

Towards continuous-variable quantum key distribution with macroscopic states of light

Vladyslav C. Usenko, Laszlo Ruppert, Radim Filip



Department of Optics, Palacký University,
Olomouc, Czech Republic

Outline

- Continuous-variable quantum key distribution
- Multimode effects in CV QKD
- Role of brightness and mode mismatch
- 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:

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

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

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

Continuous-variable states

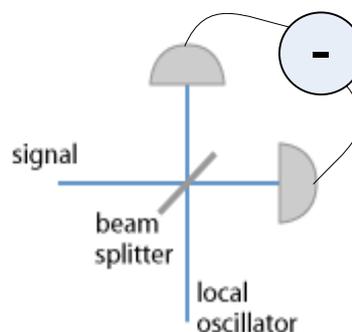
Field quadratures: analogue of the position and momentum operators of a particle:

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

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

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

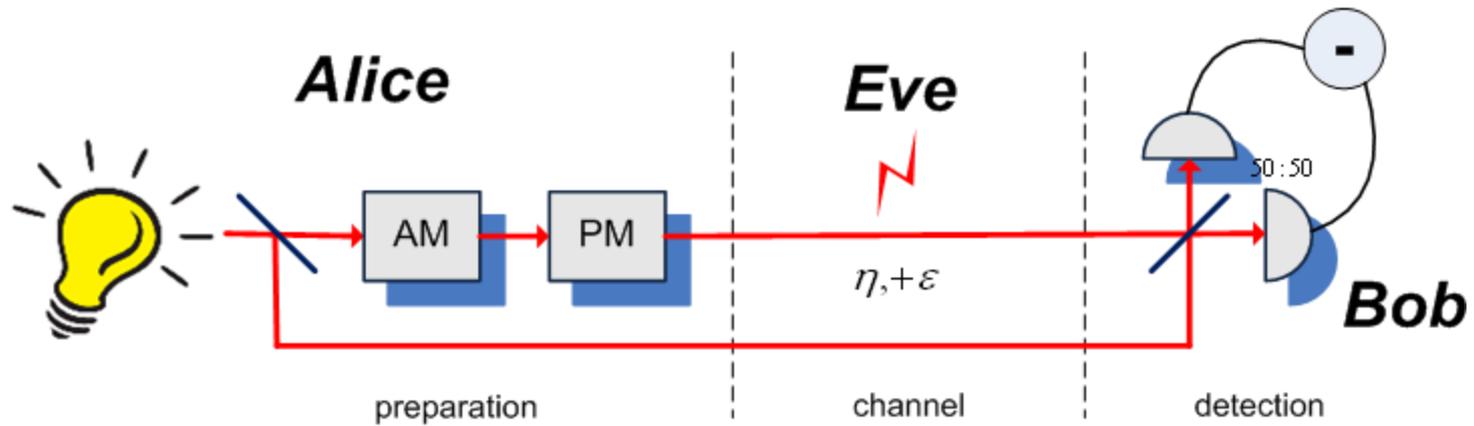
$$\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$$

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

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

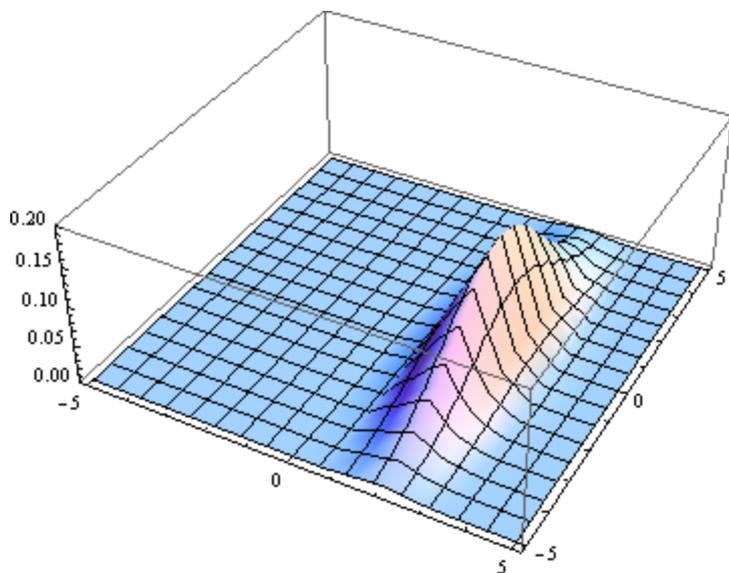
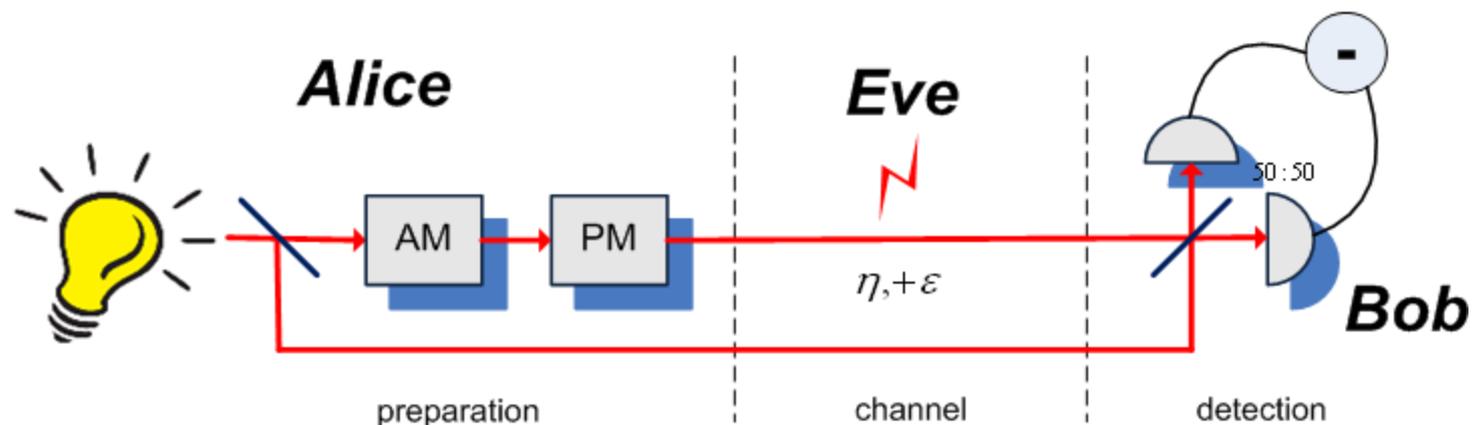
Bosonic commutation relations: $[\hat{r}_k, \hat{r}_l] = i\Omega_{kl}$

CV Quantum Key Distribution



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

CV Quantum Key Distribution

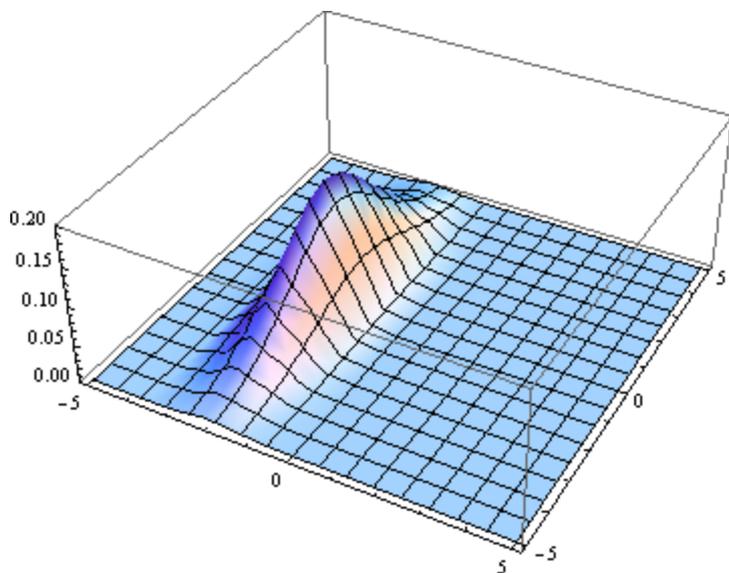
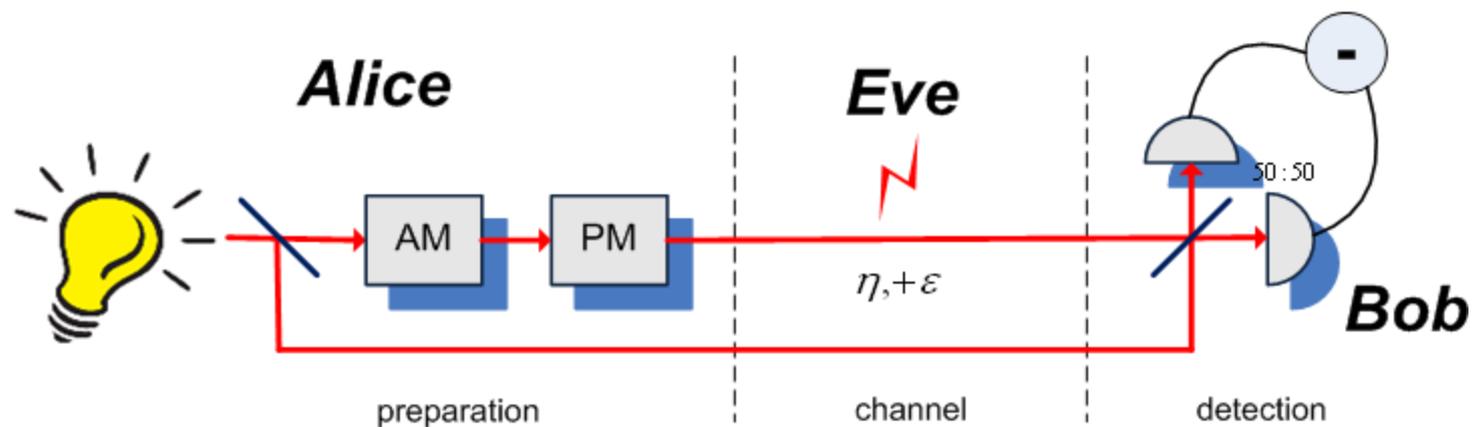


Squeezed states-based protocol:

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

- Alice generates a Gaussian random variable \mathbf{a}
- Alice prepares a squeezed state, displaced by \mathbf{a}
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

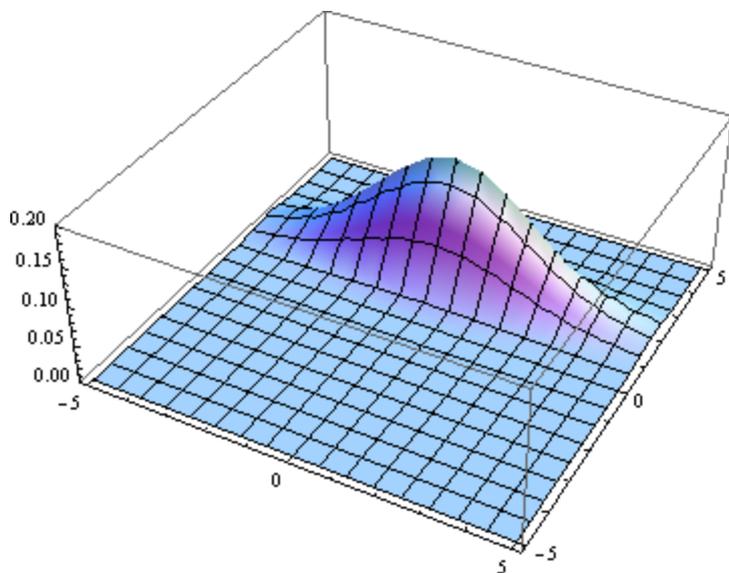
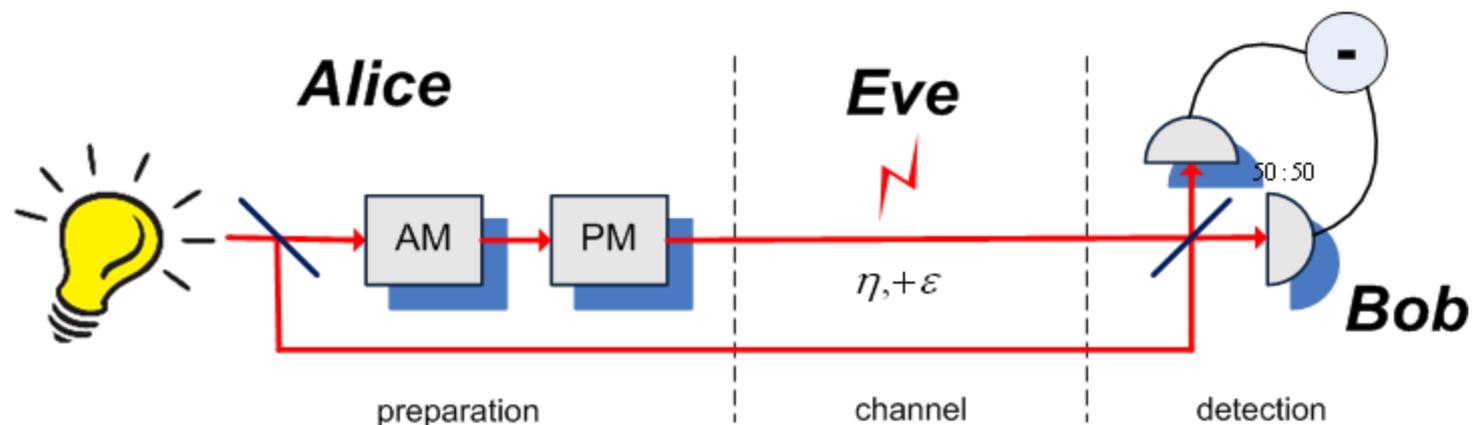


Squeezed states-based protocol:

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

- Alice generates a Gaussian random variable \mathbf{a}
- Alice prepares a squeezed state, displaced by \mathbf{a}
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

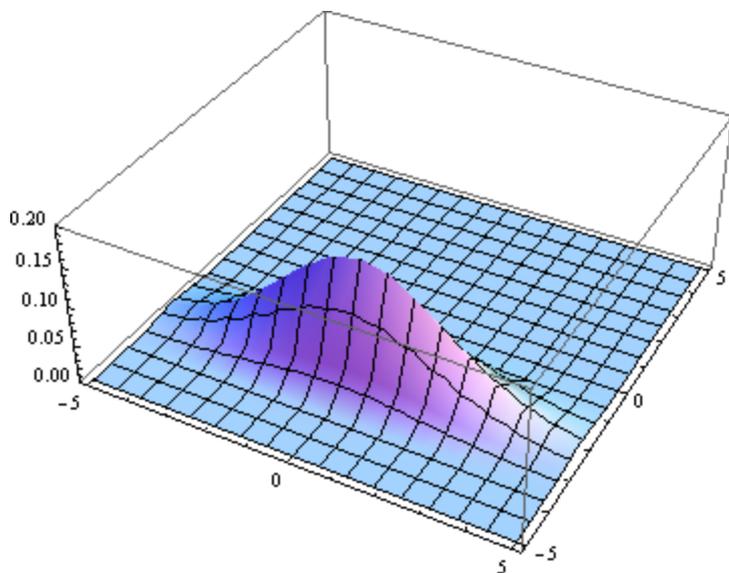
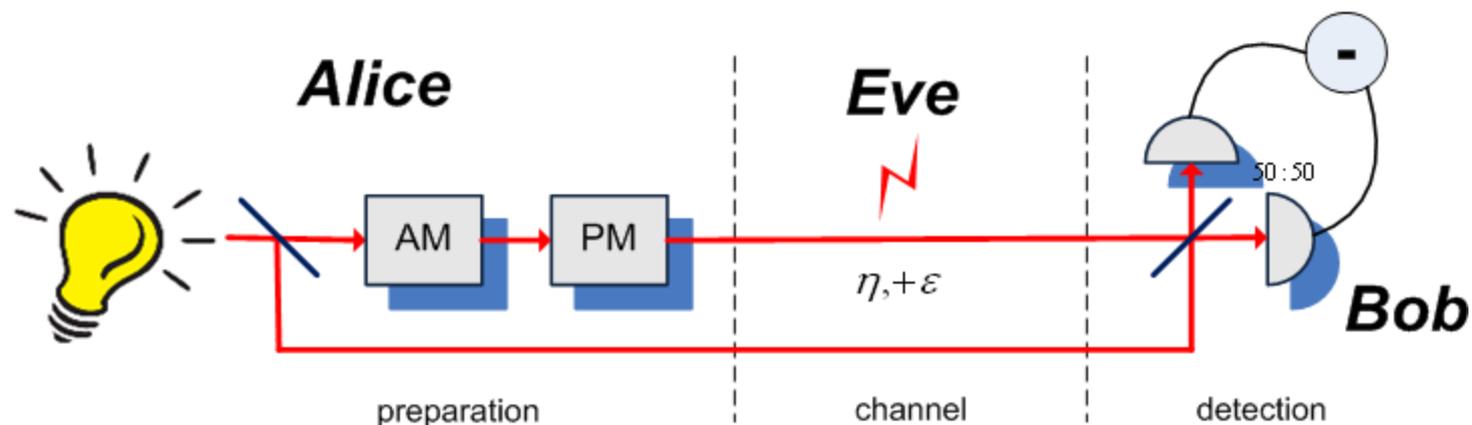


Squeezed states-based protocol:

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

- Alice generates a Gaussian random variable \mathbf{a}
- Alice prepares a squeezed state, displaced by \mathbf{a}
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution

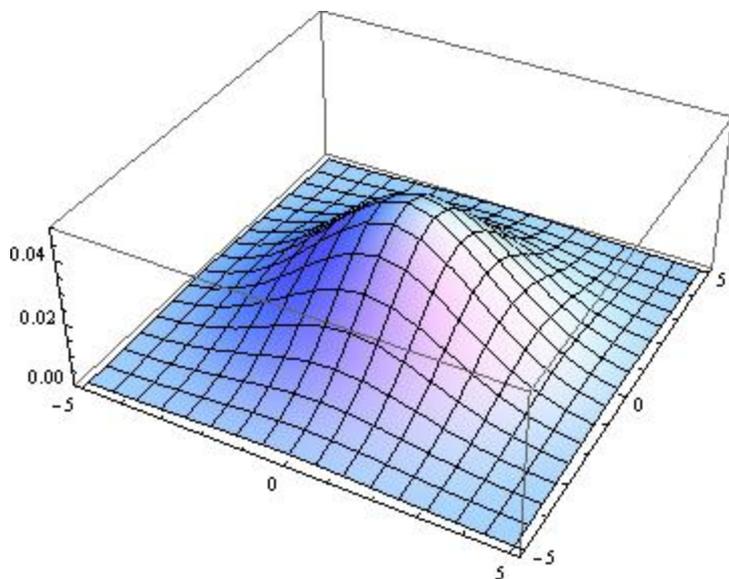
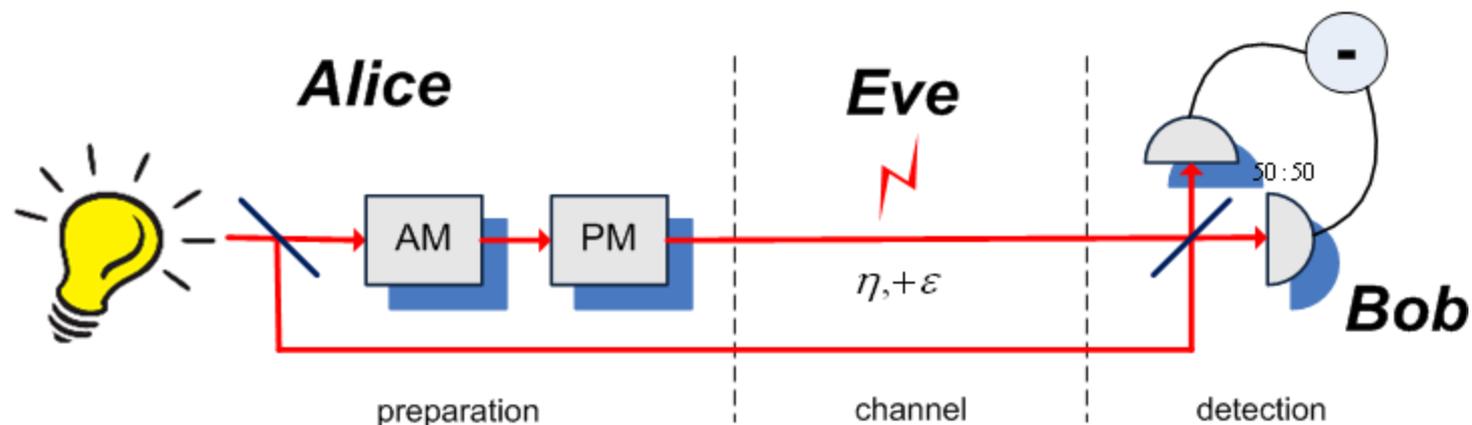


Squeezed states-based protocol:

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

- Alice generates a Gaussian random variable \mathbf{a}
- Alice prepares a squeezed state, displaced by \mathbf{a}
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution



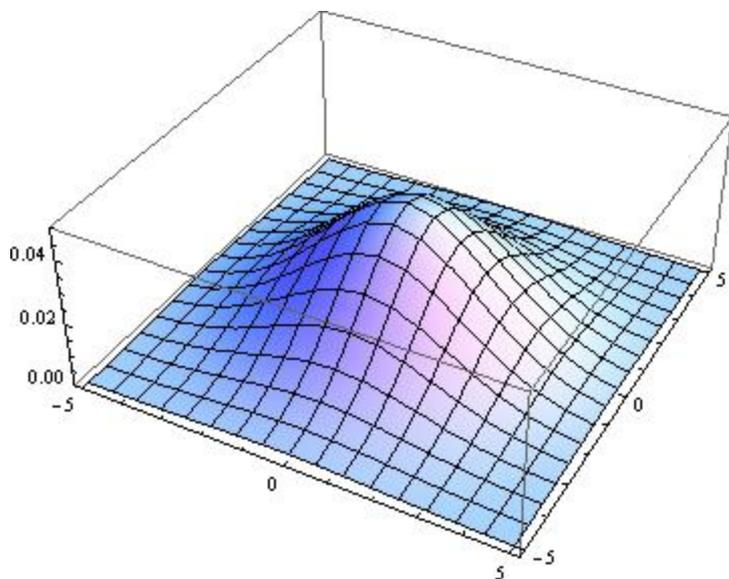
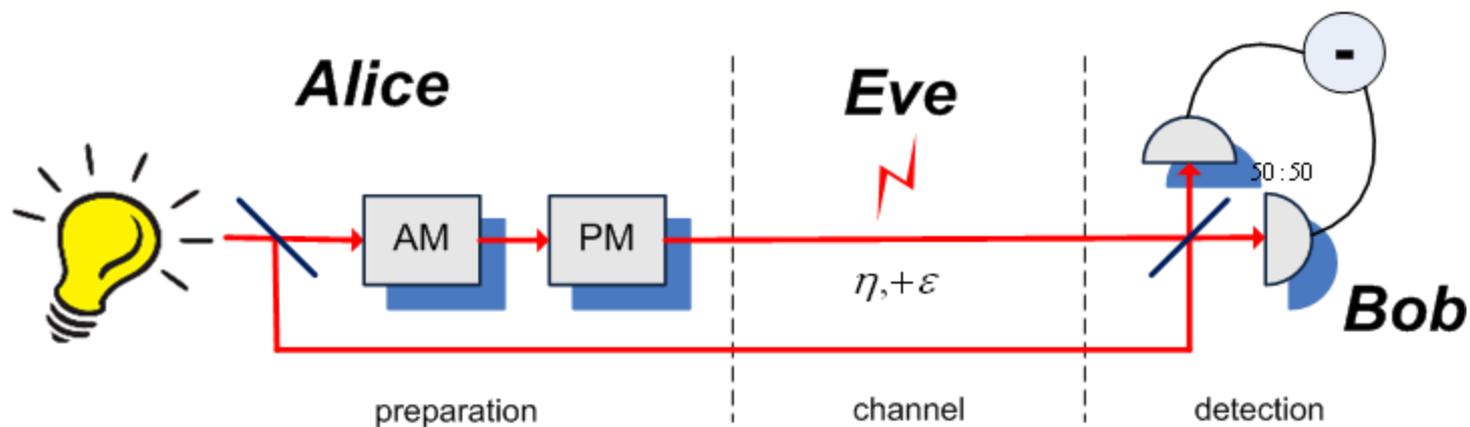
Mixture

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 \mathbf{a}
- Alice prepares a squeezed state, displaced by \mathbf{a}
- Bob measures a quadrature
- Bases reconciliation
- Error correction, privacy amplification

CV Quantum Key Distribution



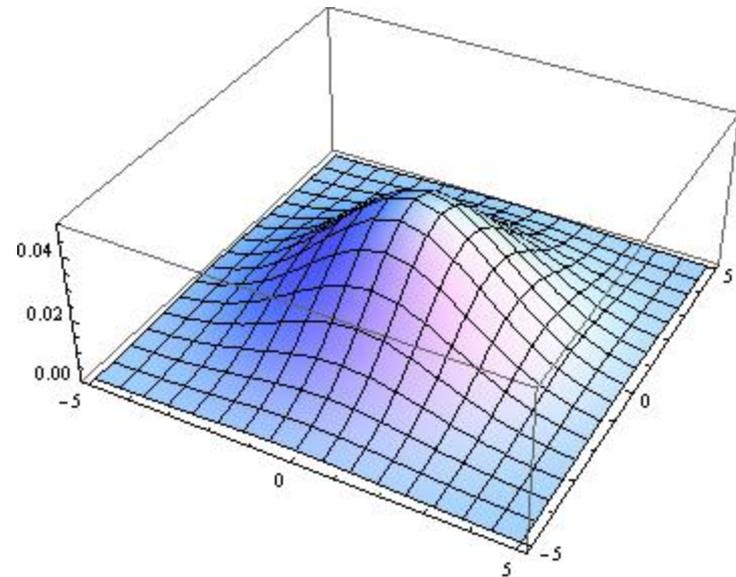
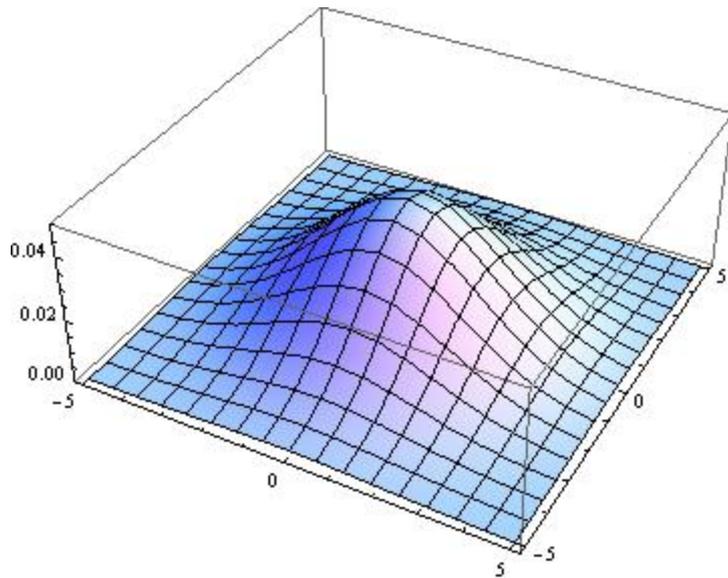
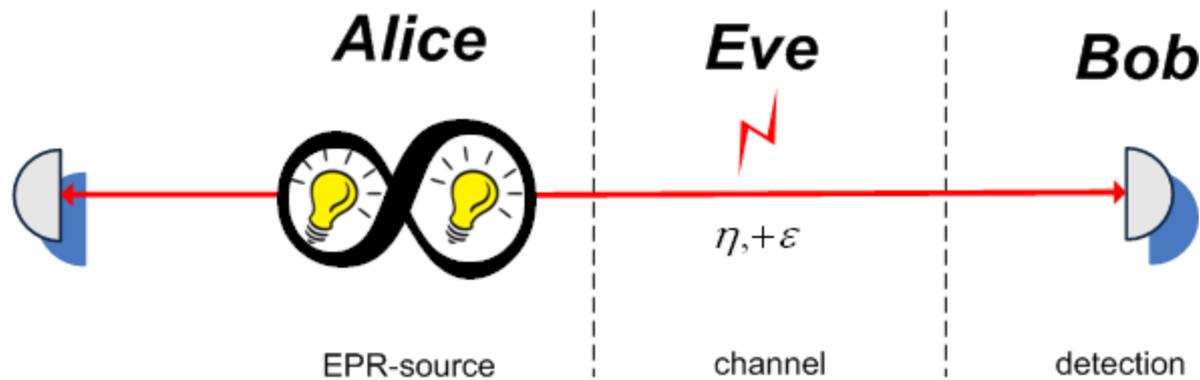
Mixture

Alternatively: coherent states-based protocol:

Laser source, modulation

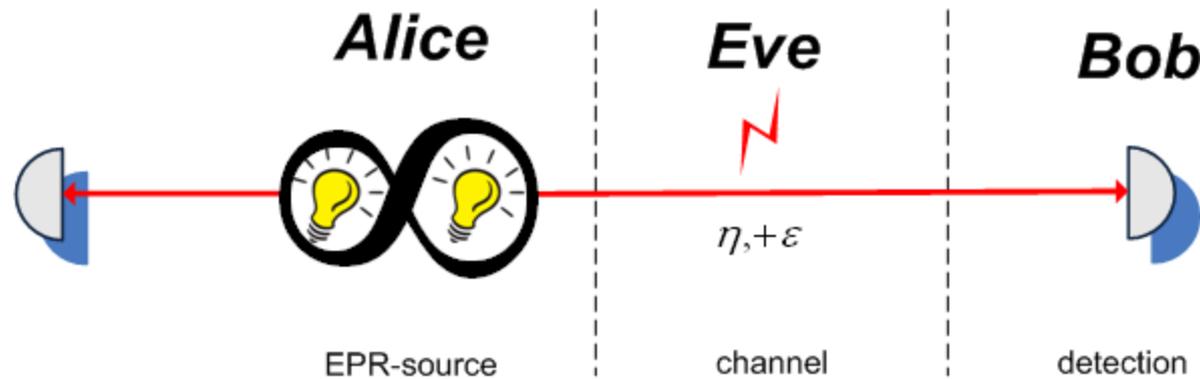
F. Grosshans and P. Grangier. PRL 88, 057902 (2002); F. Grosshans et al., Nature 421, 238 (2003)

CV QKD: entangled-based

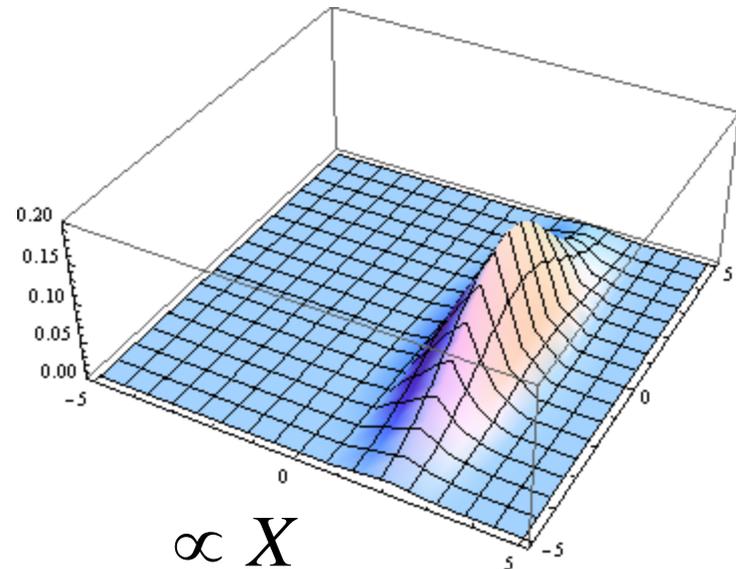


Two-mode squeezed vacuum: Before measurement

CV QKD: entangled-based



X



Two-mode squeezed vacuum: after homodyne measurement

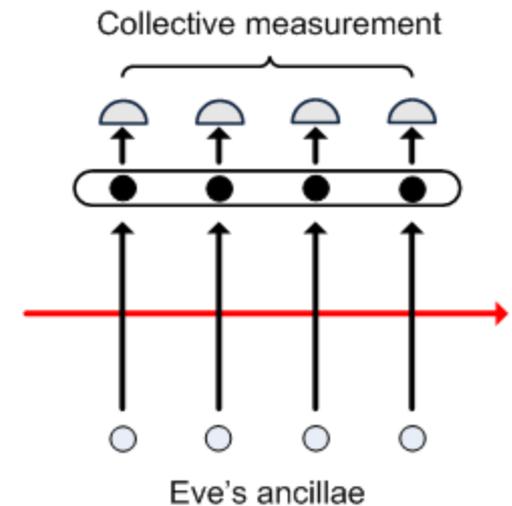
CV QKD: security

Collective attacks:

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

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

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



$$S(\rho) = -\text{Tr} \rho \log \rho$$

CV QKD: security

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

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

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:

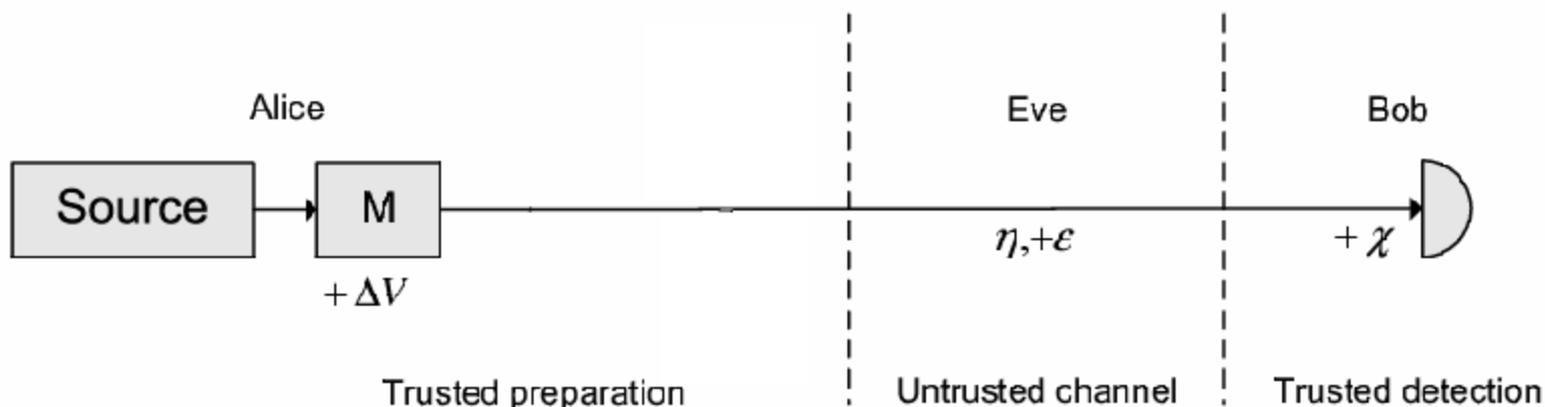
$$\gamma_E^{x_B} = \gamma_E - \sigma_{BE} (X \gamma_B X)^{MP} \sigma_{BE}^T$$

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

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

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)

CV QKD with macroscopic states?

PROS

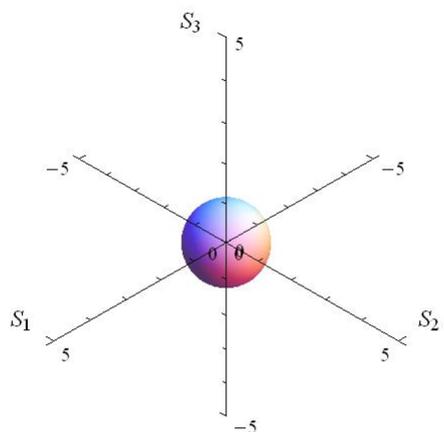
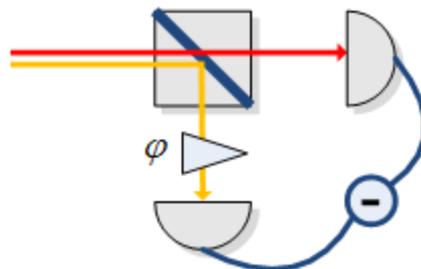
- Potentially visible light, relatively easy to manipulate
- Strong nonclassicality, potentially more robust
- Conceptually interesting

CONS

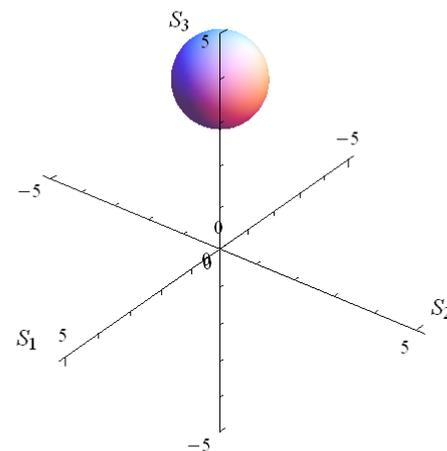
- Heavily multimode
- High brightness

CV QKD with macroscopic states?

Covariance matrix needed!



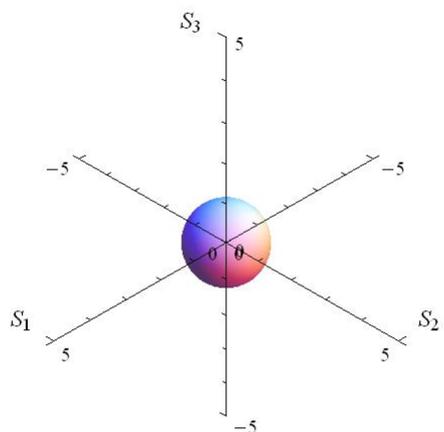
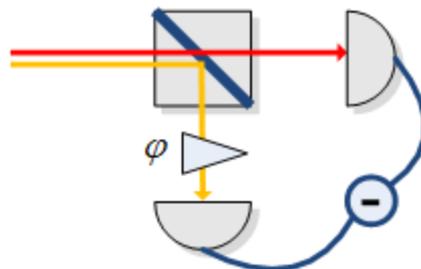
Stokes measurement



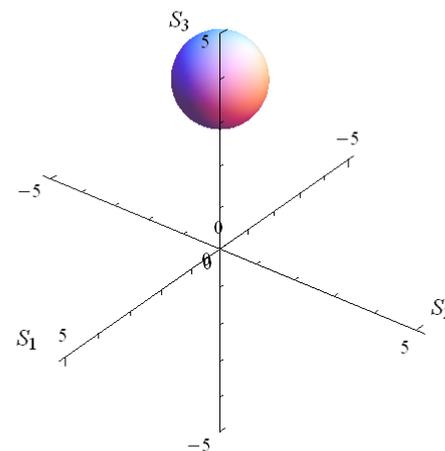
Homodyne measurement

CV QKD with macroscopic states?

Covariance matrix needed!



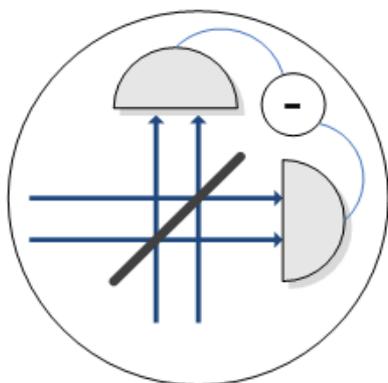
Stokes measurement



Homodyne measurement

this talk

Multimode homodyne detection



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

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 $V_0^{(N)} = \sum_{n=1}^N |g_n \alpha_n|^2$.

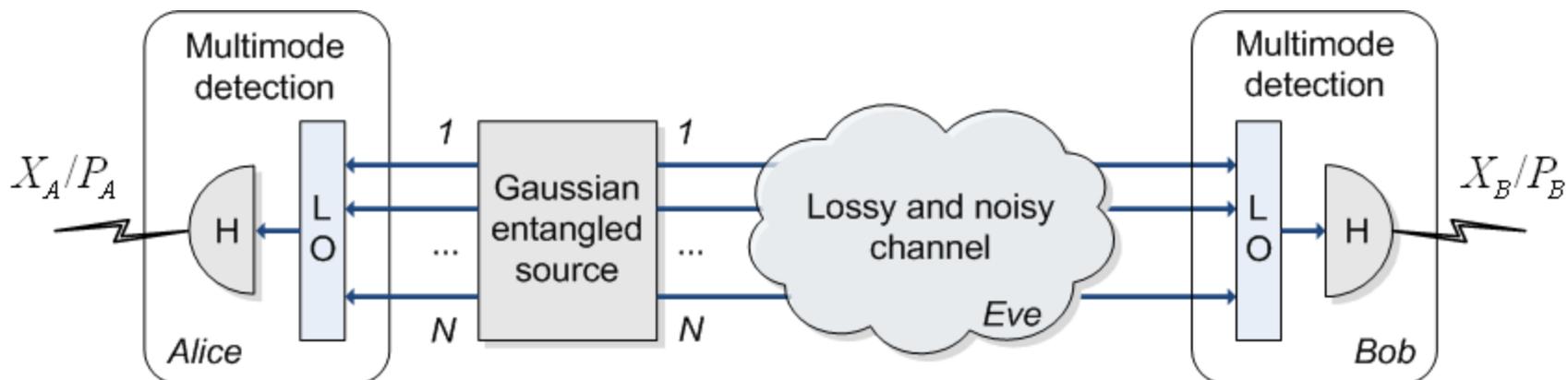
After normalization of photo-current: $X^{(N)}(\theta) = \frac{\sum_{n=1}^N G_n \tilde{X}_n(\theta)}{\sqrt{\sum_{n=1}^N G_n^2}}$

Normalization coefficients $\lambda_i = G_i / \sqrt{\sum_{n=1}^N G_n^2}$ 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 $V_0^{(N)} = NG^2$ and $X^{(N)}(\theta) = \frac{\sum_{i=1}^N \tilde{X}_i(\theta)}{\sqrt{N}}$

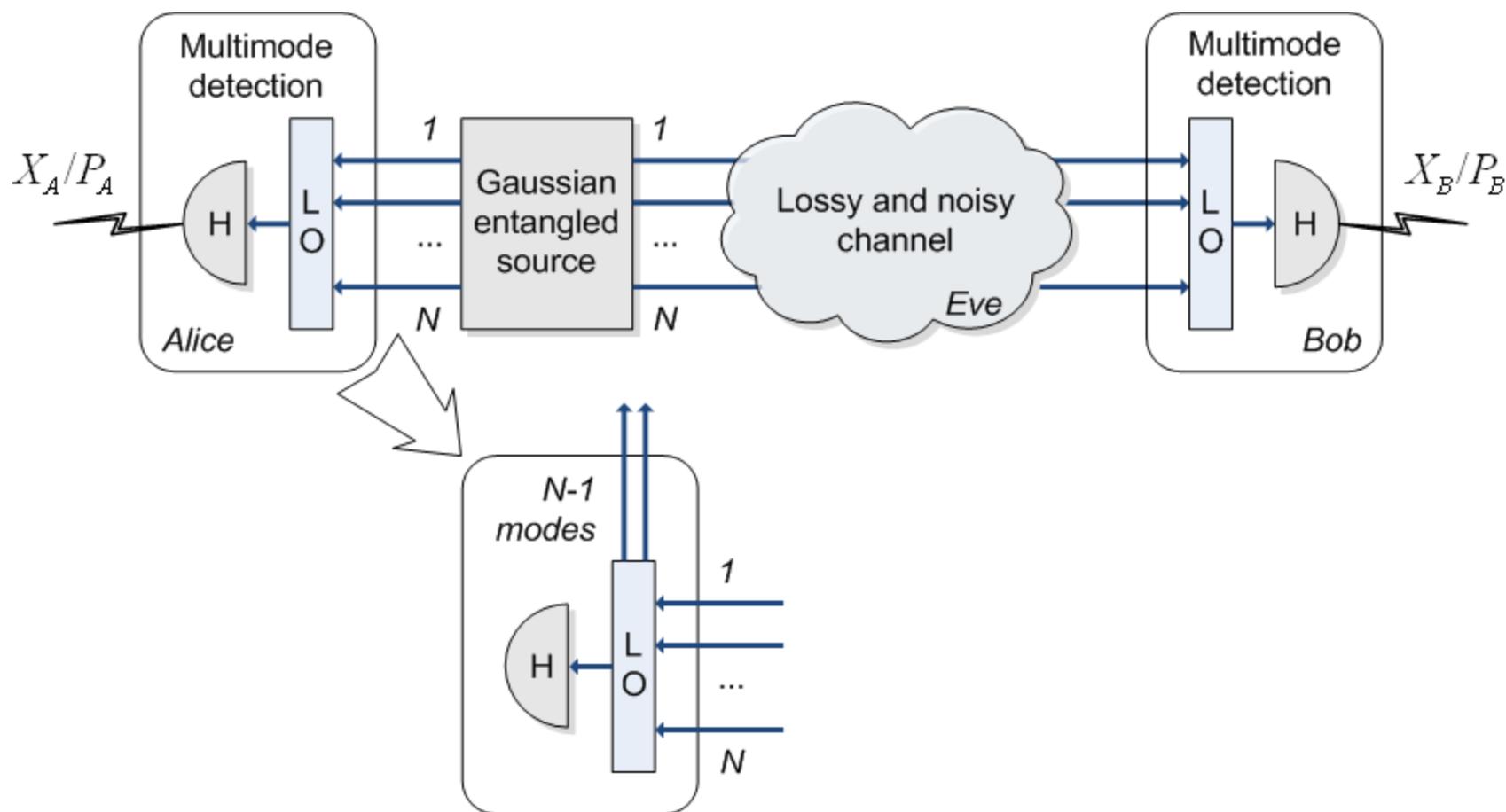
QKD with multimode states/detectors



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

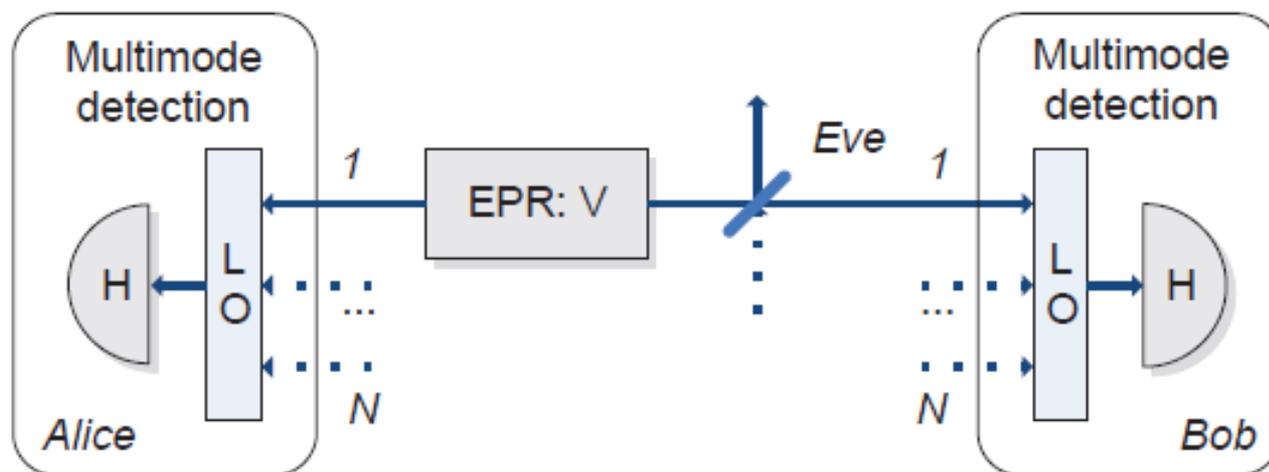


Output modes of the LO coupling before detection are available to Eve.

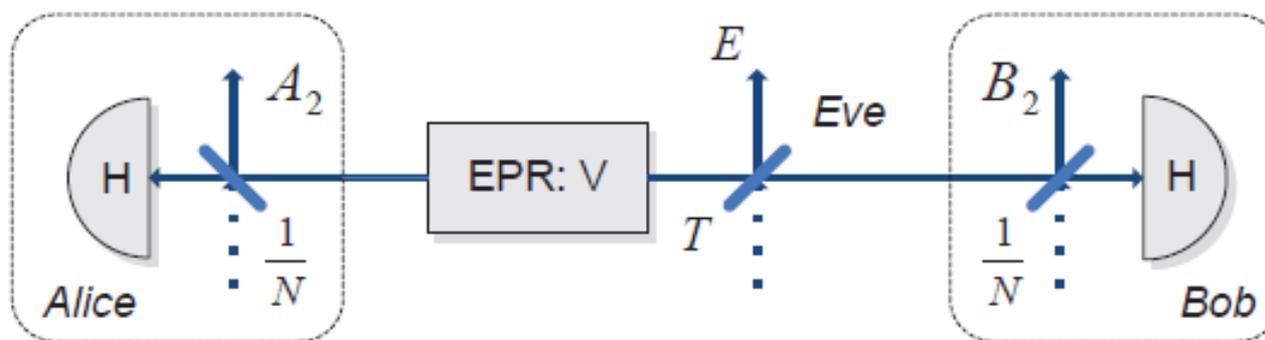
Multimode covariance matrix becomes weighted sum of single-modes ones:

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

Untrusted multimode detectors



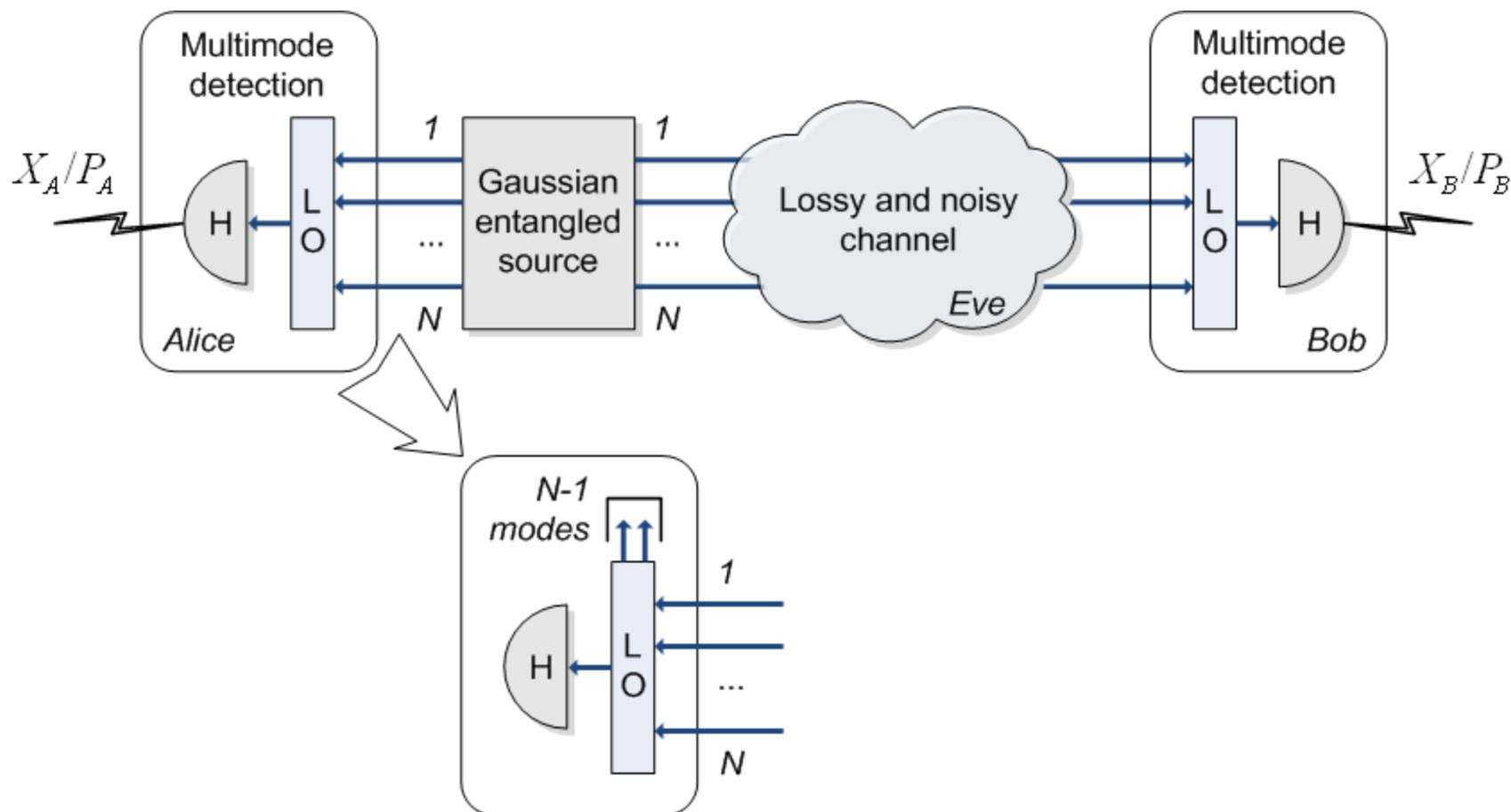
All modes, but one are in the vacuum state \rightarrow equivalent to symmetrical side-channels with untrusted outputs:



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

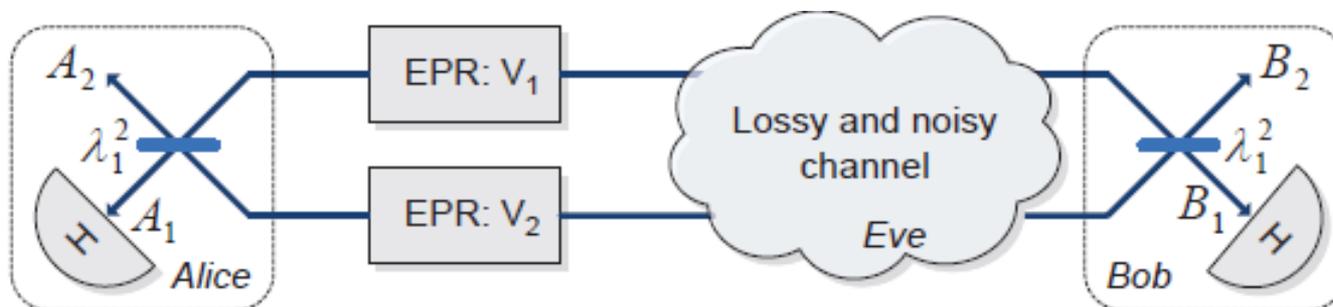
(while entanglement is preserved)

Trusted multimode detectors



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

Trusted multimode detectors



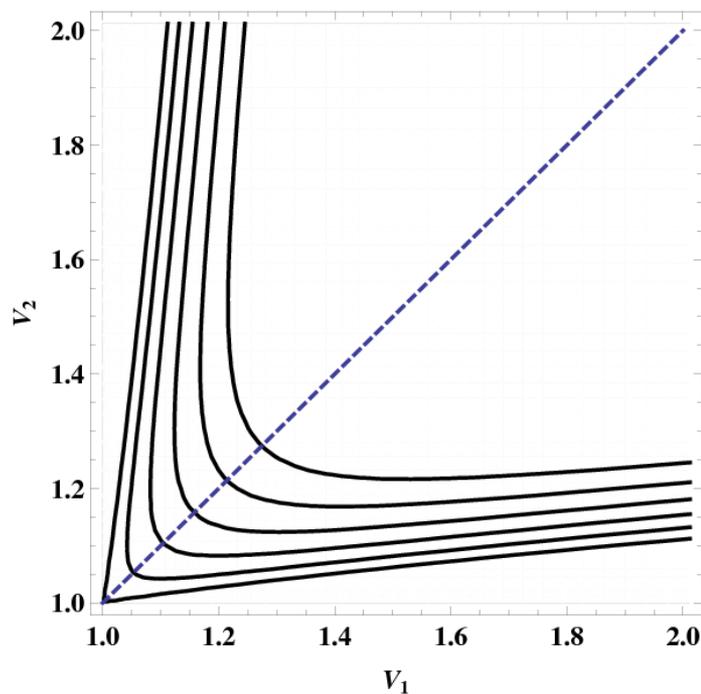
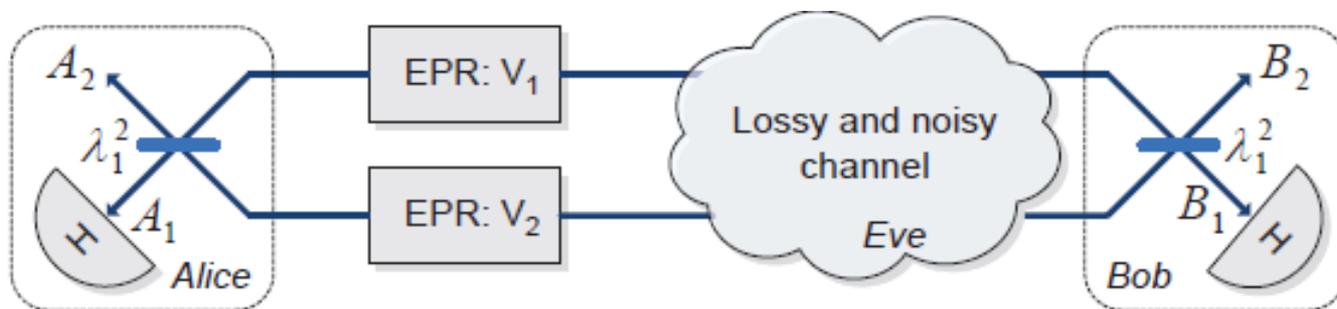
Purification of 2-mode scheme.

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

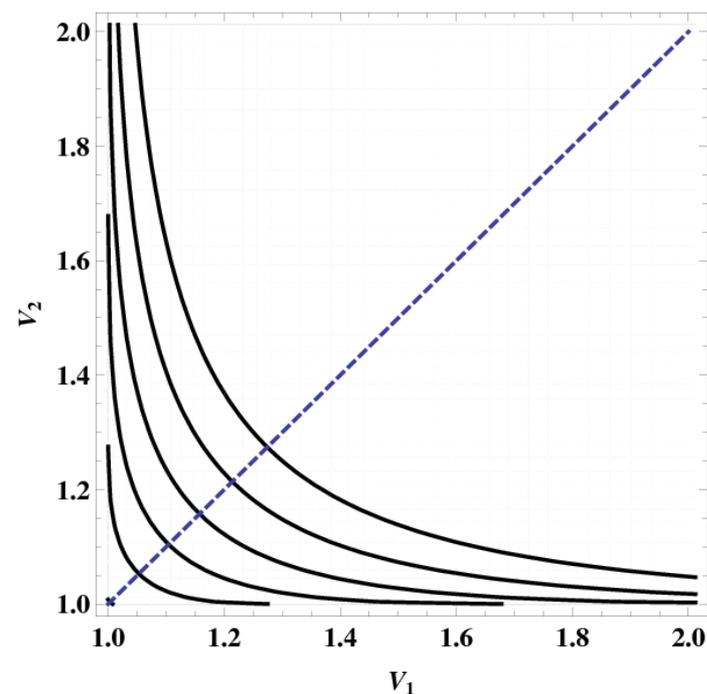
For unlimited state variance: $K^{(2)} = \frac{1}{2} \log [(1 - T/2)/(1 - T)]$

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

Unbalanced multimode sources

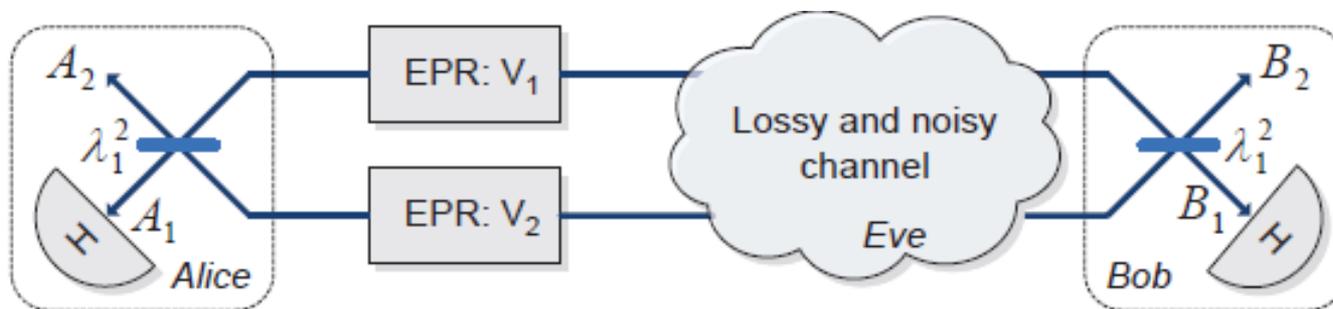


Untrusted



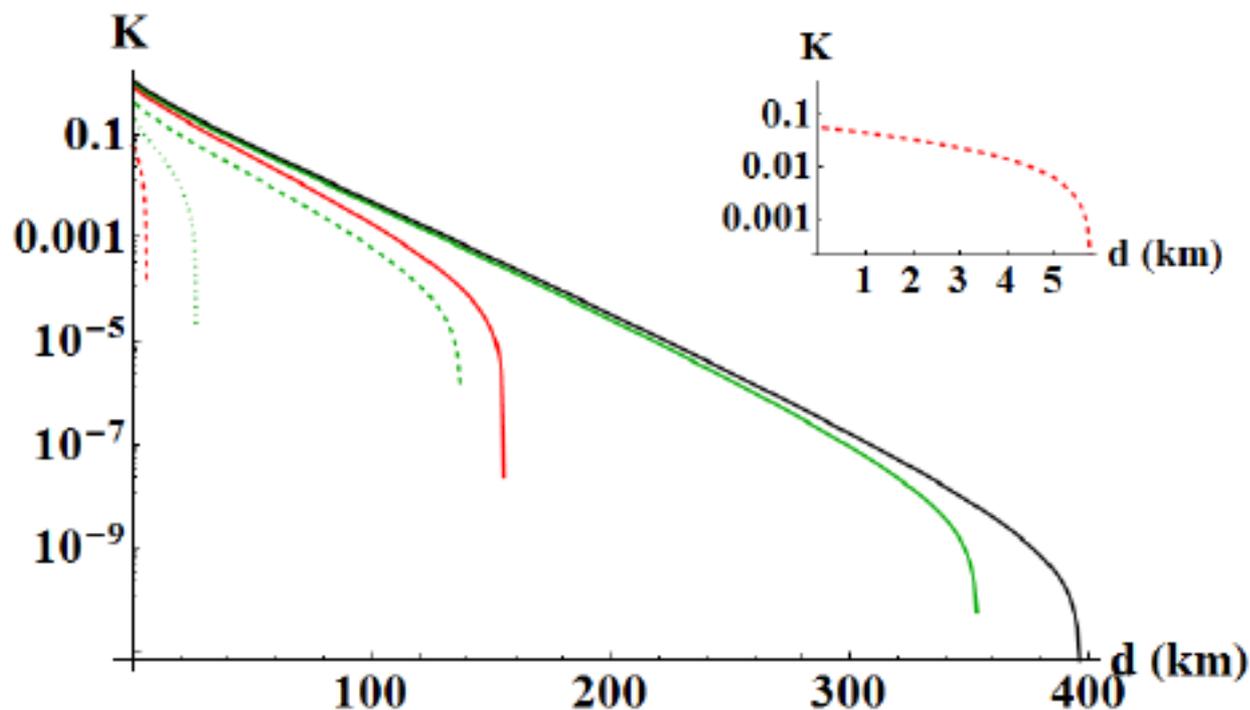
Trusted

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, $V_1 = 3, \varepsilon = 5\% \text{ SNU}, \beta = 95\%$

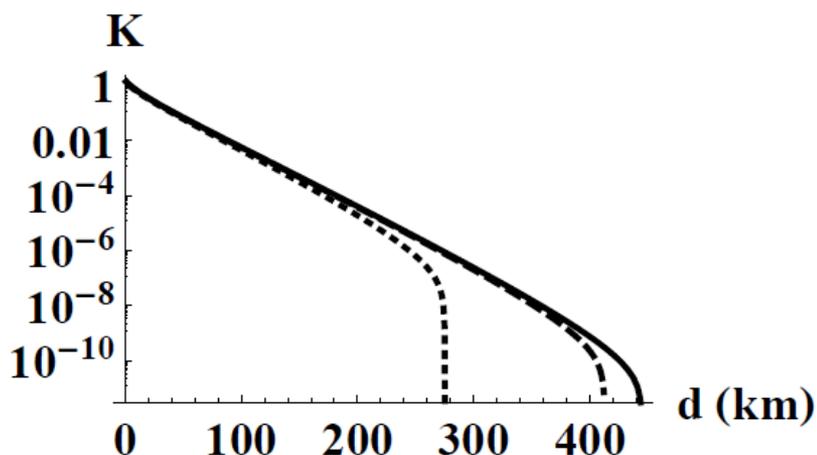
$V_2 = 1$, balanced detection (dotted lines)

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

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

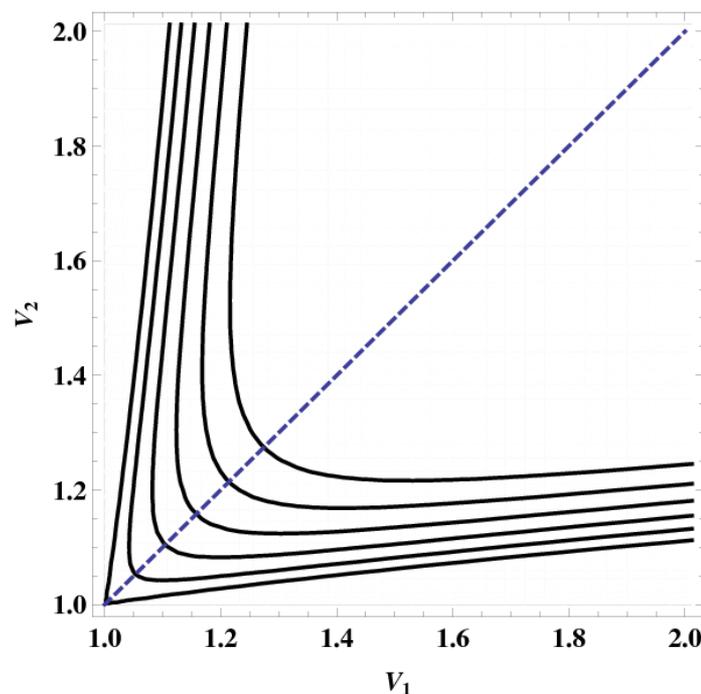
Limited knowledge of multimode structure

	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 $\epsilon = 0.05$	$T^{(2)} \approx 0.999 \cdot T$ $\epsilon^{(2)} \approx 0.0535$	$T^{(1)} \approx 0.993 \cdot T$ $\epsilon^{(1)} \approx 0.0773$

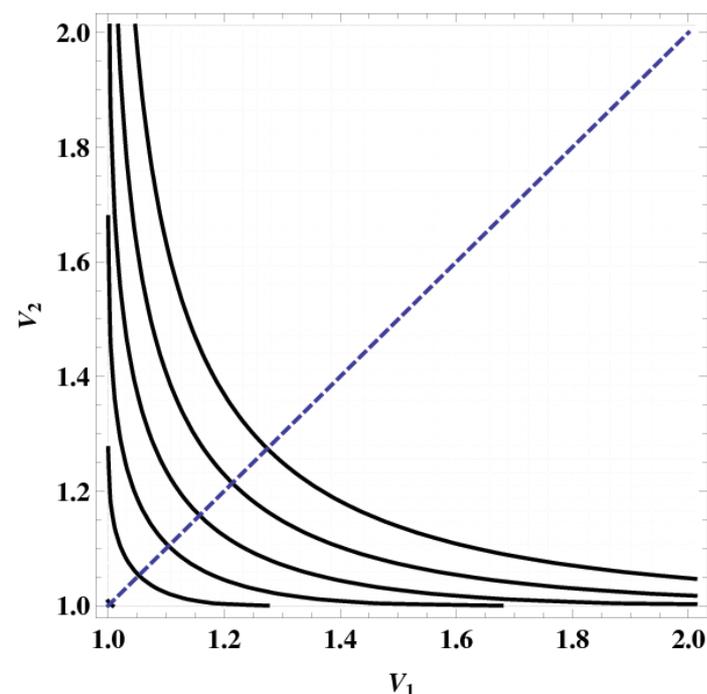


Key rate in the case 1 (solid line),
2 (dashed line) and 3 (dotted line).

Symmetrization of source modes



Untrusted



Trusted

Perfect source balancing: restores single-mode scenario;

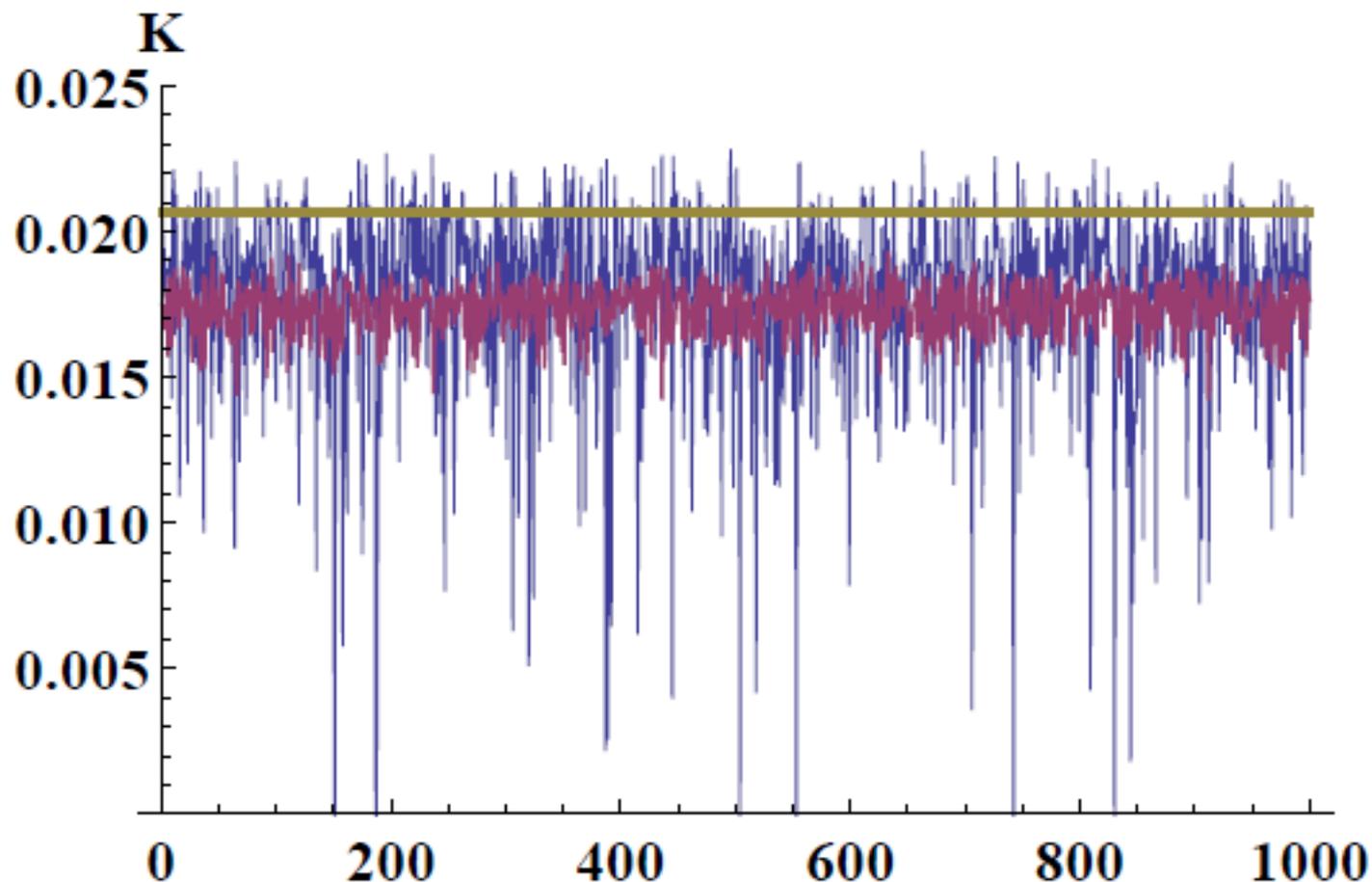
The difference between trusted/untrusted case vanishes.

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:



$V \sim N(5, 0.5)$:

$N=5$ (blue)

$N=100$ (purple)

$V=5$ (yellow)

$T=0.03$ (~ 70 km)

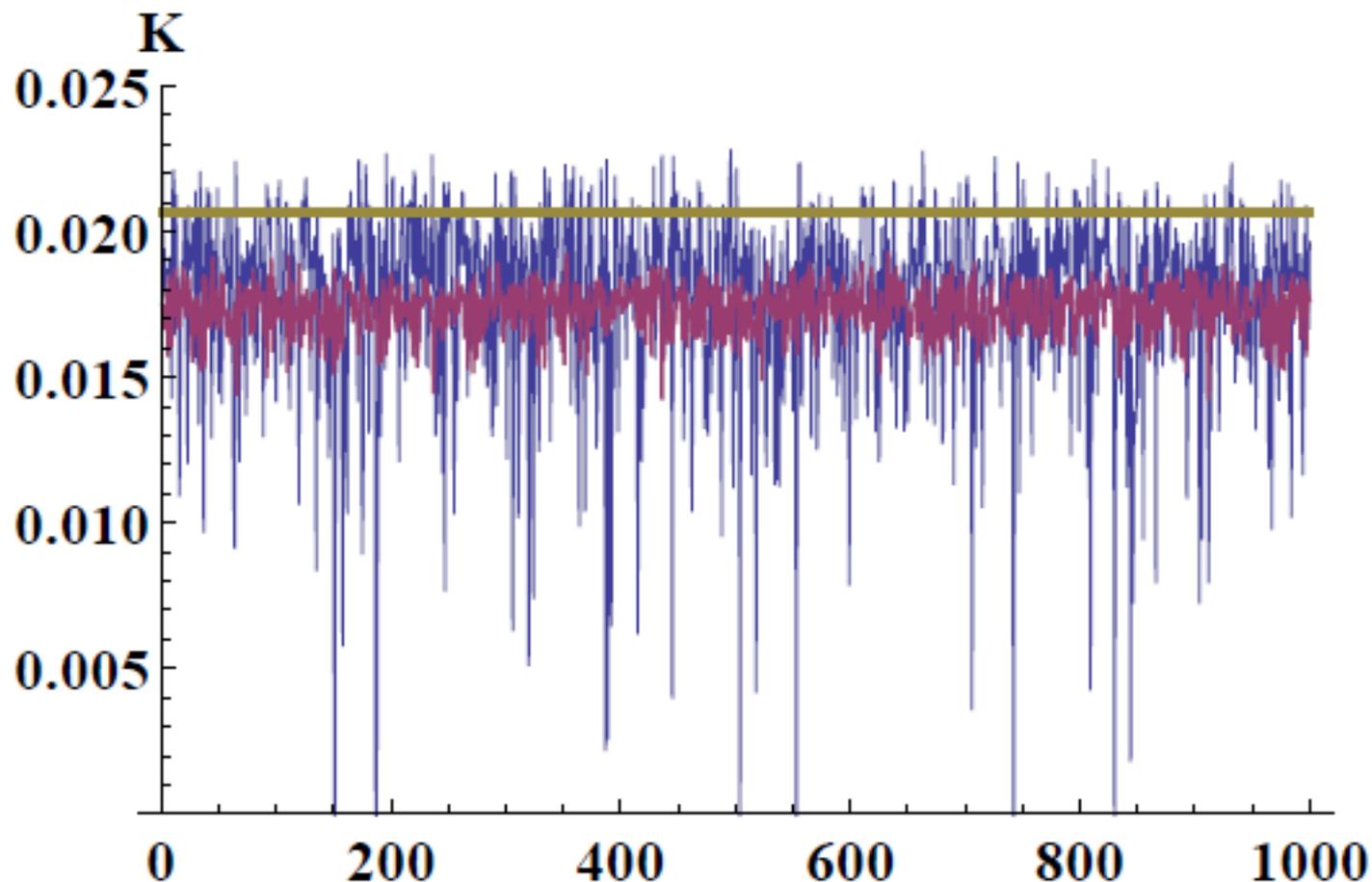
3% chan. noise

95% effic.

Security stabilization

Perspective application for bright twin-beam states

[Iskhakov, Chekhova, Leuchs, PRL 102, 183602 (2009)]



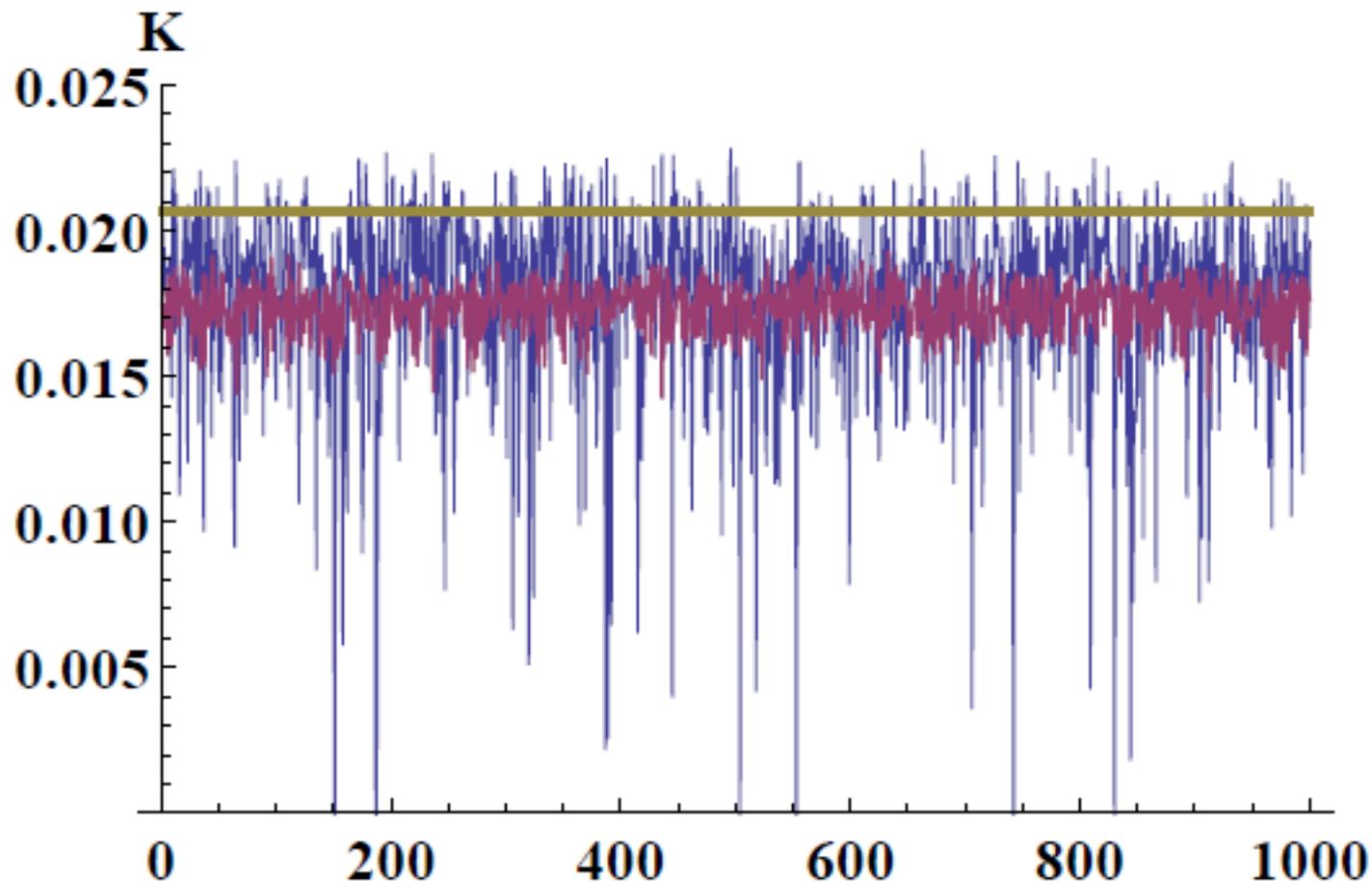
$V \sim N(5, 0.5)$:
N=5 (blue)
N=100 (purple)

V=5 (yellow)

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

Security stabilization

[VU, L. Ruppert, R. Filip, Phys. Rev. A 90, 062326 (2014)]

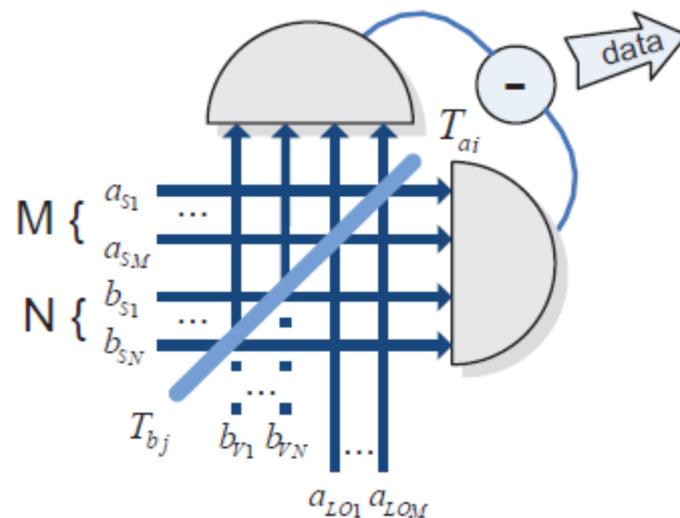


$V \sim N(5, 0.5)$:
N=5 (blue)
N=100 (purple)

V=5 (yellow)

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

Homodyning on macroscopic states



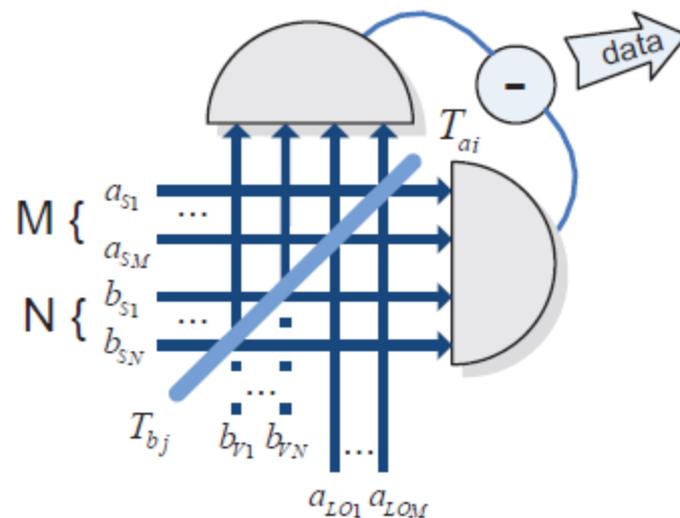
Measured photon numbers:

$$n_1 = \sum_i^M a_{S_i}^\dagger a_{S_i}' + \varepsilon \sum_j^N b_{S_j}^\dagger b_{S_j}' \quad \text{and} \quad n_2 = \sum_i^M a_{LO_i}^\dagger a_{LO_i}' + \varepsilon \sum_j^N b_{V_j}^\dagger b_{V_j}'$$

$$n_1 = \sum_i^M \left[T_{a_i} a_{S_i}^\dagger a_{S_i} + \sqrt{T_{a_i}(1-T_{a_i})} (a_{S_i}^\dagger a_{LO_i}' + a_{LO_i}^\dagger a_{S_i}) + (1-T_{a_i}) a_{LO_i}^\dagger a_{LO_i}' \right] +$$

$$+ \varepsilon \sum_j^N \left[T_{b_j} b_{S_j}^\dagger b_{S_j}' + \sqrt{T_{b_j}(1-T_{b_j})} (b_{S_j}^\dagger b_{V_j}' + b_{V_j}^\dagger b_{S_j}') + (1-T_{b_j}) b_{V_j}^\dagger b_{V_j}' \right]$$

Homodyning on macroscopic states

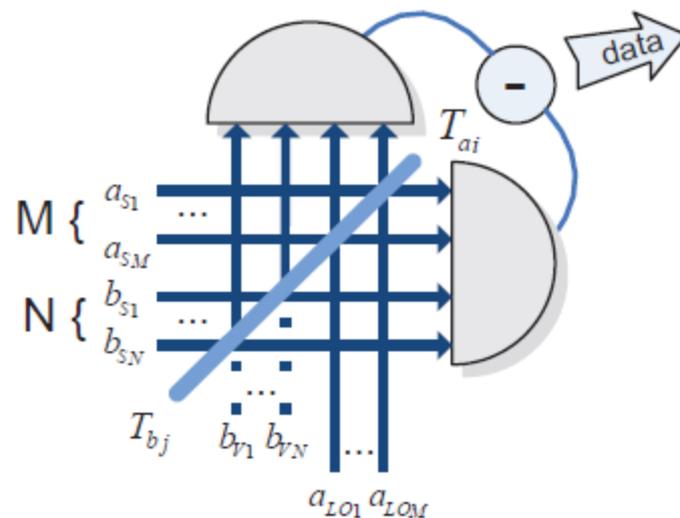


Measured photon numbers:

$$n_1 = \sum_i^M a_{S_i}^\dagger a_{S_i} + \varepsilon \sum_j^N b_{S_j}^\dagger b_{S_j} \quad \text{and} \quad n_2 = \sum_i^M a_{LO_i}^\dagger a_{LO_i} + \varepsilon \sum_j^N b_{V_j}^\dagger b_{V_j}.$$

$$n_2 = \sum_i^M \left[(1 - T_{a_i}) a_{S_i}^\dagger a_{S_i} - \sqrt{T_{a_i}(1 - T_{a_i})} (a_{S_i}^\dagger a_{LO_i} + a_{LO_i}^\dagger a_{S_i}) + T_{a_i} a_{LO_i}^\dagger a_{LO_i} \right] + \\ + \varepsilon \sum_j^N \left[(1 - T_{b_j}) b_{S_j}^\dagger b_{S_j} - \sqrt{T_{b_j}(1 - T_{b_j})} (b_{S_j}^\dagger b_{V_j} + b_{V_j}^\dagger b_{S_j}) + T_{b_j} b_{V_j}^\dagger b_{V_j} \right]$$

Homodyning on macroscopic states



1. BALANCED DETECTION

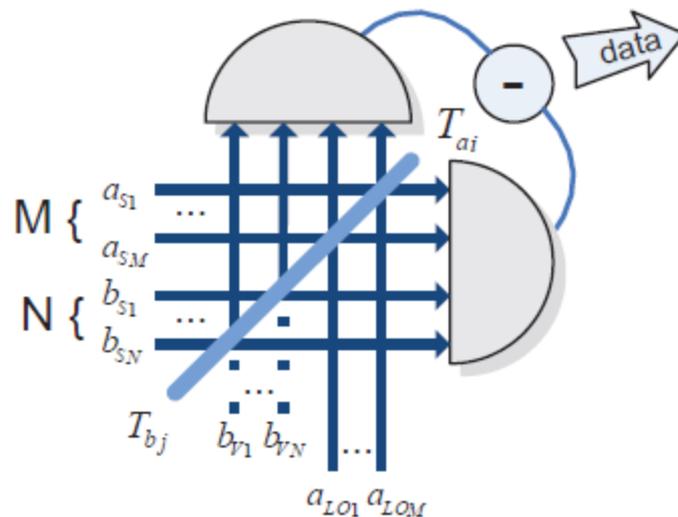
$$n_1 = \sum_i^M a_{s_i}^{\dagger} a'_{s_i} + \epsilon \sum_j^N b_{s_j}^{\dagger} b'_{s_j} \quad \text{and} \quad n_2 = \sum_i^M a_{LO_i}^{\dagger} a'_{LO_i} + \epsilon \sum_j^N b_{v_j}^{\dagger} b'_{v_j}.$$

Difference photocurrent:
$$\Delta_i = \alpha \sum_i^M x_i + \epsilon \sum_j^N (b_{s_j}^{\dagger} b_{v_j} + b_{v_j}^{\dagger} b_{s_j}).$$

Normalized variance:
$$\text{Var}(\Delta_i)_{norm} = \text{Var}(X) + \epsilon_{tot}^2 \bar{n},$$

where $\bar{n} \equiv \langle b_{s_j}^{\dagger} b_{s_j} \rangle$ and $\epsilon_{tot}^2 = \frac{N\epsilon^2}{M\alpha^2}$.

Homodyning on macroscopic states



2. UNBALANCED 2-MODE CASE $\Delta_i \propto n_1 - gn_2$

Normalized variance:

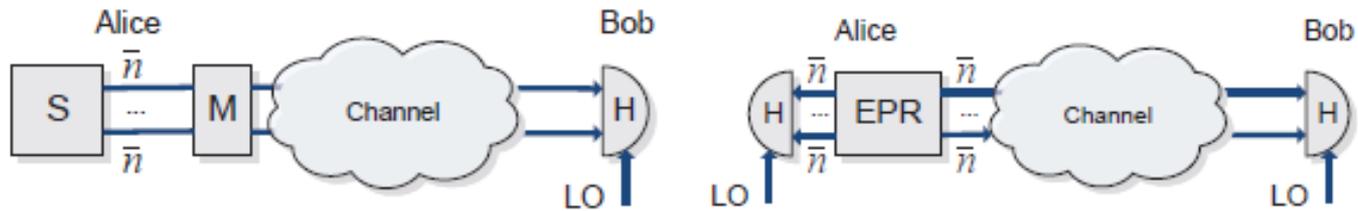
$$\text{Var}(\Delta_i)_{norm}^{(umb)} = \frac{T_a}{1-T_a} \text{Var}(X) + \frac{\epsilon_{tot}^2}{(1-T_a)^2} \left[T_b(1-T_b)\bar{n} + (T_b - T_a)^2 \text{Var}(n) \right]$$

with $g = \frac{T_a}{1-T_a}$ in order to compensate fluctuations in the main signal mode.

Scaling also applies to correlations.

Homodyning on macroscopic states

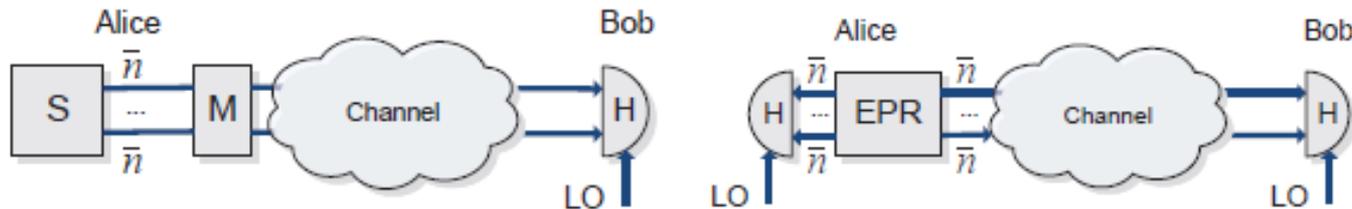
QUANTUM COMMUNICATION / RESOURCE SHARING



prepare-and-measure

entanglement-based

Homodyning on macroscopic states



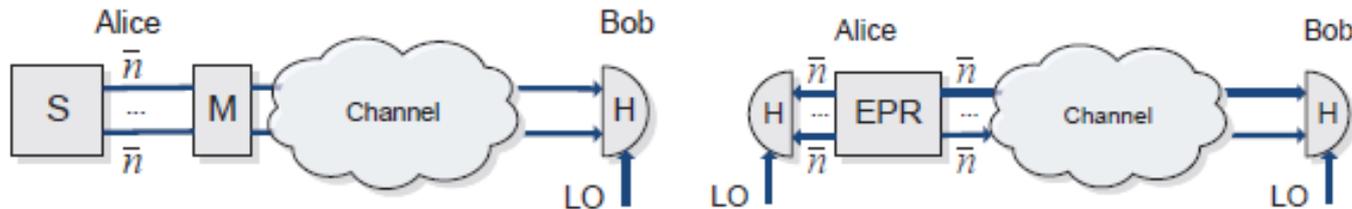
1. DETECTION OF SQUEEZING AND ENTANGLEMENT

Squeezing is lost at $\bar{n} = (1 - V_S) / \epsilon_{tot}^2$

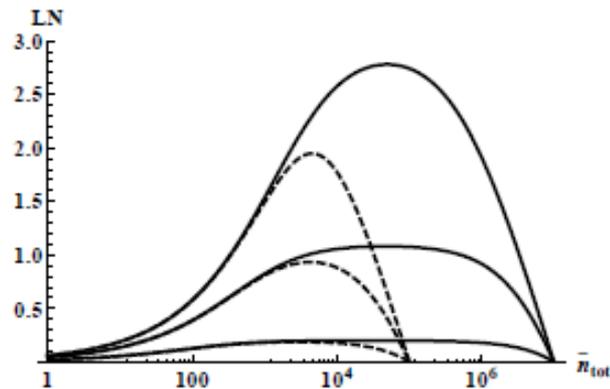
e.g. $V_S = -10$ dB upon $\epsilon_{tot} = 10^{-2}$ is lost at $\bar{n} \approx 10^4$

Entanglement is lost at $\bar{n} = \frac{1}{\epsilon_{tot}^2 (1 + \epsilon_{tot}^2 / 4)}$ approx. $\bar{n} = \epsilon_{tot}^{-2}$.

Homodyning on macroscopic states

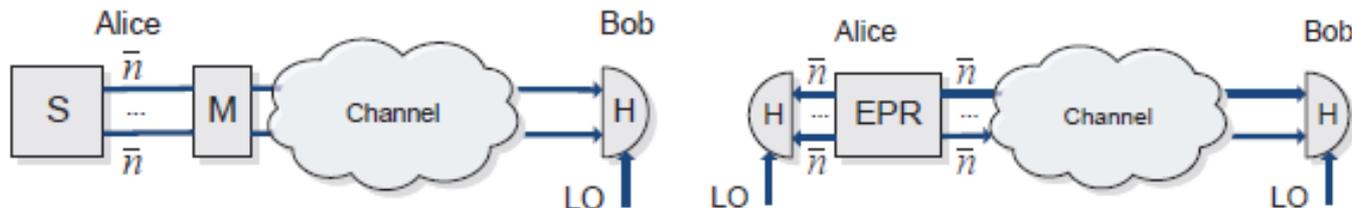


1. DETECTION OF SQUEEZING AND ENTANGLEMENT

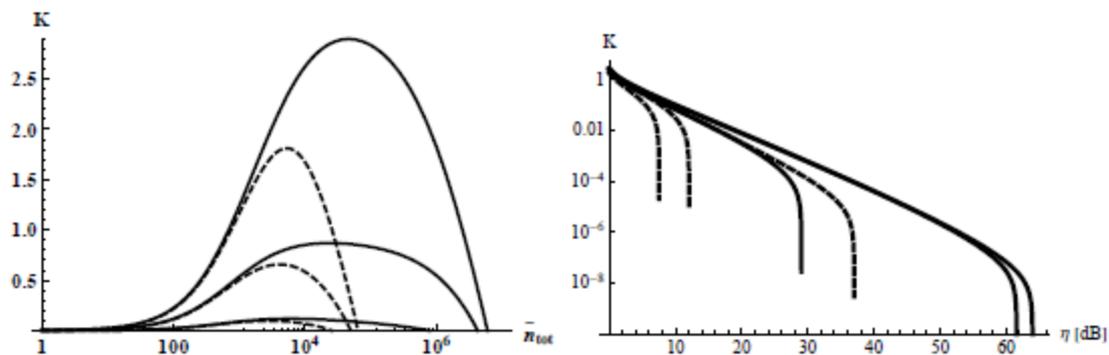


Logarithmic negativity of the macroscopic entangled states measured by the homodyne detectors versus total mean photon number upon 10^3 total number of modes and $\epsilon_{tot} = 10^{-2}$ (solid lines), $\epsilon_{tot} = 0.1$ (dashed lines). Channel transmittance (from bottom to top) $\eta = 0.1, 0.5, 0.9$, channel noise is absent.

Homodyning on macroscopic states



2. CV QKD WITH MACROSCOPICALLY BRIGHT STATES



Key rate secure against collective attacks in bits per channel use, generated from the homodyne measurement of the macroscopic squeezed states. (Left): Plotted with respect to the total mean number of photons upon 10^3 total number of modes and $\epsilon_{tot} = 10^{-2}$ (solid lines), $\epsilon_{tot} = 0.1$ (dashed lines). Channel transmittance (from bottom to top) $\eta = 0.1, 0.5, 0.9$, channel noise is absent. (Right): Plotted with respect to the channel transmittance η (in negative dB scale) in the presence of channel noise $\chi = 5\%$ SNU upon $\bar{n} = 10^3, 10^2, 10$ (from left to right), $\epsilon_{tot} = 10^{-2}$, perfect post-processing efficiency $\beta = 1$ (solid lines) and reduced efficiency $\beta = 0.97$ (dashed lines).

Summary

- Multimode effects can lead to security break in CV QKD;
- Knowledge of the mode structure improves the security bounds;
- Mode selection in the homodyne detector can be helpful, but should be precise;
- Symmetrization of source modes restores the single-mode scenario;
- Increased number of modes stabilizes the key rate in case of energy fluctuations within the modes;
- Signal brightness together with mode mismatch result in the excess noise, proportional to the mean photon number in the signal;
- Unbalancing leads to the noise proportional to the photon-number variance;
- Such noise altogether leads to a trade-off between security/entanglement and brightness/squeezing;
- The impact of noise can be suppressed by mode selection and/or increase of power of the local oscillator.

Acknowledgements



Thank you for attention!

usenko@optics.upol.cz