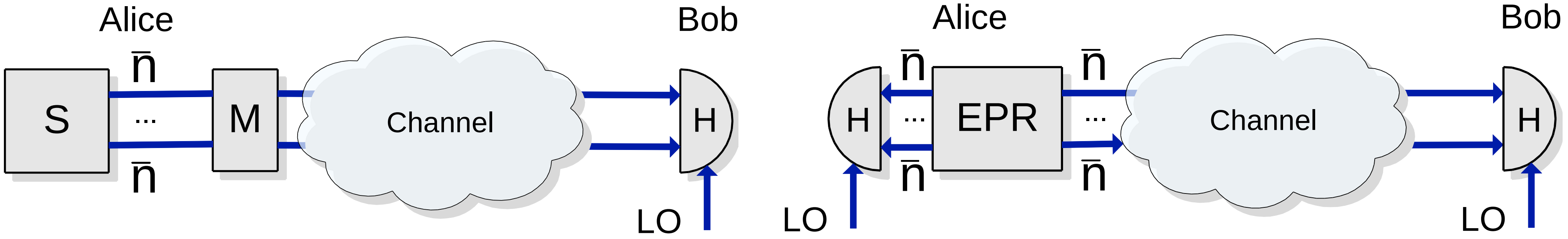
TOWARDS MACROSCOPIC QUANTUM KEY DISTRIBUTION

Vladyslav C. Usenko[1], Kirill Yu. Spasibko[2,3,4], Laszlo Ruppert[1], Maria V. Chekhova[2,3,4], Radim Filip[1], and Gerd Leuchs[2,3]

1. Department of Optics, Palacký University, 17. listopadu 50, 772 07 Olomouc, Czech Republic
2. Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/B24, 91058 Erlangen, Germany
3. University of Erlangen-Nürnberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany
4. Physics Department, Moscow State University, Leninskiye Gory 1-2, Moscow 119991, Russia

1. INTRODUCTION

Continuous-variable (CV) **quantum key distribution** (QKD) is aimed at going beyond single-photon statistics and using multiphoton quantum states for QKD. It is typically based on the Gaussian modulation of coherent or squeezed states of light [1].



Prepare-and-measure (left) and entanglement-based (right) multimode CV QKD schemes

Equivalently, it can be considered and realized on the basis of entangled CV states (two-mode squeezed vacuum). Such states can be in principle **very bright** [2] (i.e., have many modes and high intensity) so that the individual modes, possessing strongly nonclassical features, can be hardly accessed [3]. The potential **advantages of using** such **macroscopic light for QKD** can be

- **Easier manipulation (e.g., tracking);**
- **Better channel estimation with stronger probes.**

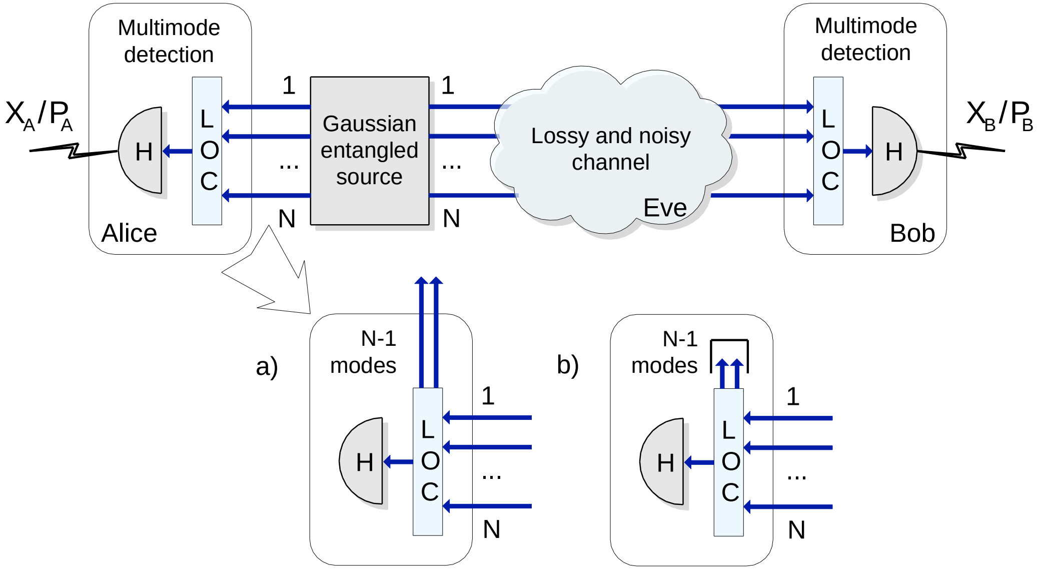
2. MULTIMODE CV QKD

Balanced N-mode homodyne detection with perfect mode matching results in the measurement of the **joint multimode quadrature** (e.g., X):

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

where $\tilde{X}_i(\theta)=a_i\exp(i\theta)+a_i^{\dagger}\exp(-i\theta)$ and the coefficients $\lambda_i=G_i/\sqrt{\sum_{n=1}^{N}G_n^2}$ satisfy $\sum_{i=1}^{N}\lambda_i^2=1$.

Such **N-mode homodyne detection can be modeled by liner-optical network and single-mode detection**. It leads to two scenarios for multimode CV QKD: with **unknown (a)** and **known (b)** detection structure.



Already **for N=2 and a single-mode source** the **security of CV QKD is broken** if the trusted parties are unaware of the multimode detection structure.

Security can be restored by i) **balancing the source**, ii) **balancing the detection** or iii) **full characterization of detection structure** in the security analysis.

[Usenko, Ruppert, Filip, Phys. Rev. A, **90** 062326 (2014)]

3. ROLE OF MODE MISMATCH

If **some of the signal modes are not matched** by the local oscillator (LO), **additional noise appears** in the outcomes of the multimode homodyne detection even for the perfectly balanced detection.

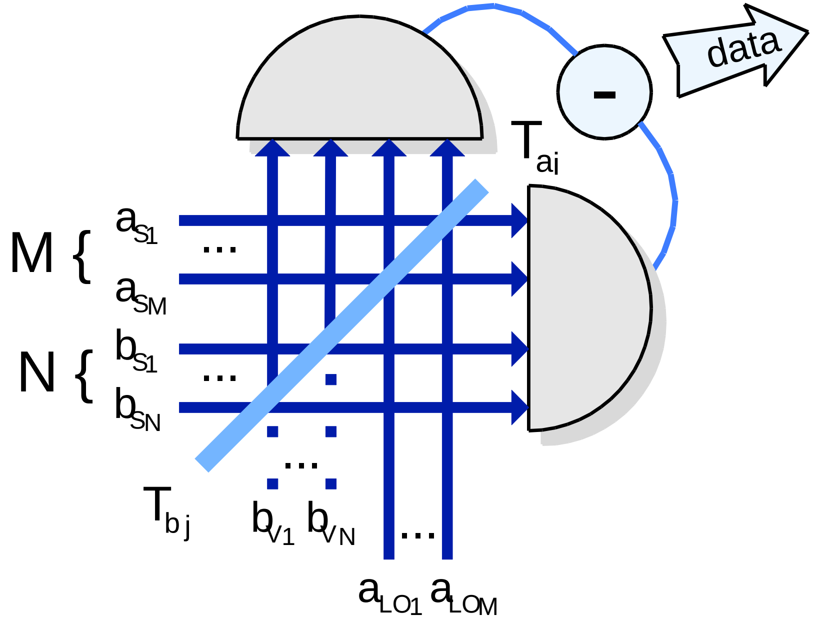
Photocurrent difference: $\Delta_i = \alpha \sum_i^M X_i + \varepsilon \sum_i^N (b_{S_j}^\dagger b_{V_j} + b_{V_j}^\dagger b_{S_j})$,

where α - LO amplitude, ε - coefficient of mode selection in the homodyne detection, M matched and N unmatched modes.

Normalized variance: $\boxed{Var(\Delta_i)_{norm} = Var(X) + \varepsilon_{tot}^2 \overline{n}}$,

where $\varepsilon_{tot}^2 = N\varepsilon^2/(M\alpha^2)$ and $\overline{n}$ is the mean photon number per mode.

Such noise is, however, negligible in practical applications when the signal modes are few and weak.

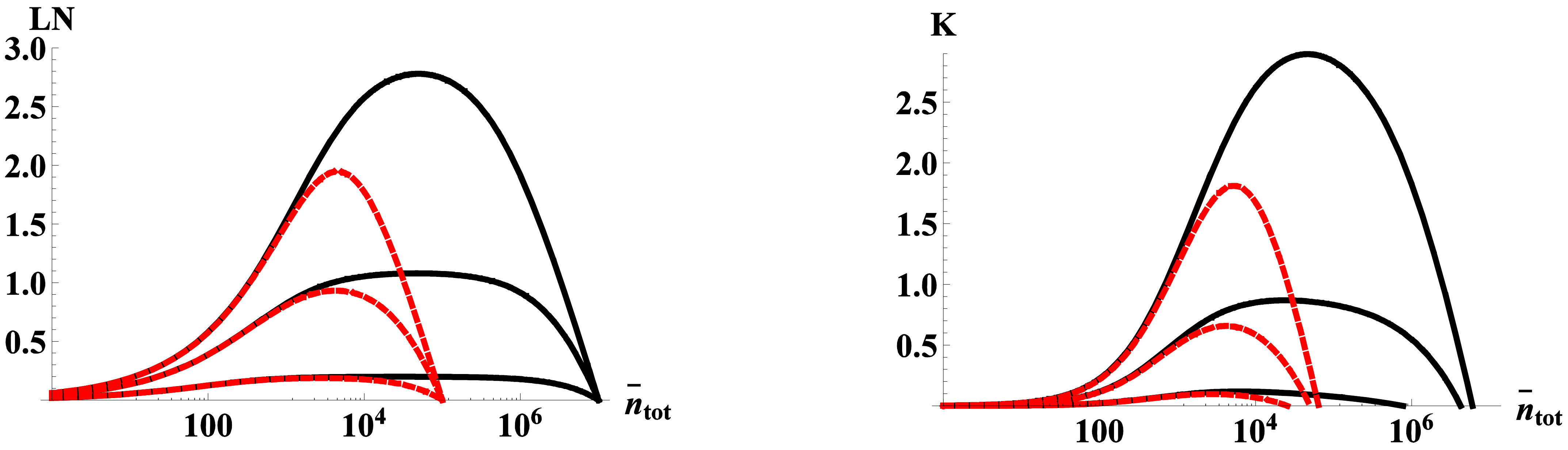


[Usenko, Ruppert, Filip, Opt. Exp., **23** 031534 (2015)]

4. ROLE OF HIGH BRIGHTNESS

If the unmatched signal is **bright** and **heavily multimode**, the **noise due to mode mismatch becomes essential**. It **limits applicability of the macroscopic states** to quantum resource sharing and QKD.

Entanglement of the states **cannot be observed** for a purely attenuating channel at $\overline{n} \approx \varepsilon_{tot}^{-2}$



Entanglement (in terms of **logarithmic negativity**, left) and **key rate secure against collective attacks** (right) versus **total mean photon number** $n_{tot} = (M+N)\overline{n}$ at $\varepsilon_{tot} = 10^{-2}$ (solid lines), $\varepsilon_{tot} = 0.1$ (red dashed lines), total number of modes is 10^3 .

[Usenko, Ruppert, Filip, Opt. Exp., **23** 031534 (2015)]

5. IMPERFECT HOMODYNING

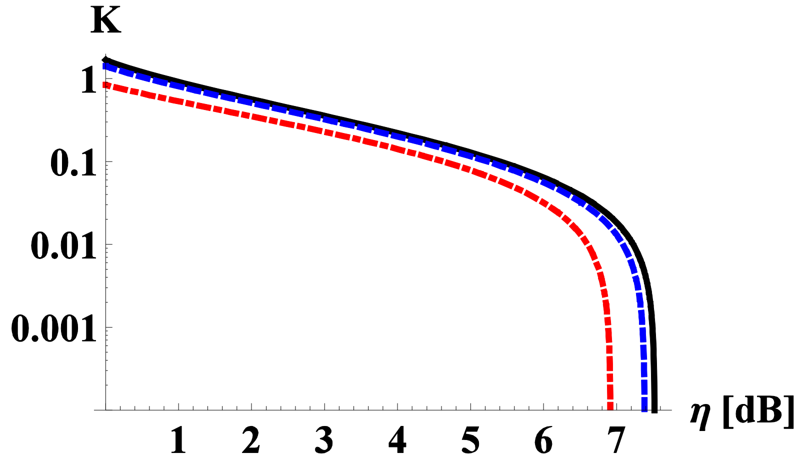
If the **homodyne detection is not perfectly balanced**, the results of the measurements contain additional term concerned with the unmatched modes. For two modes with coupling to LO being $T_a \neq T_b \neq 1/2$, the **normalized variance of the photocurrent difference** reads

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

and **contains the term proportional to the variance of the photon-number fluctuations** in a signal mode. This enforces the effect of the brightness of the unmatched signal modes in practical applications.

Key rate secure against collective attacks versus **channel transmittance in dB** at perfect balancing (black solid line), **unbalanced detection of the signal** $T_a = 1/2 + 1\%$ (blue dashed line) and additional **unbalanced detection of the unmatched mode** $T_b = 1/2 - 1\%$ (red dot-dashed line). Mean photon number per mode is 10^2, post-processing efficiency is 97%.

→

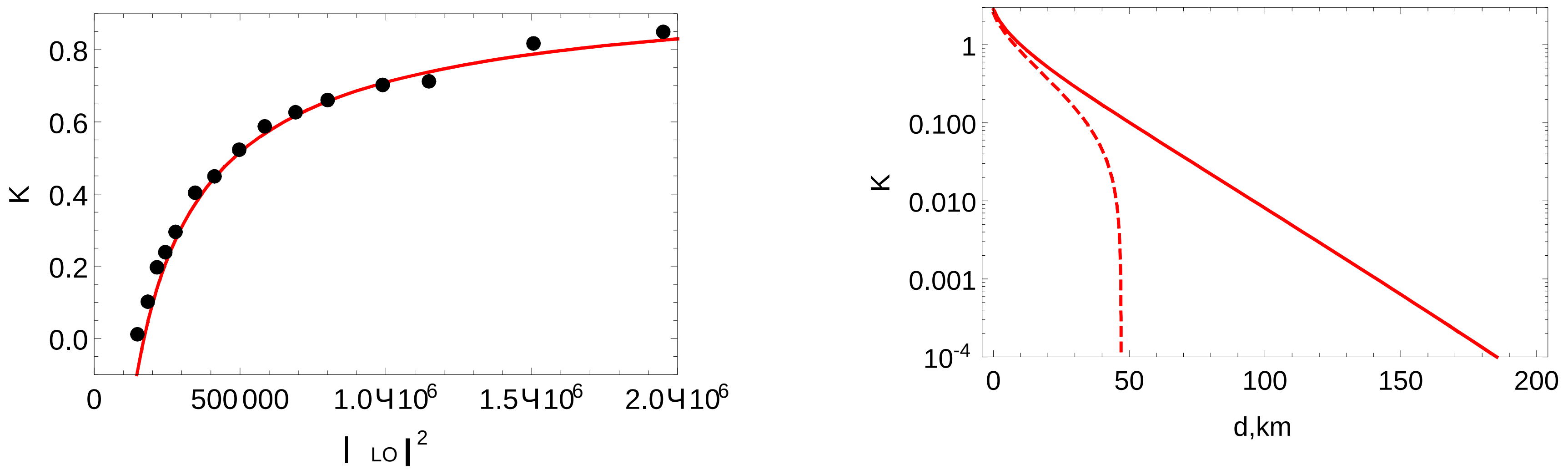


[Usenko, Ruppert, Filip, Opt. Exp., **23** 031534 (2015)]

6. PROOF-OF-PRINCIPLE TEST

It was theoretically shown above that the noise related to the bright unmatched modes can be reduced by increasing the power of LO. This conjecture was tested experimentally by performing **homodyne detection on two strong coherent signals**, one of which was matched to a single-mode LO. The results show that the **noise observed by the homodyne detector** was indeed **decreased by stronger LO**, thus achieving $\varepsilon_{tot}^{2} \approx . 4.3 \cdot 10^{-7}$ at the maximum LO power of $2 \cdot 10^{6}$ mean photons.

Using the obtained data the key rate of CV QKD with macroscopic states was modeled:



Key rate secure against collective attacks at mean photon number of 10^{5} per mode versus **power of LO** (left) and **distance** in a standard telecom fiber at the maximum LO power (right).

CONCLUSIONS

We considered the possibility to implement **QKD with macroscopic light** and analysed the **multimode homodyne detection** taking into account **bright unmatched modes**. We shown the presence of excess noise in the quadrature variance measured with such a detector, which has to be assumed untrusted and therefore limits the applicability of the macroscopic protocol. We performed a **proof-of-principle experimental test** which confirms the **noise reduction in the multimode homodyne detection** of bright states. Our results pave the way to the macroscopic implementation of quantum key distribution.

REFERENCES

[1] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001); F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[2] T. S. Iskhakov, M. V. Chekhova, and G. Leuchs, Phys. Rev. Lett. **102**, 183602 (2009); T. S. Iskhakov, I. N. Agafonov, M. V. Chekhova, and G. Leuchs, Phys. Rev. Lett. **109**, 150502 (2012).

[3] T. S. Iskhakov, V. C. Usenko, R. Filip, M. V. Chekhova, G. Leuchs, Phys. Rev. A **93**, 043849 (2016).

Acknowledgements

The research leading the these results has received funding from the EU FP7 under Grant Agreement No. 308803 (project BRISQ2). V.C.U. and L.R. acknowledge the project 13-27533J of GAČR.