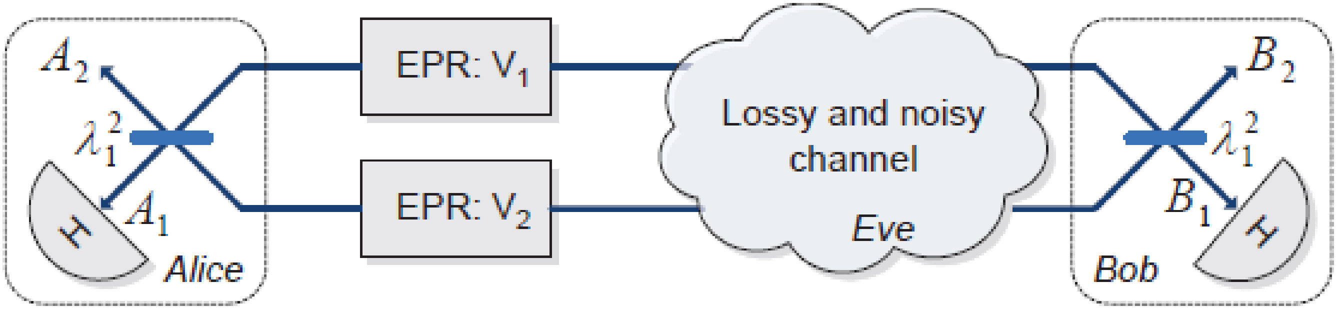


Untrusted



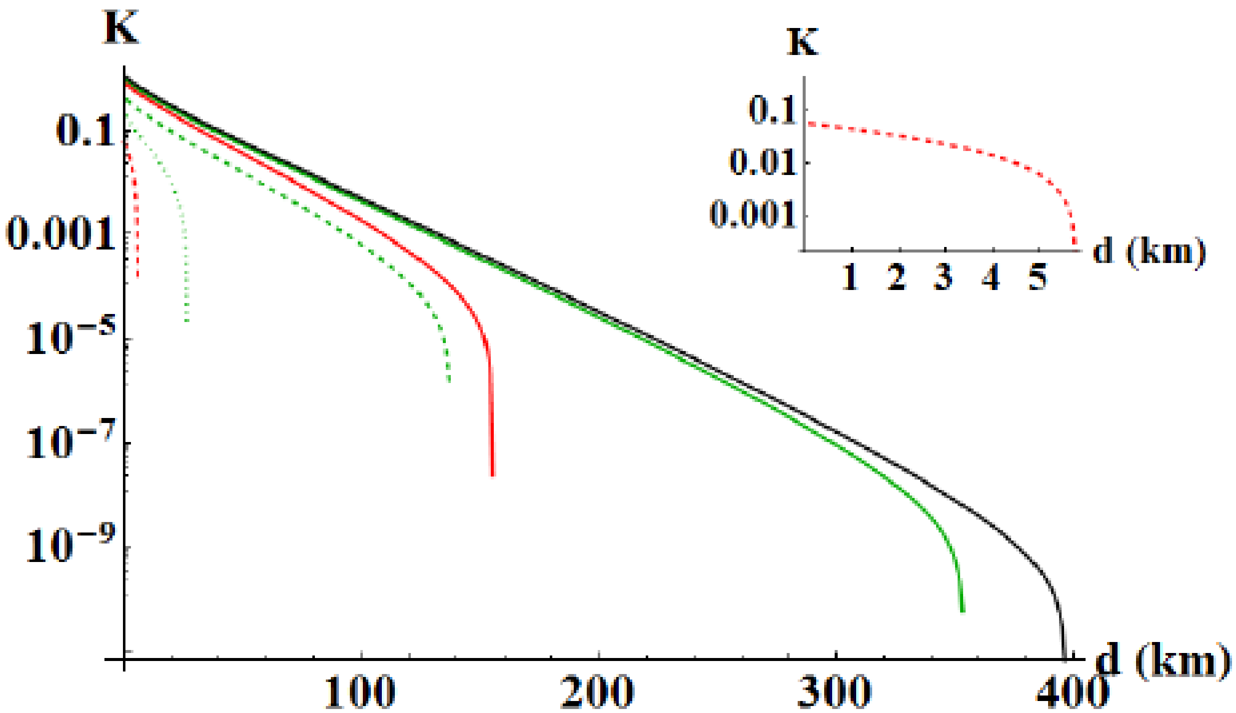
Trusted

Mode selection in homodyne detection



Unbalanced multimode homodyne VS unbalanced source

Mode selection in homodyne detection



Green: trusted multimode detection, **red**: untrusted, **black** line – coherent-states protocol, $V_1 = 3, \varepsilon = 5\% SNU, \beta = 95\%$

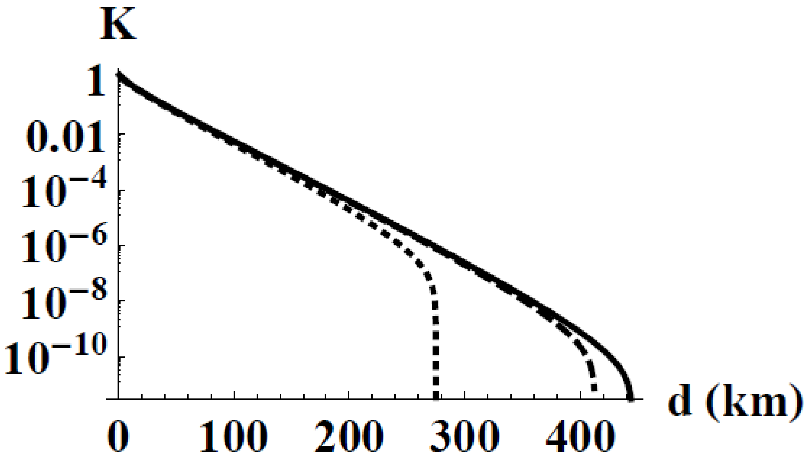
$V_2 = 1,$ balanced detection (dotted lines)

$V_2 = 1.1,$ balanced detection (dashed lines)

$V_2 = 1, \lambda_1^2 = 0.95$ (solid lines)

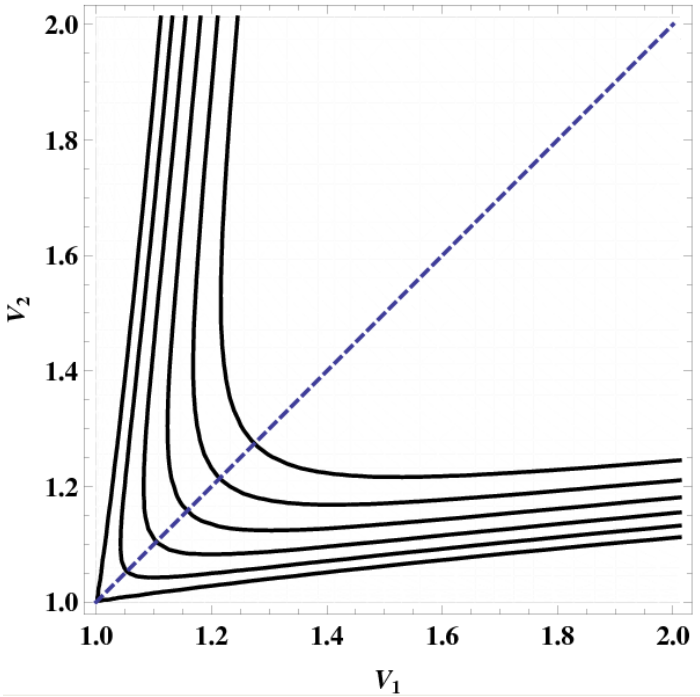
Limited knowledge of multimode structure

	3-mode (reality)	2-mode (limited knowledge)	1-mode ("ignorant" approach)
Setup parameters	$V_1 = 5,\ \lambda_1^2 = 95\%$ $V_2 = 1.5,\ \lambda_2^2 = 2.5\%$ $V_3 = 1.1,\ \lambda_3^2 = 2.5\%$	$V_1^{(2)} = 5,\ \lambda_1^2 = 95\%$ $V_2^{(2)} = 1.3,\ \lambda_2^2 = 5\%$	$V_1^{(1)} = 4.815$
Channel parameters	T $\epsilon = 0.05$	$T^{(2)} \approx 0.999 \cdot T$ $\epsilon^{(2)} \approx 0.0535$	$T^{(1)} \approx 0.993 \cdot T$ $\epsilon^{(1)} \approx 0.0773$

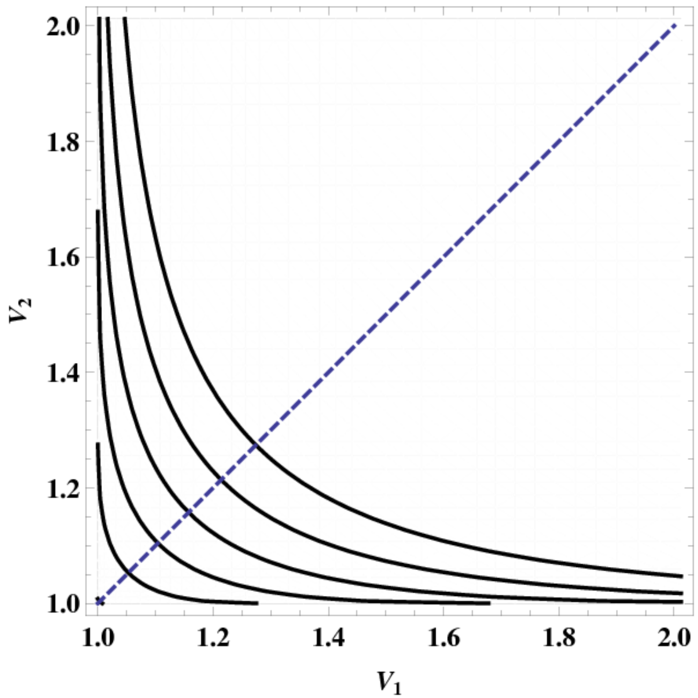


Key rate in the case 1 (solid line), 2 (dashed line) and 3 (dotted line).

Symmetrization of source modes



Untrusted



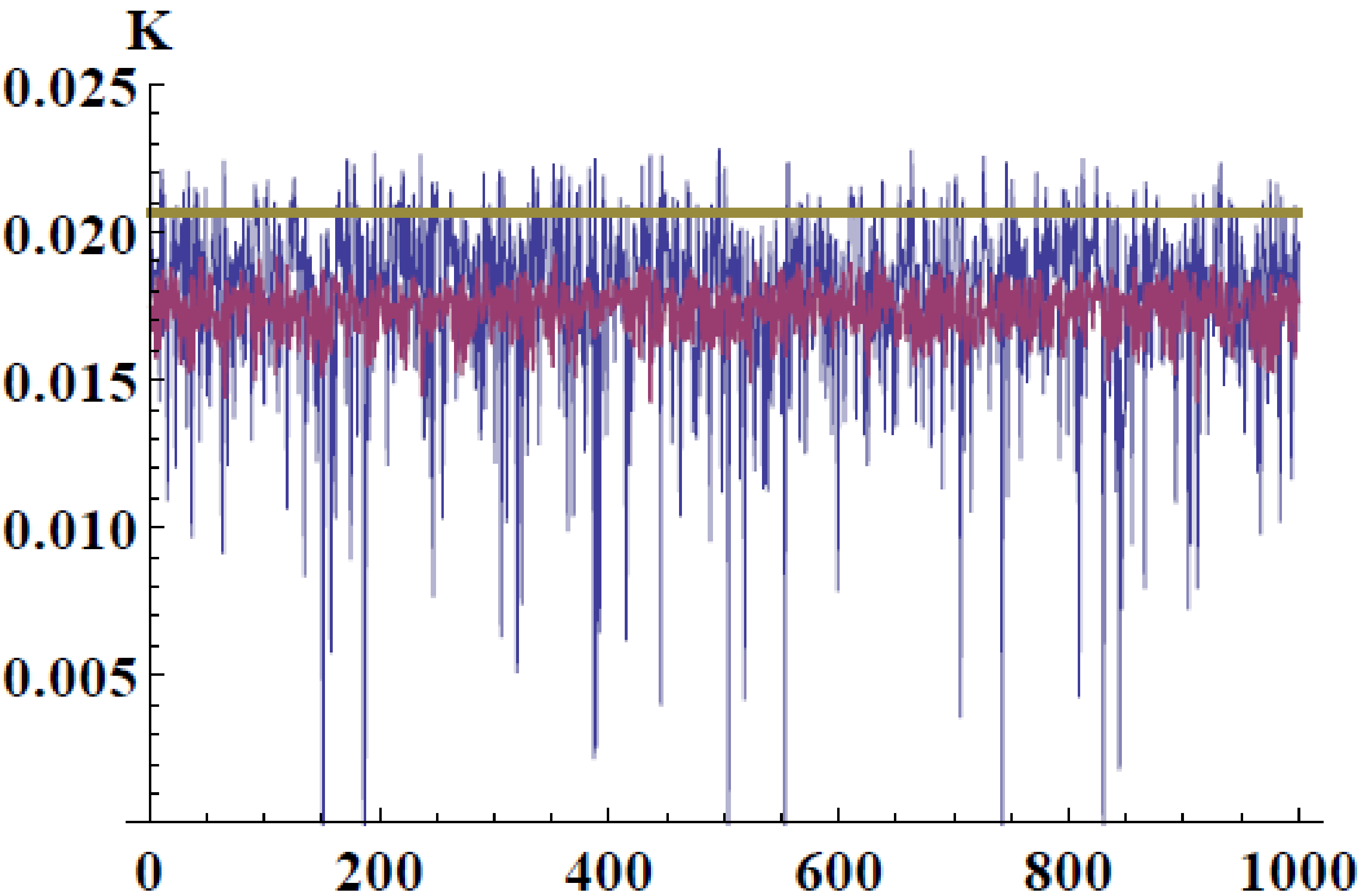
Trusted

Perfect source balancing: restores single-mode scenario;

The difference between trusted/untrusted case vanishes.

Security stabilization

If modes remain asymmetrical, key rate is reduced.
If modes fluctuate in addition, the key rate can drop below 0.
However, key rate is stabilized when number of modes increases:



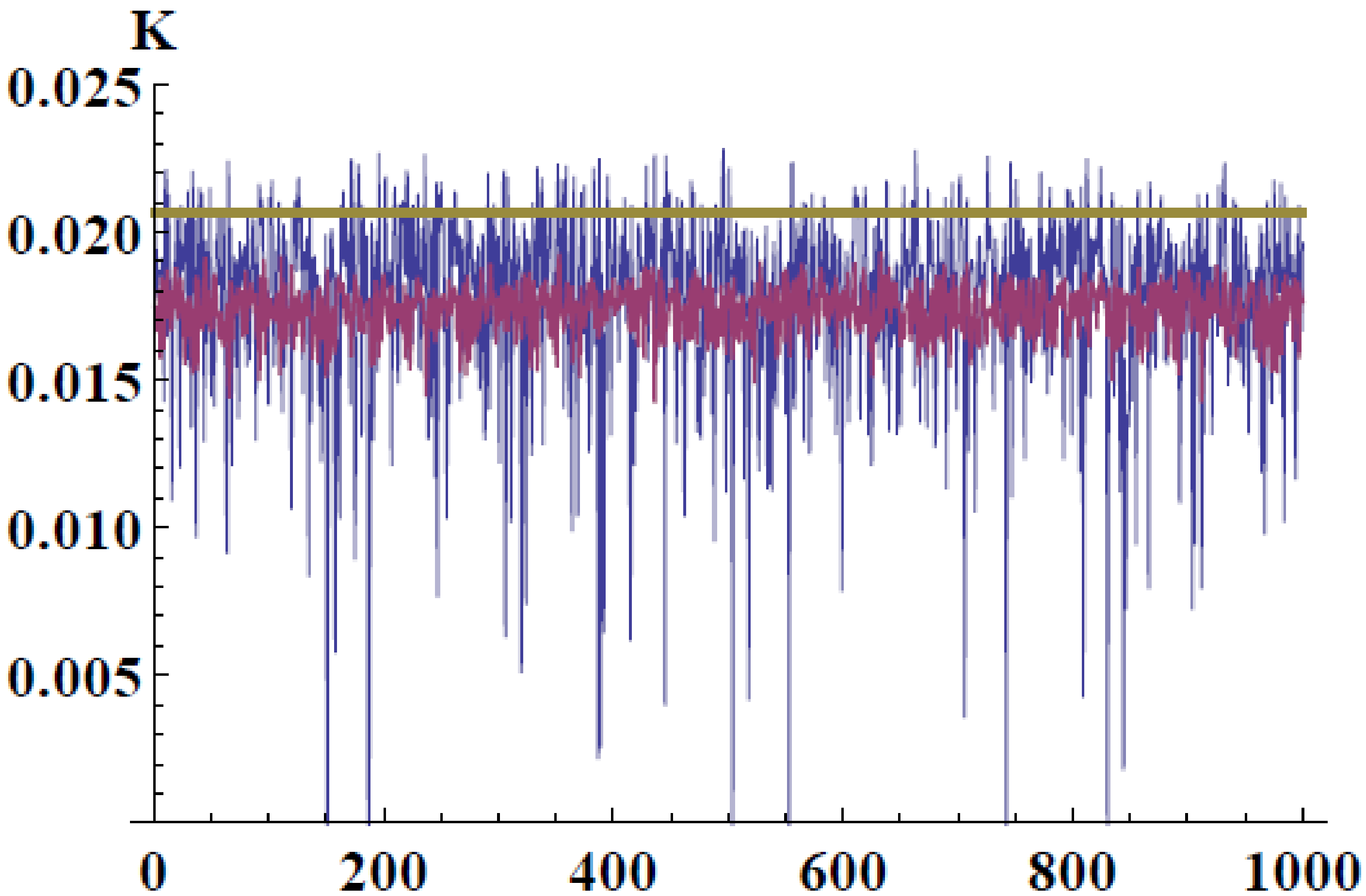
V~N(5,0.5):
N=5 (blue)
N=100 (purple)

V=5 (yellow)

T=0.03 (~70km)
3% chan. noise
95% effic.

Security stabilization

Perspective application for bright twin-beam states
[Iskhakov, Chekhova, Leuchs, PRL 102, 183602 (2009)]



V~N(5,0.5):
N=5 (blue)
N=100 (purple)

V=5 (yellow)

T=0.03 (~70km)
3% chan. noise
95% effic.

Summary

- Multimode effects must be carefully considered in any real-life implementation of CV QKD

- Knowledge of the mode structure improves the security analysis

- Mode selection in detector can be helpful, but should be precise

- Symmetrization of source modes restores single-mode scenario

- Increased number of modes stabilizes the key rate in case of energy fluctuations within the modes.

Acknowledgements

SEVENTH FRAMEWORK PROGRAMME

Thank you for attention!

usenko@optics.upol.cz