CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH MULTIMODE ENTANGLED STATES

Vladyslav Usenko

Department of Optics, Palacký University,
Olomouc, Czech Republic

1. Introduction

We address the CV QKD based on multimode homodyne detection and generally multimode entangled states. We model the multimode homodyne detection and derive security bounds assuming either trusted or untrusted detection.

We suggest several methods to compensate the negative effect of homodyne structure such as mode balancing in the source, mode selection in the detection and security stabilization by increasing number of modes.

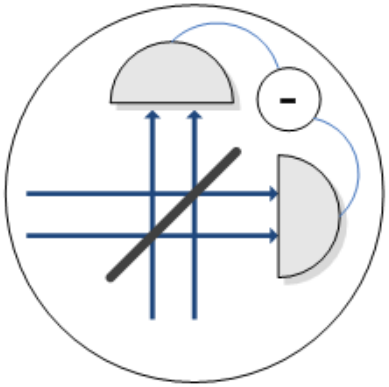
We assume: no crosstalk between the modes; no mode mismatch in the detection; etectors are identical in both the beams; channel is the same for all the modes; **Multimode structure is completely known to Eve.**

Security analysis is based on the optimality of Gaussian collective attacks [1] on Gaussian CV QKD [2], Eve holds the purification of the states.

Lower bound on key rate is expressed through mutual information and Holevo bound:

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

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

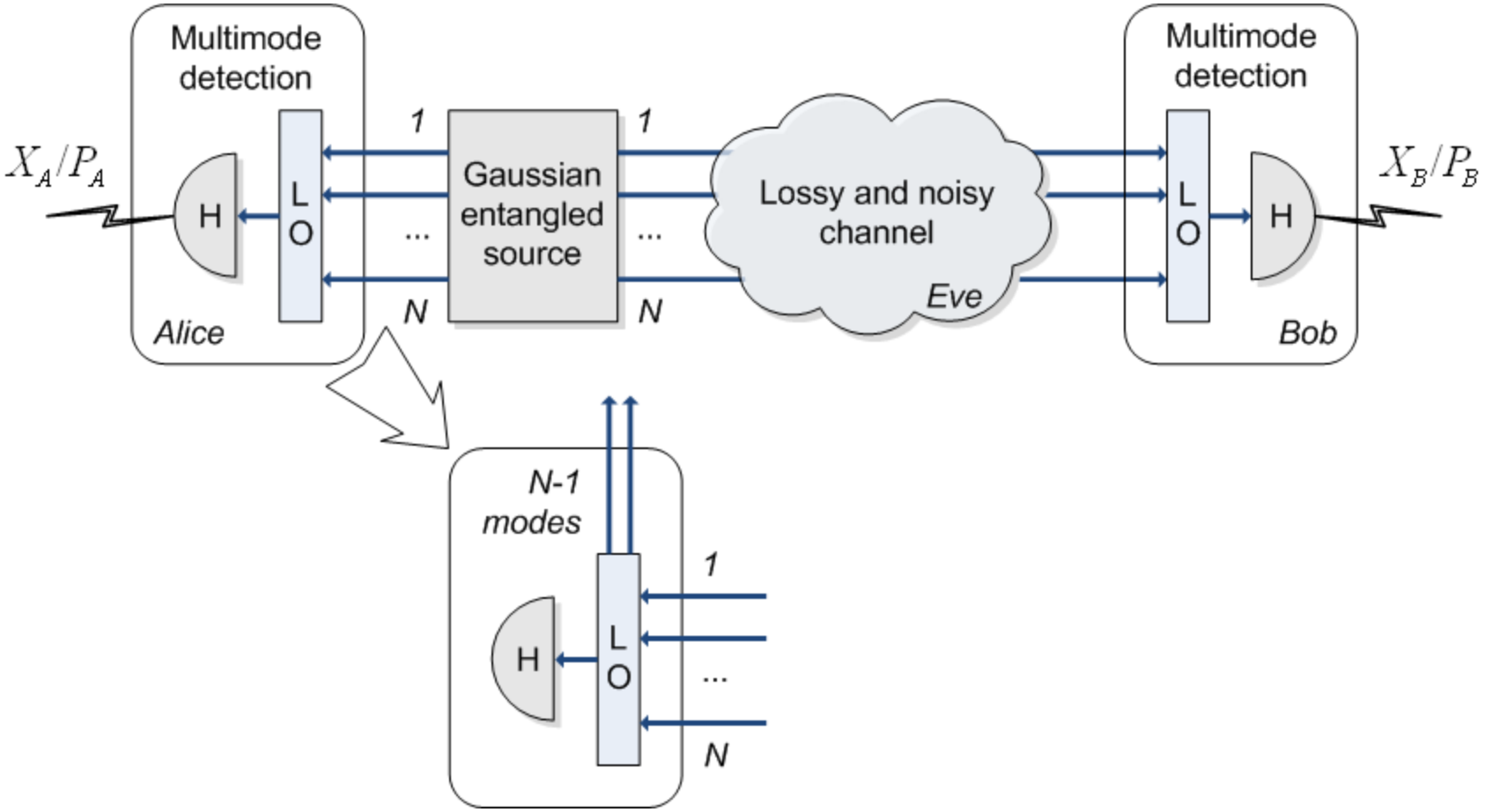
After normalization of photo-current: $X^{(N)}(\theta) = \dfrac{\sum_{n=1}^{N} G_i\tilde{X}_i(\theta)}{\sqrt{\sum_{n=1}^{N} G_i^2}}$

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

Multimode homodyne = linear optical (LO) network + single-mode homodyne

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

3. Untrusted multimode detectors

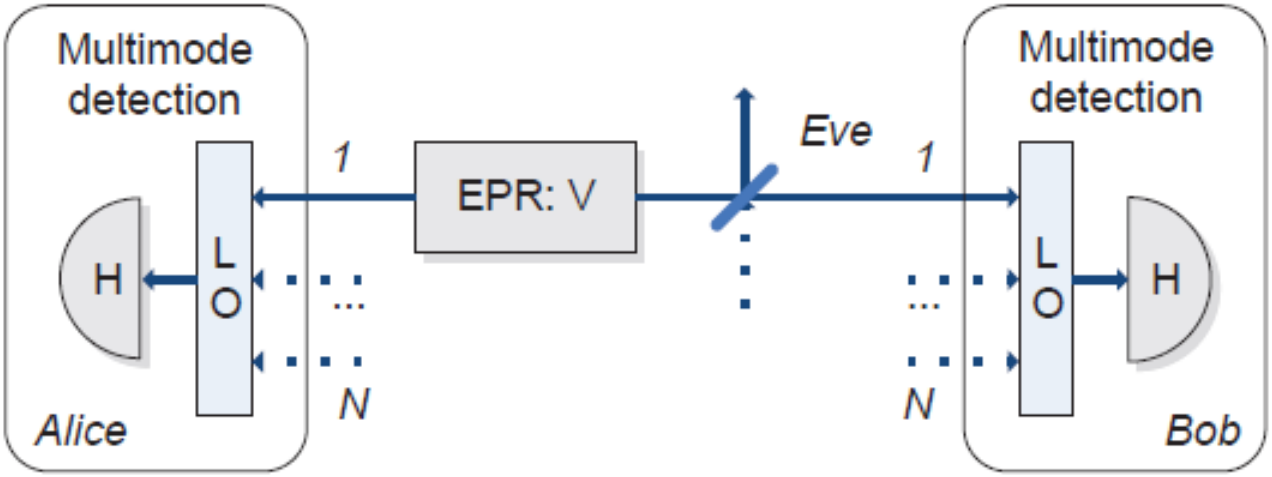


Output modes of the LO coupling before detection are available to Eve.

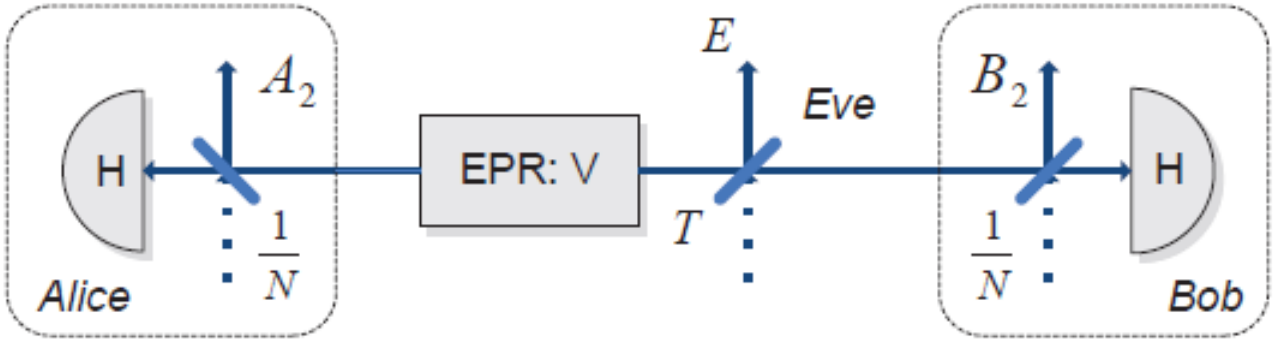
Multimode covariance matrix becomes the weighted sum of single-mode ones:

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

4. Untrusted multimode detectors



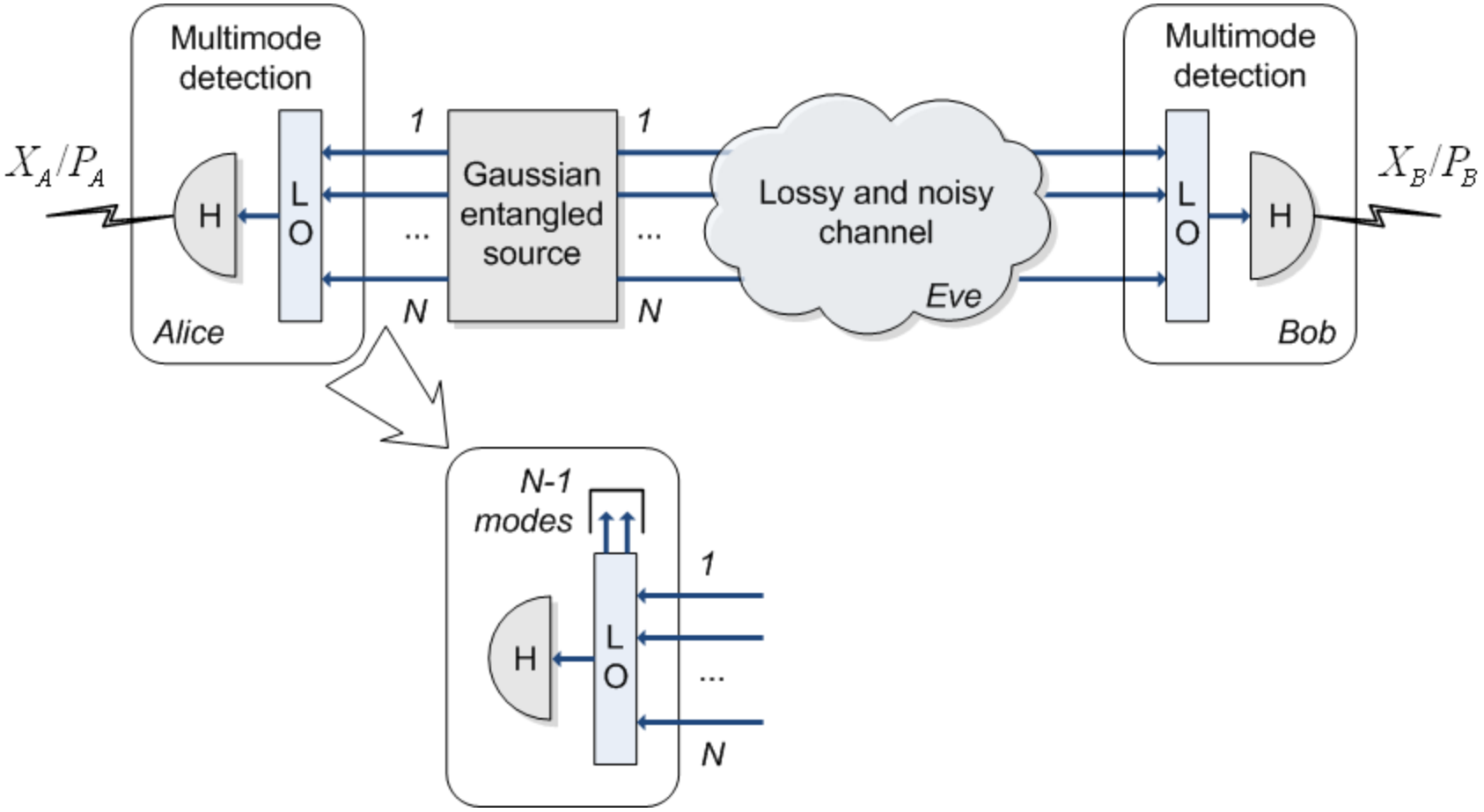
All modes, but one are in the vacuum state -> equivalent to symmetrical side-channels with untrusted outputs:



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

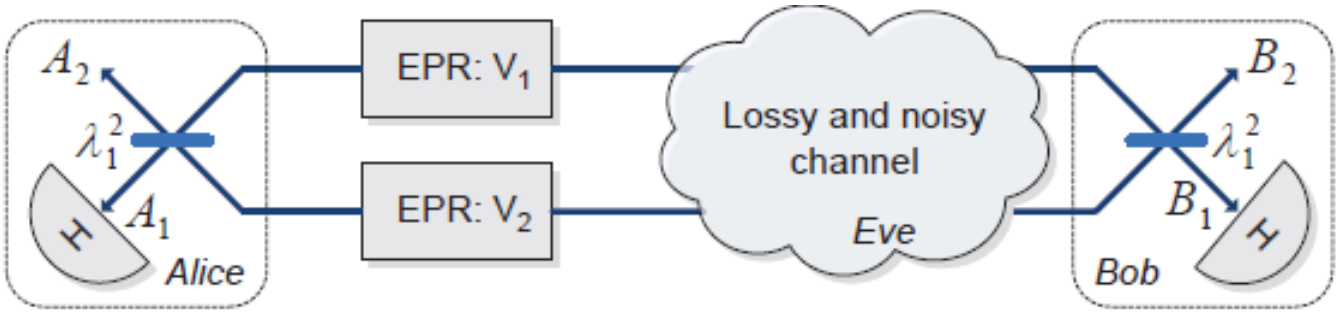
(while entanglement is preserved)

5. Trusted multimode detectors



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

6. Trusted multimode detectors



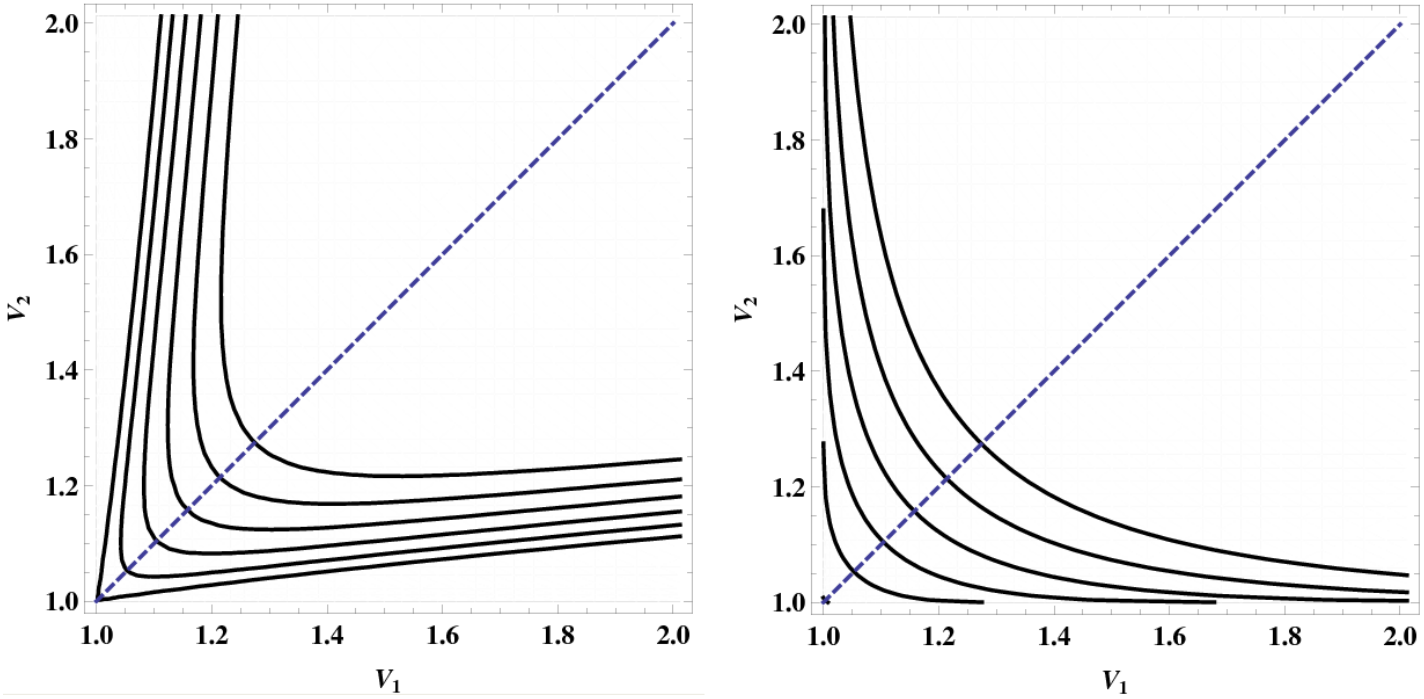
Purification of a 2-mode scheme.

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 $K^{(1)} = \log\left[1/(1-T)\right]$

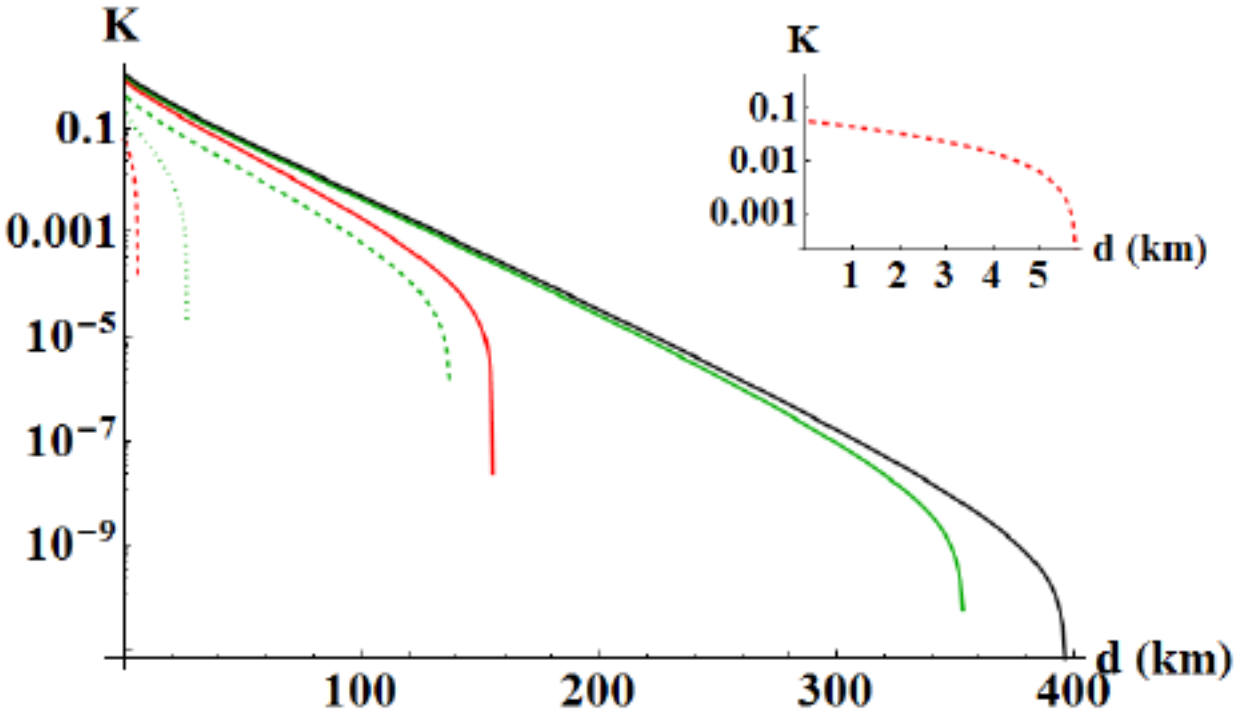
7. Unbalanced multimode sources



Security region in terms of mode variances in the case of trusted (left) and untrusted (right) multimode homodyne detection on the two-mode state.

Note that symmetrization of the modes makes the two cases equivalent.

8. Mode selection in homodyne detection



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

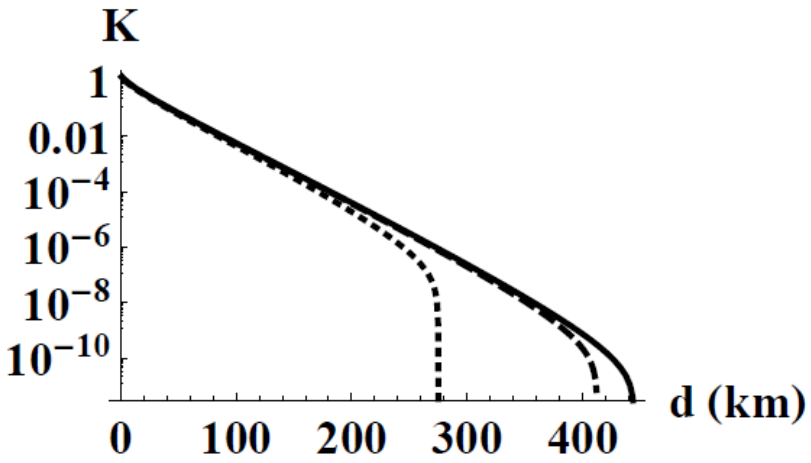
$V_2 = 1$, balanced detection (dotted lines)

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

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

9. Limited knowledge of multimode structure

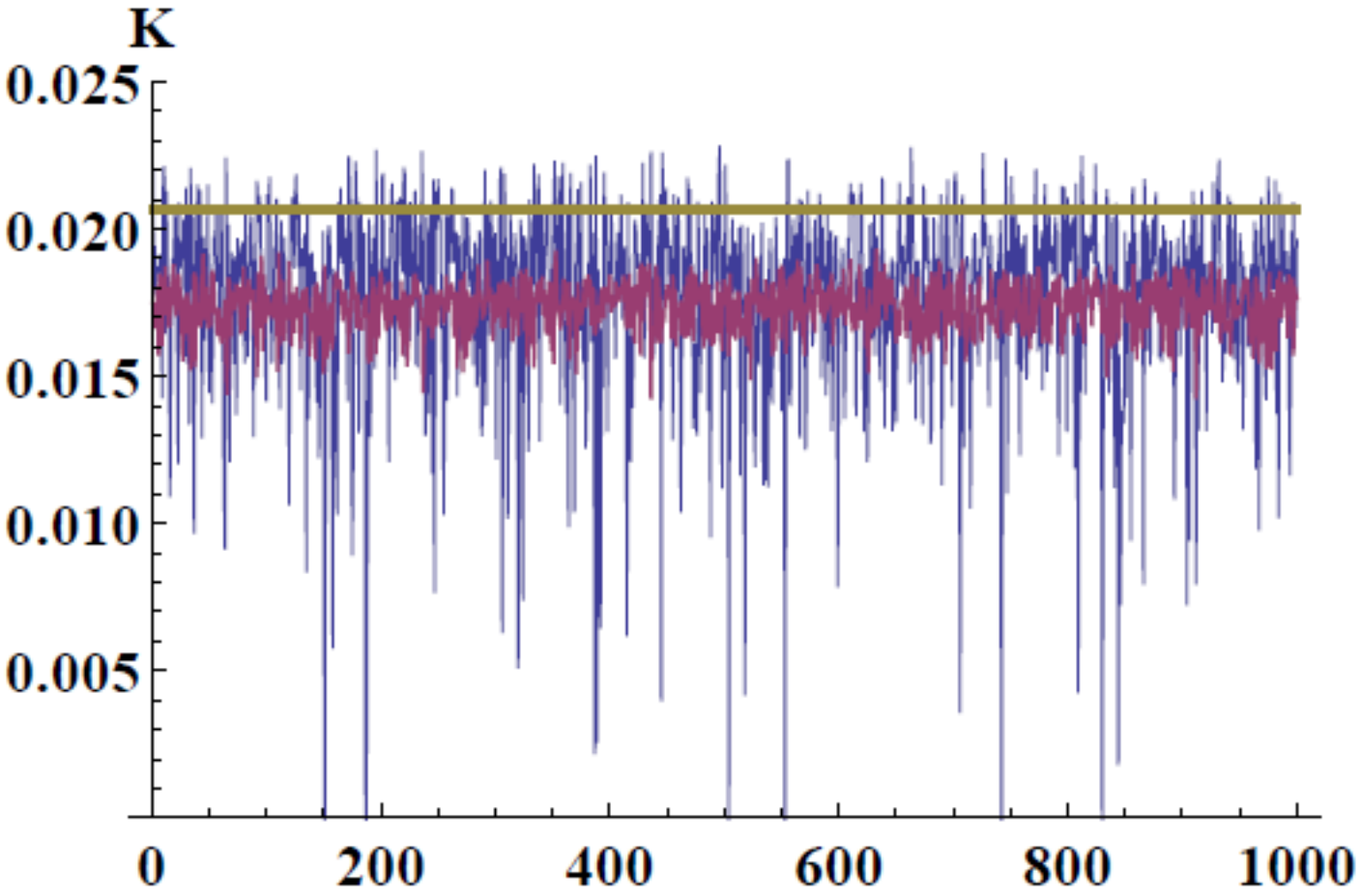
	3-mode (reality)	2-mode (limited knowledge)	1-mode ("ignorant" approach)
Setup parameters	$V_1 = 5,\ \lambda_1^2 = 95\%$ $V_2 = 1.5,\ \lambda_2^2 = 2.5\%$ $V_3 = 1.1,\ \lambda_3^2 = 2.5\%$	$V_1^{(2)} = 5,\ \lambda_1^2 = 95\%$ $V_2^{(2)} = 1.3,\ \lambda_2^2 = 5\%$	$V_1^{(1)} = 4.815$
Channel parameters	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).

10. 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% efficiency.

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.

References

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

[2] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, Nature 421, 238 (2003)