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*

We address the possibility to implement continuous-variable quantum key distribution using macroscopic (intense and multimode) states of light. We take into account mode mismatch in the detection and high brightness of the modes, and show that it results in the intensity-dependent excess noise in the quadrature measurements, limiting the applicability of quantum key distribution with bright multimode states. We theoretically show that mode selection, suppressing the contribution from the unmatched modes in the homodyne measurements, and increasing the power of the local oscillator are potentially able to improve the performance of quantum key distribution with macroscopic light. We further confirm this conjecture by performing a proof-of-principle test of multimode homodyne measurement with an unmatched bright mode and show that by increasing the power of the local oscillator the quadrature excess noise is indeed suppressed. Our results pave the way to the implementation of quantum key distribution with macroscopic light.

I. INTRODUCTION

Quantum key distribution (QKD) [1] was first proposed on the basis of qubits (two-level quantum systems) realized by single-photon states or entangled photon pairs. QKD was later extended to the realm of continuous-variable (CV) states defined on the infinite-dimensional Hilbert spaces and realized by multiphoton quantum states of light [2]. It was a particularly important step in the development of QKD, when coherent states were shown sufficient to provide security of the key even in the strongly attenuating channels using Gaussian quadrature modulation, homodyne detection, and reverse information reconciliation [3]. It was further shown that the use of nonclassicality is able to enforce CV QKD protocols [4]. The proposals and realizations of QKD protocols were however mainly remaining in the realm of relatively weak (less intense) states of light, where quantum features are naturally more pronounced. In our work we go beyond this approach and study the possibility of implementing QKD with macroscopic quantum states, i.e. strongly multimode and intense beams, possessing nonclassical features. Our work therefore aims at bringing QKD to the furthest extreme from its origin of single-photon states, motivated by the recent successful generation of macroscopic nonclassical states [5]. This way we extend the previously carried out analysis of the multimode effects in CV QKD, when the multimode structure of light, detected by a homodyne detector, was shown crucial in security analysis of CV QKD unless the detection is perfectly balanced [6]. In the present work, in order to study the applicability of macroscopic states for CV QKD, we consider multimode homodyne detection in more detail and reveal the effect of bright signal modes mismatch with the local oscillator (LO) resulting in the intensity-dependent excess noise. Such noise undermines the security of CV QKD if being attributed to the result of an eavesdropping attempt. We then consider the possibility to suppress the negative influence of unmatched bright signal modes by increasing the power of the LO. Finally, we report a proof-of-principle test of homodyne detection of bright multimode signal and confirm the reduction of noise through the increase of the LO power. Our results open the possibility to implement QKD with macroscopic states of light.

II. HOMODYNE DETECTION OF MULTIMODE BRIGHT SIGNAL

In order to reveal the peculiarities of the macroscopic signal in CV QKD we describe the detection of the bight multimode signal on a homodyne detector taking into account mode mismatch. Homodyne detection is well known to be based on the coupling (ideally perfectly balanced) of a quantum signal with a strong shot-noise limited LO, being a phase reference for the signal measurement, and subsequent photodetection of the outputs followed by the substraction of the photocurrents so that the result can be set proportional to either amplitude or phase quadrature of the signal depending on the phase difference between the signal and the LO. We assume that some M signal modes of a generally multimode bright signal are matching the LO, and some N modes are not. Using the input-output formalism for the quantum operators of the signal matched a_{S_i} or unmatched b_{S_j} modes coupled to either LO a_{LO_i} or vacuum b_{V_j} (in case of mismatch) modes, and assuming that a certain weight ϵ can be attributed to the contribution from the unmatched modes in the resulting photocurrents, the photocurrent difference observed on a balanced homodyne detector reads [7]

$$\Delta = \alpha \sum_{i}^{M} x_i + \epsilon \sum_{j}^{N} (b_{S_j}^{\dagger} b_{V_j} + b_{V_j}^{\dagger} b_{S_j}). \qquad (1)$$

where x_i is the quadrature value of the i-th matched mode. Here and further with no loss of generality we assume that the x-quadrature is measured, with an intense coherent LO having a real amplitude α. The homodyne measurement of a bright multimode signal therefore involves the direct detection of the

*Electronic address: usenko@optics.upol.cz

auxiliary unmatched signal modes b_{S_j}. It results in the noise contribution to the variance of the quadrature measurements, being essential for the security of CV QKD. Such variance of the photocurrent difference after normalization by the vacuum variance (measured with the signal being blocked), reads

$$Var(\Delta)_{norm} = Var(x) + \epsilon_{tot}^2 \bar{n}, \tag{2}$$

where $\bar{n}$ is the mean number of photons in a signal mode, $Var(x)$ is the quadrature variance of a signal mode, and $\epsilon_{tot}^2 = N\epsilon^2/(M\alpha^2)$. Thus the quadrature variance even in the case of perfectly balanced homodyne detection involves the noise term which is proportional to the mean photon-number in the additional signal modes. This inefficiency of mode selection can be reduced by decreasing N (using better mode matching) or by increasing the amplitude α of the LO. By reducing the inefficiency ϵ_{tot} the noise term concerned with the macroscopic brightness of the signal can be strongly reduced. However it does not vanish as long as the bright unmatched modes are present. Therefore the homodyne detection of the multimode bright light becomes equivalent to the homodyne detection on the single-mode signal with the excess noise proportional to the mean photon number of a signal mode.

III. EFFECT OF MACROSCOPIC CHARACTER OF THE SIGNAL ON SECURITY

We analyze the effect of noise related to the macroscopic character of the signal states on the security of a Gaussian squeezed-state CV QKD protocol [8] using bright squeezed vacuum (BSV) as the signal. We assess the security of the protocol against the optimal Gaussian collective attacks [9] by estimating the lower bound on the key rate, which, in the case of reverse reconciliation, reads

$$K = \beta I_{AB} - \chi_{BE}, \tag{3}$$

where $\beta \in (0,1)$ is the post-processing efficiency (we further use realistic $\beta = 97\%$), I_{AB} is the mutual (Shannon) information between the trusted parties, and χ_{BE} is the Holevo bound, which upper limits the information leakage from the given channel. The information quantities involved in Eq. (3) are obtained from the elements of the covariance matrix of the state effectively shared between Alice and Bob in the equivalent entanglement-based representation [10]. The matrices then involve the noise concerned with the macroscopic character of the beams. Such noise is considered untrusted in our study since the intensity of the unmatched modes can be controlled by a potential eavesdropper. Therefore, a trade-off between the brightness of the source and the security of CV QKD appears. The excess noise due to the macroscopic structure can lead to the security break already in the case of a highly transmitting (even perfect) channel and perfectly balanced homodyne detection. It therefore requires the optimization of the total mean photon number for the given number of modes and ϵ_{tot}, which effectively characterizes the imperfection of the homodyne detector, as shown in Fig. 1, left.

We show that when the unmatched modes are properly suppressed by mode selection and/or power of the LO and when the number of modes is large (so that individually the modes are not bright), Gaussian CV QKD with bright multimode states is possible at reasonably long distances, as depicted in Fig. 1 (right), where the key rate is plotted versus channel attenuation for $\epsilon_{tot} = 10^{-2}$ and for different mean photon numbers.

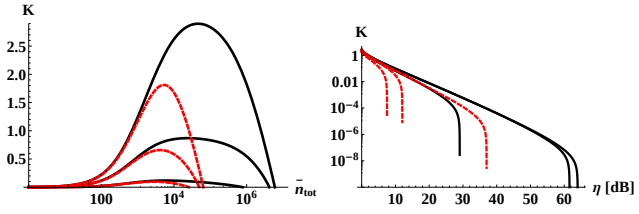

FIG. 1: (Left): Key rate secure against collective attacks in bits per channel use, generated from the homodyne measurement of the BSV states versus the total mean number of photons. On both graphs the total number of modes is 10^3 and $\epsilon_{tot} = 10^{-2}$ (solid lines), $\epsilon_{tot} = 0.1$ (red dashed lines). Channel transmittance (from bottom to top) is $\eta = 0.1, 0.5, 0.9$, the channel noise is absent. (Right): Key rate secure against collective attacks in bits per channel use, generated from the homodyne measurement of the BSV states plotted with respect to the channel transmittance η (in negative dB scale) in the presence of a channel noise of 5% of a shot-noise unit (SNU), and upon $\epsilon_{tot} = 0.1$. The post-processing efficiency is $\beta = 1$ (black solid lines) or $\beta = 0.97$ (red dashed lines), $\bar{n} = 10^3, 10^2, 10$ (from left to right).

Our result justifies the possibility to build CV QKD using experimentally generated bright macroscopic entangled states containing e.g. up to 10^5 photons per pulse distributed by 10^4 modes [11]. Assuming state generation at a telecom wavelength, the presence of 5% SNU of channel noise, realistic post-processing, and total auxiliary mode suppression inefficiency $\epsilon_{tot} = 10^{-2}$, the CV QKD can be therefore implemented in the asymptotic limit at up to 180 km with $\bar{n} = 10$, at up to 60 km with $\bar{n} = 10^2$, and at up to 40 km with $\bar{n} = 10^3$. The distances, however, would strongly depend on the particular implementation. Moreover, if the LO is reconstructed locally [12], the quantum signal appears to be the only state of light propagating through the channel and the brightness of the signal beams becomes crucial for handling the beams, which then waives the necessity in using additional bright pulses for beam pointing. Also the channel estimation with stronger beams can be more efficient. This suggests a promising application of macroscopically bright nonclassical light in quantum communication.

IV. TEST OF NOISE SUPPRESSION IN THE MULTIMODE HOMODYNE DETECTION

To show the potential of QKD with macroscopic states we report a proof-of-principle experimental test which verified the possibility of suppressing the noise in the homodyne detection arising from bright unmatched modes. In the experiment the two signal modes were realized by coherent beams, obtained by splitting a single beam in two in a birefringent crystal (calcite). One of the beams was matched and coupled

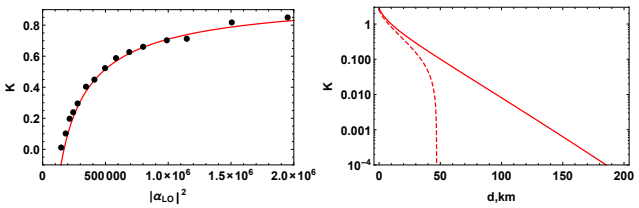

FIG. 2: Key rate secure against collective attacks in macroscopic CV QKD protocol as a function of the LO power (left) and as a function of the channel distance d for the maximal experimentally tested LO power (right) with perfect implementation (solid line) and with $\beta = 97\%$ and channel excess noise of 1% SNU (dashed line).

to another strong coherent beam, being the LO for the homodyne detection, while the other (unmatched) signal mode was coupled to vacuum. The coupling was performed by the combination of a half-wave plate and a polarizing beam splitter. For the two signal modes and LO this combination realizes a 50/50 beam splitter required for the homodyne detection. The photocurrents were measured at the outputs of the beam splitter and subtracted, and the variance of the photocurrent difference was normalized by the LO power. The results first of all confirmed the excess noise in the quadrature variance scaling linearly with the increase of the power of the unmatched mode. Then the measurements were performed for different powers of the LO. A reduction of the excess noise in the normalized variance of the photocurrent difference was observed, as predicted by the theory.

The ratio between the excess noise in the quadrature variance measured by the homodyne detector and the mean photon number in the auxiliary mode defines the parameter ϵ^2_{tot}, which is the overall inefficiency of mode selection in the homodyne detector measuring the bright multimode signal. Using this experimentally obtained parameter, we estimated the lower bound on the secure key rate in the macrosopic CV QKD protocol [7]. Assuming that the numbers of matched and unmatched modes are equal and that the mean photon number in a BSV signal mode is 10^5, one can see how the increase of the LO power can enable the security (providing the positivity of the key rate) and further improve the performance of the protocol in terms of the secure key rate, given in Fig. 2 (left) for the channel transmittance of 50%. It well fits the theoretical curve based on the analytical estimation of ϵ^2_{tot} for the given LO power (given in red) and demonstrates the possibility to improve CV QKD with multimode BSV states through the mode selection in the homodyne detector.

We also estimate the maximum secure distance in a standard telecom fiber channel of the BSV-based CV QKD protocol with the parameters given above, assuming that the BSV state is measured by the homodyne detector with $\epsilon^2_{tot} \approx 4.3 \cdot 10^7$ corresponding to the maximum LO power of $2 \cdot 10^6$ as realized in the experiment. The results are given in Fig. 2 (right) as a solid line for the perfect implementation and as a dashed line for imperfect post-processing (with 97% efficiency) and channel excess noise (1% of SNU). The results confirm the possibility of implementing CV QKD with BSV states in the long-distance channels.

V. SUMMARY

We considered the possibility to implement quantum key distribution with macroscopic light and analyzed 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 homodynde detection of bright states. Our results therefore pave the way to the macroscopic implementation of quantum key distribution.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[2] S. L. Braunstein and P. Van Loock, Reviews of Modern Physics **77**, 513 (2005).

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

[4] R. García-Patrón and N. J. Cerf, Physical Review Letters **102**, 130501 (2009); L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nature Communications **3**, 1083 (2012).

[5] T. Iskhakov, M. V. Chekhova, and G. Leuchs, Physical Review Letters **102**, 183602 (2009).

[6] V. C. Usenko, L. Ruppert, and R. Filip, Physical Review A **90**, 062326 (2014).

[7] V. C. Usenko, L. Ruppert, and R. Filip, Optics Express **23**, 31534 (2015).

[8] N. J. Cerf, M. Levy, and G. Van Assche, Physical Review A **63**, 052311 (2001).

[9] R. Garcia-Patron and N. J. Cerf, Physical Review Letters **97**, 190503 (2006); M. Navascués, F. Grosshans, and A. Acin, Physical Review Letters **97**, 190502 (2006).

[10] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Info. Comput. **3**, 535 (2003), ISSN 1533-7146.

[11] T. S. Iskhakov, I. N. Agafonov, M. V. Chekhova, and G. Leuchs, Physical Review Letters **109**, 150502 (2012).

[12] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Physical Review X **5**, 041009 (2015); D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Physical Review X **5**, 041010 (2015).