Research Article Vol. 27, No. 25 / 9 December 2019 / *Optics Express* 36154

Optics EXPRESS

Feasibility of quantum key distribution with macroscopically bright coherent light

OLENA KOVALENKO,[1,*] KIRILL YU. SPASIBKO,[2,3] MARIA V. CHEKHOVA,[2,3,4] VLADYSLAV C. USENKO,[1] AND RADIM FILIP[1]

[1] *Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*
[2] *Max Planck Institute for the Science of Light, Staudtstr. 2, 91058 Erlangen, Germany*
[3] *University of Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*
[4] *Department of Physics, M.V. Lomonosov Moscow State University, Leninskie Gory GSP-1,119991 Moscow, Russia*
[*] *kovalenko@optics.upol.cz*

Abstract: We address feasibility of continuous-variable quantum key distribution using bright multimode coherent states of light and homodyne detection. We experimentally verify the possibility to properly select signal modes by matching them with the local oscillator and this way to decrease the quadrature noise concerned with unmatched bright modes. We apply the results to theoretically predict the performance of continuous-variable quantum key distribution scheme using multimode coherent states in scenarios where modulation is applied either to all the modes or only to the matched ones, and confirm that the protocol is feasible at high overall brightness. Our results open the pathway towards full-scale implementation of quantum key distribution using bright light, thus bringing quantum communication closer to classical optics.

1. Introduction

Quantum key distribution (QKD) is well known to be a practical application of quantum information science. It is aimed at providing trusted parties with the means to share a secret cryptographic key to be further used in classical symmetrical cryptosystems (such as widely used AES system), so that security of the key is guaranteed by the very laws of quantum physics (see [1–4] for reviews). The first suggestions of QKD, namely discrete-variable protocols, were based on single-photon states [5], and are being practically realized with weak coherent pulses, typically accompanied by so-called decoy states to reveal the photon-number splitting attacks [6].

In order to waive the need highly efficient single-photon detectors, continuous-variable (CV) QKD was suggested on the basis of quadrature modulation of squeezed light, subsequently measured using homodyne detectors [7]. It was later extended to the use of coherent states, potentially enabling QKD without nonclassicality and with off-the-shelf telecommunication components [8–10] at a cost of acceptable reduction of efficiency and robustness of the protocols [11–13], also compared to the discrete-variable protocols [14]. This development brought QKD closer to a border between classical and quantum communication. However, light that carries information in classical optics is typically bright and multimode. It allows to easily operate the intensive and stable beams and to increase information capacity by multiplexing. Thus as the further development towards the use of bright light for QKD, far from the originally suggested single-photon states, QKD was shown potentially applicable with multimode [15] and macroscopically bright [16] nonclassical states.

Besides the conceptual interest in enabling QKD with macroscopic bright light, contrary to the low-energy single-photon states, the high brightness can largely simplify manipulations with the beams, such as pointing by a sender, beam guiding at intermediate stations (repeaters), and signal recognition at a receiver. This can be especially fruitful for free-space applications with quick link deployment and, in particular, in satellite-based channels, and can be further enforced

#375401 https://doi.org/10.1364/OE.27.036154
Journal © 2019 Received 21 Aug 2019; revised 25 Oct 2019; accepted 27 Oct 2019; published 25 Nov 2019

by multiplexing techniques. Moreover, as the local oscillator (LO) beam, which serves as a phase reference for the homodyne detection in CV QKD, can be advantageously generated locally instead of being sent through the channel [17–19], the light arriving from the channel will not have a bright component, which complicates beam manipulations and may deem auxiliary bright modes necessary.

The multimode structure of bright coherent light is imposed by the limitations on the modulation, that can be applied in CV QKD, which is caused by imperfect post-processing [12,20]. Thus the modulated signal must remain relatively dim and the high brightness can only be provided by the additional modes. However, mode mismatch can be present in the detection when some of the modes emitted by the source do not match the LO modes, which results in quadrature noise and limits the secure distance of the protocols [16]. Therefore, in this paper we analyze the applicability of CV QKD using bright multimode coherent states, containing up to 10^5 photons, which is much larger than tens of photons used in the existing implementations of CV QKD [20–24]. We consider the role of bright mode mismatch and show how its negative effect can be reduced. In order to comply with the security proofs for CV QKD, we keep to the quantum description of bright multimode light, resulting in the noise due to the mode mismatch. In our work we consider joint homodyne detection of incoming modes, which is much more feasible than discrimination between the modes. However, the LO should match the signal modes despite the joint measurement. Even in such simplified scenario we experimentally confirm the possibility to select signal modes and reduce the noise arising from the mode mismatch by increasing the brightness of the local oscillator beam, serving as a phase reference for the homodyne detection. This is particularly important for QKD because the unmatched modes can be tampered with by a potential eavesdropper. The resulting noise has therefore to be assumed untrusted; this has a strong impact on the security of CV QKD with bright multimode light as a side channel in the receiving station [25]. Using the obtained results we predict the performance of CV QKD with bright multimode coherent light and confirm its feasibility.

2. Homodyne detection of bright states with mode mismatch

We first study the homodyne detection of macroscopically bright light that consists of multiple modes. In the detection setup, multiple modes in the signal are not perfectly overlapped with the modes of the LO beam, which serves as a phase reference for the measurement. These unmatched modes add extra noise to the measurement results [16]. This problem was tested in our experiment with a simplified version of the homodyne detection of bright multimode coherent light.

In contrast to the standard scheme of homodyne detection (Fig. 1, left), where the LO overlaps with a single mode of the radiation, we study the basic case when the input beam contains two modes (Fig. 1, right), being in the coherent states. One of the modes (in the state $|\alpha\rangle$) is properly overlapped with the LO, the other one (in the state $|\beta\rangle$) is not. As theoretically shown in [16], in this case the measured variance of, e.g., amplitude quadrature $\hat{x}_i = \hat{a}_i^\dagger + \hat{a}_i$ in the i-th signal mode is influenced by additional noise coming from the modes that are not matched with the LO. In the general case of M matched modes and N unmatched modes of a multimode state, the measured variance of the difference photocurrent of the two detectors (normalized to the measured vacuum variance) is

$$Var\,(x)_{meas} = Var(x) + \varepsilon_{tot}^2 \overline{n}, \tag{1}$$

where $Var(x)$ is the quadrature variance of the matched signal modes (being $Var(x) = 1$ for pure coherent states, also referred to as the shot-noise unit, SNU, using the above given quadrature definition), $\overline{n}$ is the mean number of photons in an unmatched signal mode, and

$$\varepsilon_{tot}^2 \equiv \frac{N\varepsilon^2}{M\,|\alpha_{LO}|^2}, \tag{2}$$

where $|\alpha_{LO}|^2$ is the mean photon number of the LO and ε is the weight of the unmatched modes, corresponding, e.g., to filtering prior to detection.

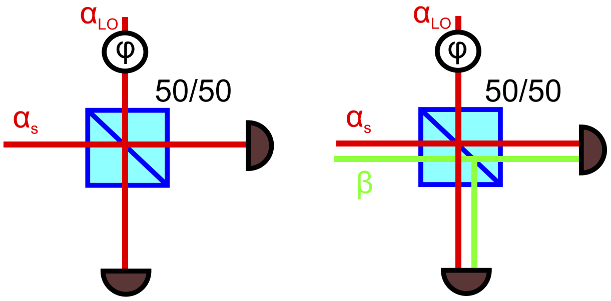

Fig. 1. The standard scheme for homodyne detection (left) and the scheme with uncompensated modes in the multimode signal beam (right).

In the simplified version realized in our experiment, there was one matched and one unmatched mode, both being coherent beams. In this case, instead of Eq. (1), one should have

$$Var\,(x)_{meas} = 1 + \frac{|\beta|^2}{|\alpha_{LO}|^2}, \tag{3}$$

which is equivalent to having $\varepsilon^2_{tot} = 1/|\alpha_{LO}|^2$. Equations (1)–(3) show that the result of the Gaussian measurement of the multi-mode bright signal is equivalent to the measurement of a one-mode dim signal (containing few photons on average, which for a CV QKD implementation would be imposed by an imperfect post-processing, that limits the modulation depth [12]) with a bright unmatched mode, containing more than 10^5 photons on average. The bright unmatched mode manifests itself in the form of extra noise that contributes to the overall quadrature noise (in contrast to a possible background radiation arriving at the homodyne detector, which does not match the LO but is as well too weak to non-negligibly contribute to the quadrature noise). The extra noise induced by imperfect modes matching depends on the ratio of brightness (mean photon number) of unmatched mode to LO brightness.

The above given results were verified in the experiment. The setup is shown in Fig. 2. We used picosecond-pulsed radiation of Ti:sapphire laser with the wavelength 800 nm and 5 kHz repetition rate. After a half-wave plate HWP1 and a polarizing beamsplitter PBS1, the beam was split into a stronger one, further used as LO, and a weaker one, further used as a coherent state under test. The latter was controlled in intensity by means of a half-wave plate HWP2 and a film polarizer, and then split into two spatially displaced beams in a calcite beam displacer oriented at 45° to the vertical direction. The intensity ratio between the two spatially displaced beams, whose role was to mimic the two independent coherent modes, was controlled by means of polarizer orientation. One of the two modes was spatially overlapped with the LO on another polarizing beamsplitter PBS2, while the other one was spatially separated from the LO, which defined mode matching and unmatching, respectively. The losses arising in the PBS2 do not spoil the measurement, because the modes under test are coherent. Finally, because the LO and the coherent mode were orthogonally polarized, they were projected on the same polarization direction on the polarizing beamsplitter PBS3, where, at the same time, both beams were split and directed at two detectors D1 and D2 for homodyne detection. The balancing of the homodyne detection scheme was performed using the half-wave plate HWP3. As D1 and D2, we used charge-integrating detectors based on p-i-n diodes [26]. Their output pulses, scaling as the photon numbers in the input light pulses, were digitized in an Analog-to-Digit Converter (ADC) and then numerically subtracted to obtain the signal.

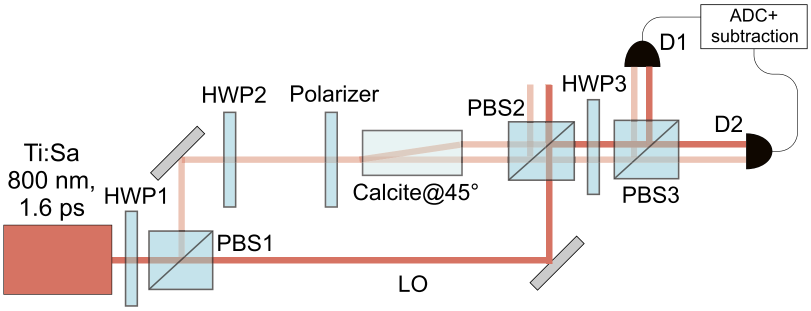

Fig. 2. The experimental setup used for the test of homodyne measurement of bright multimode coherent light.

The experimental results are shown in Fig. 3 along with the theoretical prediction given by Eq. (3). In agreement with the theory, the variance of the difference signal (quadrature variance, normalized to the variance of vacuum measurements) depends linearly on the mean photon number in the unmatched mode (normalized to the LO power of $1.04 \cdot 10^5$ mean photons), as can be seen from Fig. 3 (left panel). This fact can considerably reduce the applicability of bright multimode radiation to CV QKD. As a remedy against the increase in the quadrature variance, one can increase the LO brightness. The corresponding dependence of the normalized quadrature variance on the LO power (in terms of the mean photon number normalized to that of the unmatched mode, being $1.1 \cdot 10^5$) is given in Fig. 3 (right panel), along with the theoretical line defined by Eq. (3). Note that our system was optimized to work in the linear regime in the tested range of LO brightness between 10^5 and $2 \cdot 10^6$ photons on average, but the further drastic increase of LO brightness may lead to nonlinear detection regime. It is evident from the plot, that the experimental results are well matching the theory and that by ten-fold increase in the LO mean photon number the additional noise is reduced from 0.6 SNU to 0.06 SNU. Our results therefore confirm that the excess noise in the quadrature variance scales as the brightness of the unmatched mode (Fig. 3, left) and as the inverse brightness of the LO (Fig. 3, right). The coefficient ε^2 in our scheme was equal to 1, because no additional filtering, aimed at reducing the impact of the unmatched modes, was performed.

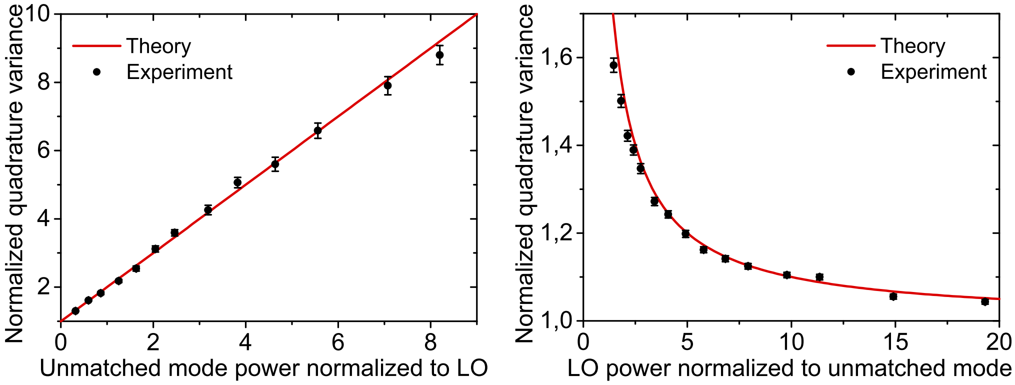

Fig. 3. Dependence of the normalized variance in SNU, experimentally measured (points) and theoretically predicted, according to Eq. (3) (lines), on unmatched mode power (left panel) and on LO power (right panel).

This was confirmed in various settings, including and excluding the unmatched mode, as shown in the histograms in Fig. 4, plotted for an intermediate LO setting with the power, normalized to the power of the unmatched mode, of 6.25, the latter having $1.14 \cdot 10^5$ mean photon number. Note that the measured quadrature variance of the coherent sate $|\alpha\rangle$ was slightly above 1 SNU. It is evident from the histograms, that the appearance of an additional bright mode in the state $|\beta\rangle$ leads to a drastic increase of the detected quadrature noise, even though the mode is not matched to the LO. This increase is observed both in the absence of the signal (i.e., at $|\alpha|^2 = 0$) and in its presence (i.e., when $|\alpha|^2 > 0$). Note that the coherent state $|\alpha\rangle$ representing the signal in our experiment was dim (as it would be in a practical CV QKD implementation), containing few photons on average. The experimental verification gave us an estimate of the multimode homodyne detection for $N = M = 1$ unmatched and matched modes, respectively, in the absence of the filtration prior to detection, i.e., with $\epsilon = 1$.

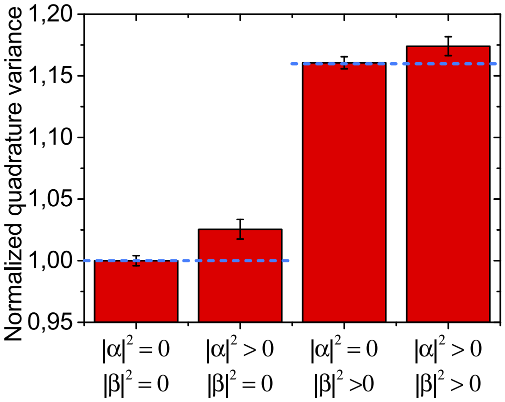

Fig. 4. Normalized variance of the quadrature measurements in SNU in the absence and presence of matched $|\alpha\rangle$ and unmatched $|\beta\rangle$ modes, $|\beta|^2 = 0.16|\alpha_{LO}|^2$. Theoretical prediction according to Eq. (3) is given in blue dashed lines.

Normalized variance of the quadrature noise in Fig. 3 (right) decreases with $|\alpha_{LO}|^2$. However, the impact of a small residual noise can be still detrimental in applications such as CV QKD. Therefore, we apply the experimentally obtained results and parameters in order to evaluate the performance of CV QKD with multimode bright coherent states.

3. CV QKD with bright multimode coherent states and mode mismatch

Based on the experimental evidence obtained in the previous Section we can evaluate the feasibility of CV QKD with bright multimode coherent states using homodyne detection. We consider prepare-and-measure CV QKD protocol based on Gaussian modulation of multimode coherent states of light and homodyne detection, and analyze its security against collective attacks (which also implies security against general attacks in the asymptotic limit [27] and can be directly extended to finite-size regime up to data-size-dependent correction to the key rate [28,29]). In this protocol, the sender, Alice, modulates coherent states according to two Gaussian distributed zero-centered random variables by applying random quadrature displacements with variance V_M, further referred to as the modulation variance. The signal states travel through the quantum channel to a remote party, Bob, who performs quadrature detection in either of the conjugate quadratures: above defined $\hat{x} = \hat{a}^\dagger - \hat{a}$ or $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, so that Alice and Bob estimate the channel parameters and evaluate the information leakage. The channel is parametrized by transmittance T, which stands for the ratio of the signal coupling to a vacuum mode, corresponding to the signal loss, and the excess noise V_N, which contributes to the overall variance of the modulated signal upon channel transmittance. Both the excess noise and the noise due to losses are attributed and assumed to be fully controlled (purified) by an eavesdropper Eve. We assess the security of the scheme by evaluating the lower bound on the secure key rate in the reverse reconciliation scenario (which is known to be robust against high loss and is therefore suitable for long-distance quantum communication [21]). The key rate reads

$$K = max\{0, \zeta I_{AB} - \chi_{BE}\}, \tag{4}$$

where $\zeta \in (0,1)$ is the post-processing efficiency, which shows how close the trusted parties are able to reach I_{AB}, the classical (Shannon) mutual information shared between Alice and Bob, and χ_{BE} is the Holevo bound. The latter upper-limits the information accessible to Eve on Bob's measured data and is relevant in the reverse reconciliation scenario. Following the optimality of Gaussian attacks and the purification-based approach to security analysis, we evaluate I_{AB} and χ_{BE} from the covariance matrix of the equivalent entangled state shared between Alice and Bob. The evaluation is in terms of von Neumann entropies, obtained from symplectic eigenvalues of the covariance respective matrices (see details on covariance matrix formalism for Gaussian states in [30] and on symplectic security analysis in CV QKD in [31]). The influence of the multimode structure and the mode mismatch then consists in the contribution of the respective detection noise $\varepsilon_{tot}^2\overline{n}$ to the excess noise induced by the channel. As it was mentioned, since Eve can tamper with the unmatched modes, the noise contribution from these modes has to be assumed untrusted. Then the two-mode covariance matrix, which corresponds to the CV QKD protocol with multimode coherent light and homodyne detection with mode mismatch, reads

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & \left[T(V+V_N)+1-T+\varepsilon_{tot}^2\overline{n}\right]\mathbb{I} \end{pmatrix}, \tag{5}$$

where $V = 1 + V_M$, the diagonal matrices $\mathbb{I} = diag(1,1)$ and $\sigma_z = diag(1,-1)$ are the unity matrix and the Pauli z-matrix, respectively. Now if Alice conducts heterodyne measurement on mode A, matrix Eq. (5) corresponds to the purification of the prepare-and-measure scheme with multimode coherent states and detection mode mismatch. The mutual information then straightforwardly reads $I_{AB} = (1/2)\log_2(1+\Sigma)$, where $\Sigma = T(V-1)/(1+TV_N+\varepsilon_{tot}^2\overline{n})$ is the signal-to-noise ratio. Now, using symplectic security analysis methodology we evaluate and plot the lower bound on the key rate Eq. (4).

In our analysis we consider two different scenarios: i) when only matched modes are modulated, while the unmatched ones remain in the bright coherent state and ii) when all the modes are modulated. The two scenarios can in principle be combined so that part of the modes are modulated and a nonequivalent part of the modes is matched to a generally multimode LO. However, if the same modulation is applied to the signal modes and some of the modes do not arrive at the detection, this may lead to side channels concerned with excessive modulation in CV QKD [32] and should be avoided. In our work we therefore study the cases when either only matched modes or all the modes are modulated and the modulation is different in different modes so that the side channel is ruled out (independent multimode modulation and joint homodyne detection is discussed in context of CV QKD in [15]). In the first scenario the contribution from different modes can be effectively joined into one mode up to the scaling of the mean photon number. Indeed, the mean photon number of the multimode coherent state, containing N modes with $\overline{n}$ mean photons in each, has the mean total of $N\overline{n}$ photons. In the second scenario the overall brightness of the unmatched modes will be defined by the total number of modes and by the modulation variance. This is because the latter is related to the mean photon number in the modulated mode as $V_M = 2\overline{n}$, because Gaussian modulated coherent states have thermal quadrature distribution. Therefore, in either of the scenarios the same amount of detection noise would correspond either to different total unmatched modes brightness or to different number of modes for given modulation variance V_M, which we optimize to improve the performance of the protocols at given parameters (first of all, the efficiency ζ). The results are given in Fig. 5 versus the LO brightness, as set in the experiment (left panel) and versus total signal beam brightness at the maximum reached LO brightness of 10^6 photons (right) at $T = 0.5$, which would correspond to a few kilometers long free-space channel [33–35] (or cca. 15 kilometers of the telecom fiber with attenuation of -0.2 dB/km). The modulation variance V_M is optimized for the given settings, the error correction efficiency is $\zeta = 0.96$ (which complies with the current post-processing techniques [36]). In Fig. 5 (left) we evaluate the key rate Eq. (4) for the experimentally obtained values of noise (points with error bars corresponding to the uncertainty of the noise estimation) and theoretically predict the key rate for the quadrature variance calculated as in Eq. (1) with $\varepsilon_{tot}^2 = 1/|\alpha_{LO}|^2$ as observed in the experiment (solid lines). We compare it to the ideal case of the perfect matching (horizontal solid lines), the key rate with mode mismatch then approaches the one with a perfect matching for higher LO intensities. In Fig. 5 (right) we theoretically evaluate the key rate Eq. (4), similarly predicting the measured quadrature variance Eq. (1) for the given LO brightness and varying the brightness of the unmatched modes. It is evident from the plots in Fig. 5 (left) that for relatively low attenuation (higher values of T) the key rate saturates with the brightness of the LO (similarly to the saturated decrease of the normalized variance in Fig. 3, right) and that 10^6 photons on average in the LO mode should be sufficient for CV QKD with the same brightness in the unmatched modes. Stronger attenuation (lower values of T) however puts higher demand on the LO brightness, which should contain at least one order of magnitude more photons on average to provide non-negligible key rates. Similarly, for a fixed LO brightness and transmittance $T = 0.5$, corresponding to a mid-range free-space channel, we show how the key rate is continuously degraded with the increase in the brightness of the unmatched modes and is bound by cca $8 \cdot 10^4$ mean photons (equivalent to $1.5 \cdot 10^4$ modes with a weak optimized modulation on the order of a few SNU) at the maximum LO brightness. This limitation is even more strict once the LO brightness is lower. However, already at 10^4 photons (or $2 \cdot 10^3$ modulated modes) the performance of CV QKD with bright coherent states and a bright LO is comparable (with the key rate being roughly 15% lower) to that with the conventional low-energy signal. Thus we have shown that coherent-state CV QKD is possible at very high brightness, even despite the mode mismatch, in either of the modulation scenarios, i.e., if all the modes or only matching modes are modulated, provided a bright LO is used. The applicability of the method can be limited by nonlinear detection response for very high brightness, but we demonstrated drastic reduction of excess noise concerned with mode mismatch already in the accessible linear regime. Increase of LO brightness can therefore be a feasible alternative to filtering of unmatched modes as the latter would increase set-up complexity and additionally attenuate the matched signals. Note that we consider the LO brightness at the detection input. In order to maintain such a strong LO, either proportionally higher brightness is needed at the channel input or the "local" LO scheme [17–19] with a locally generated LO can be applied. Furthermore, for a heavily multimode light the coupling efficiency between the signal and LO or vacuum may vary and be not exactly balanced for some modes, which may lead to slight increase of the noise concerned with unmatched modes observed in the detection [16].

In addition to the increase of the LO brightness, the trusted parties may also increase the number of matched modes M by properly constructing the multimode modulated signal and LO states. It is evident from Eqs. (1) and (2) that this would reduce the quadrature excess noise concerned with the mode mismatch in the detection. For example, the use of $M = 10$ matched modes would then be equivalent to increase of the LO brightness by the factor of ten, allowing to achieve key rates as shown in Fig. 5 (left) for $2 \cdot 10^6$ LO mean photon number upon much weaker LO of $2 \cdot 10^5$ photons on average. This illustrates the promising application of signal multiplexing in CV QKD even for a homodyne detector with joint measurement of the multiple signal modes. The obtained results can be further combined with the use of bright nonclassical states [16,26],

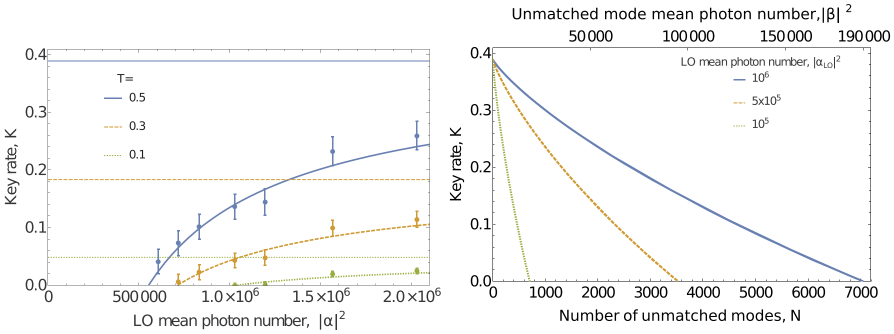

Fig. 5. Left: the key rate for multimode coherent-state CV QKD in the presence of mode mismatch versus the LO brightness at different values of the channel transmittance T, obtained from the experimentally measured noise (points with error bars) and from the calculated quadrature variance Eq. (1), $N/M = 1$ (lines). The straight horizontal lines represent the ideal case where all the modes match perfectly. Right: the key rate for multimode coherent-state CV QKD in the presence of mode mismatch (theoretically evaluated using Eq. (1) for the given parameters) versus the unmatched mode brightness, $|\beta|^2$, when only the matched mode is modulated, or, equivalently, versus the number of unmatched modes, N, when all the modes are modulated, and the LO brigthness is varied, $T = 0.5$. In both plots, the modulation variance is optimized, $\zeta = 0.96$ and $\epsilon^2 = 1$ as confirmed in the experiment.

broadband homodyne detection [37] and channel multiplexing [38] to increase secure key rate of the CV QKD protocol with bright light. Although in our work we have addressed spatially multimode light, frequency modes can be considered as well. Furthermore, the broadband signal can be combined with multimode homodyne detection, addressing the modes individually [39], in order to further improve the key rate of bright-light CV QKD using signal multiplexing.

4. Conclusion

In a proof-of-principle experiment we have demonstrated the homodyne detection of bright multimode coherent light with some of the modes not matching the local oscillator. We have shown that their influence leads to the noise in the measurement, which, however, can be overcome by increasing the LO brightness. These tests, along with the numerical modeling, confirm the feasibility of quantum key distribution with macroscopically bright (intense and multimode) coherent states, which can be now fully implemented in real optical channels. Indeed, we show that key rates of about 0.25 bits per channel should be achievable with the states containing 10^4 photons at attenuation of 50%, which corresponds to a few kilometers long atmospheric link [33–35] (or 15 kilometers of a telecom fiber) and at local oscillator brightness of 10^6 photons, so that the key rate is only 15% reduced compared to the standard quantum key distribution with low-energy signals. In addition to increasing the LO brightness, the trusted parties can suppress the noise, concerned with the mode mismatch, by increasing the number of matched modes, which shows the potential of multiplexed continuous-variable quantum key distribution even in the case of join measurement of the multiple signal modes. Our results therefore demonstrate that quantum key distribution can be realized with beams similar to classical ones and thus shift quantum cryptography even closer to classical optical technology.

Funding

Grantová Agentura České Republiky (19-23739S); Ministerstvo Školství, Mládeže a Tělovýchovy (7AMB17DE034, LTC17086); European Cooperation in Science and Technology (CA15220);

Deutscher Akademischer Austauschdienst (57319488); Univerzita Palackého v Olomouci (IGA-PrF-2019-010); Horizon 2020 Framework Programme (820466 'CiViQ').

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
3. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**(1), 16025 (2016).
4. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," arXiv:1906.01645[quant-ph] (2019).
5. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proceedings of International Conference on Computers, Systems and Signal Processing* (IEEE, 1984), pp. 175–179.
6. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
7. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**(1), 010303 (1999).
8. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**(5), 057902 (2002).
9. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," Phys. Rev. Lett. **93**(17), 170504 (2004).
10. V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**(6), 062337 (2015).
11. R. García-Patrón and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," Phys. Rev. Lett. **102**(13), 130501 (2009).
12. V. C. Usenko and R. Filip, "Squeezed-state quantum key distribution upon imperfect reconciliation," New J. Phys. **13**(11), 113007 (2011).
13. L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," Nat. Commun. **3**(1), 1083 (2012).
14. M. Lasota, R. Filip, and V. C. Usenko, "Robustness of quantum key distribution with discrete and continuous variables to channel noise," Phys. Rev. A **95**(6), 062312 (2017).
15. V. C. Usenko, L. Ruppert, and R. Filip, "Entanglement-based continuous-variable quantum key distribution with multimode states and detectors," Phys. Rev. A **90**(6), 062326 (2014).
16. V. C. Usenko, L. Ruppert, and R. Filip, "Quantum communication with macroscopically bright nonclassical states," Opt. Express **23**(24), 31534–31543 (2015).
17. D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**(4), 041010 (2015).
18. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**(4), 041009 (2015).
19. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," Opt. Lett. **40**(16), 3695–3698 (2015).
20. J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**(4), 042305 (2007).
21. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**(6920), 238–241 (2003).
22. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**(5), 378–381 (2013).
23. D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 mbps secure key rate," Opt. Express **23**(13), 17511–17519 (2015).
24. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**(1), 19201 (2016).
25. I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," Phys. Rev. A **93**(3), 032309 (2016).
26. T. Iskhakov, M. V. Chekhova, and G. Leuchs, "Generation and direct detection of broadband mesoscopic polarization-squeezed vacuum," Phys. Rev. Lett. **102**(18), 183602 (2009).
27. A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," Phys. Rev. Lett. **110**(3), 030502 (2013).
28. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**(6), 062343 (2010).
29. A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction," Phys. Rev. Lett. **118**(20), 200501 (2017).

30. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**(2), 621–669 (2012).
31. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: A threat and a defense," Entropy **18**(1), 20 (2016).
32. I. Derkach, V. C. Usenko, and R. Filip, "Continuous-variable quantum key distribution with a leakage from state preparation," Phys. Rev. A **96**(6), 062309 (2017).
33. V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, "Entanglement of gaussian states and the applicability to quantum key distribution over fading channels," New J. Phys. **14**(9), 093048 (2012).
34. D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, O. Bayraktar, and C. Marquardt, "Free-space quantum links under diverse weather conditions," Phys. Rev. A **96**(4), 043856 (2017).
35. I. Derkach, V. C. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels," arXiv:1809.10167 [quant-ph] (2018).
36. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a gaussian modulation," Phys. Rev. A **84**(6), 062317 (2011).
37. Y. Shaked, Y. Michael, R. Z. Vered, L. Bello, M. Rosenbluh, and A. Pe'er, "Lifting the bandwidth limit of optical homodyne measurement with broadband parametric amplification," Nat. Commun. **9**(1), 609 (2018).
38. T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels," Commun. Phys. **2**(1), 9 (2019).
39. G. Ferrini, J. P. Gazeau, T. Coudreau, C. Fabre, and N. Treps, "Compact gaussian quantum computation by multi-pixel homodyne detection," New J. Phys. **15**(9), 093015 (2013).