PHOTONICS Research

Frequency-multiplexed entanglement for continuous-variable quantum key distribution

Olena Kovalenko,[1,*] Young-Sik Ra,[2,3] Yin Cai,[2,4,5] Vladyslav C. Usenko,[1] Claude Fabre,[2] Nicolas Treps,[2] and Radim Filip[1]

[1]Department of Optics, Palacky University, 77146 Olomouc, Czech Republic
[2]Laboratoire Kastler Brossel, Sorbonne Université, CNRS, ENS-Université PSL, Collège de France, 75252 Paris, France
[3]Department of Physics, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, Republic of Korea
[4]Key Laboratory for Physical Electronics and Devices of the Ministry of Education & Shaanxi Key Laboratory of Information Photonic Technique, Xi'an Jiaotong University, Xi'an 710049, China
[5]e-mail: caiyin@xjtu.edu.cn
*Corresponding author: kovalenko@optics.upol.cz

Received 24 June 2021; revised 4 October 2021; accepted 5 October 2021; posted 5 October 2021 (Doc. ID 434979); published 12 November 2021

Quantum key distribution with continuous variables already uses advantageous high-speed single-mode homodyne detection with low electronic noise at room temperature. Together with continuous-variable information encoding to nonclassical states, the distance for secure key transmission through lossy channels can approach 300 km in current optical fibers. Such protocols tolerate higher channel noise and also limited data processing efficiency compared to coherent-state protocols. The secret key rate can be further increased by increasing the system clock rates, and, further, by a suitable frequency-mode-multiplexing of optical transmission channels. However, the multiplexed modes couple together in the source or any other part of the protocol. Therefore, multiplexed communication will experience cross talk and the gain can be minuscule. Advantageously, homodyne detectors allow solving this cross-talk problem by proper data processing. It is a potential advantage over protocols with single-photon detectors, which do not enable similar data processing techniques. We demonstrate the positive outcome of this methodology on the experimentally characterized frequency-multiplexed entangled source of femtosecond optical pulses with natural cross talk between eight entangled pairs of modes. As the main result, we predict the almost 15-fold higher secret key rate. This experimental test and analysis of frequency-multiplexed entanglement source open the way for the field implementation of high-capacity quantum key distribution with continuous variables.

https://doi.org/10.1364/PRJ.434979

1. INTRODUCTION

Quantum key distribution (QKD) [1] is a pioneering application of quantum information theory enabled by fundamental particle and wave quantum features of light. Advantageously, in experiments at optical wavelengths, QKD can exploit complementary photon counting and homodyne detection methods of quantum optics. Naturally, both methods have advantages and disadvantages, fundamental as well as technical. Therefore, optimal implementation of a quantum-secure network will be likely hybrid in the future, combining advantages and suppressing the weaknesses of different protocols respectively to the requirements and conditions [2]. Currently, homodyne detection is fast, efficient, with extremely low-noise, and tolerant to background noise in the channel [3]. This hardware already opened space for a high-speed secret key generation. For a long time, the homodyne detection stimulated a large set of theoretical proposals [4–6] and experimental protocols with coherent states of light [7–12]. With nonclassical squeezed and entangled states, the continuous-variable (CV) protocols [13–15] become more robust and potentially applicable at distances up to 300 km [16] in optical fibers with attenuation 0.2 dB per kilometer, and tolerant to data processing inefficiency [17]. Such protocols can be advantageously implemented in both optical fiber links [16] and free-space atmospheric channels with realistic turbulence [18]. Moreover, higher security can be offered by relaxing the assumption about trusted devices for both coherent-state and entanglement-based protocols, as it was demonstrated by implementation of one-sided device-independent protocols [19,20].

A rate of secret key can be increased in CV QKD by frequency multiplexing of transmission channels [21]. Frequency (wavelength) multiplexing is a well-known technique from classical optical communications [22], also with the homodyne detection [23]. It can be similarly considered to increase the secret key rate of CV QKD protocols and has recently been studied using Gaussian modulation of frequency comb states

[24], as well as using independent lasers for each mode for subsequent discrete [21] or Gaussian modulation [25]. In this paper we test the entanglement-based CV QKD protocol that uses multiple frequency modes to multiplex the signal. However, in practice generated multiple entangled modes can become mutually coupled to each other, resulting in cross correlations as well as excess noise in the modes that can be destructive for CV QKD. Importantly, homodyne detection of field quadratures gives sufficient information about states of light in the individual modes in order to compensate for the cross talk. Based on these advantages, a cross-talk elimination based on state or data manipulations has been addressed in Refs. [26,27] demonstrating that such a limiting factor for multiplexed QKD can be in principle deterministically eliminated by optimized data manipulation, using the whole multimode structure (contrary to modes selection, e.g., used to improve quantum steering in Ref. [28]). Different to protocols with single-photon detectors, it is therefore not required to implement an active strategy of optical decoupling which is very challenging for a large number of transmitted modes.

Nowadays, CV QKD reaches a new level at which a substantial increase of secret key rate of mid-range protocols is a relevant target of the ongoing development and requires, in particular, development of cross-talk elimination methods. The previously suggested methods either required heterodyne detection with optimal engineering of auxiliary input states and were not applied to CV QKD security analysis [26] or considered only cross-talk interaction between the neighboring modes of the otherwise perfect entangled states [27]. In the current paper we suggest the multimode cross-talk compensation method based on data manipulation, equivalent to linear state manipulations, experimentally test it on the real multiplexed entangled states measured with the mode-discriminating homodyne detection suitable for CV QKD, and evaluate security of the resulting CV QKD protocol. Without such a test on the multimode state with real cross talk and errors it is impossible to estimate applicability of the cross-talk compensation for a large number of modes. A positive result demonstrating that secret key rate can be enhanced by channel multiplexing with high efficiency, despite cross talk substantially reducing the achievable key rate already in the source, is necessary to open a pathway for further implementations and applications of frequency-multiplexed CV QKD. For the test we use simultaneously frequency-multiplexed source of entanglement with eight pairs of modes and mode-discriminating homodyne detection. For them, the cross talk is a very natural phenomenon pronouncedly reducing the key rate to a tiny number of 0.015 bits. We suggest and apply optimized data manipulation, which allows decoupling of modes under cross talk and brings large improvement to an achievable secret key rate. The secret key rate can be enhanced by almost a factor of 15. Reducing the channel noise in all frequency-multiplexed channels by this data manipulation, alternatively, can extend the secure distance (channel range at which generation of the secret key is still possible) by approximately 100 km. Moreover, as the source emits femtosecond pulses, allowing for high system clock rates, the performance of the system can be also further increased by time multiplexing. Our result solves the major problem of mode cross talk in the source; however, it can be equally applicable to cross talk in the link and detection (although the mode coupling inside an optical fiber is weak, if present at all, hence one can expect the mode interaction in the source to be the dominating cause of cross talk). Therefore, it opens the possibility for high-speed and high-capacity entanglement-based CV QKD with femtosecond frequency-multiplexed states.

2. RESULTS

We consider the use of an entanglement source in the multimode CV QKD testbed based on the frequency-multiplexed femtosecond pulses of light, consisting of 16 modes and with mode-discriminating homodyne detection, as described in Fig. 1. In our proof-of-principle experiment, all the 16 modes are generated in a single beam, and to test the applicability of the source for QKD purpose, we assume that the lower half of the frequency modes are distributed to Alice, and the other half are to Bob.

The experimental setup is shown in Fig. 2. The main laser is a Ti-sapphire pulse laser, having a duration of 120 fs centered at λ_0 (=795 nm) with a repetition rate of 76 MHz. The beam from the laser splits into two beams, where one is used for generating frequency-multiplexed entangled light, and the other serves as a local oscillator (LO) for mode-discriminating homodyne detection. To generate the entangled light, we employ a synchronously pumped optical parametric oscillator (SPOPO) including a 2 mm thick BiB_3O_6 (BiBO) crystal, which operates below the threshold [29,30]. The pump laser for the SPOPO (centered at $\lambda_0/2$) is prepared by second-harmonic generation

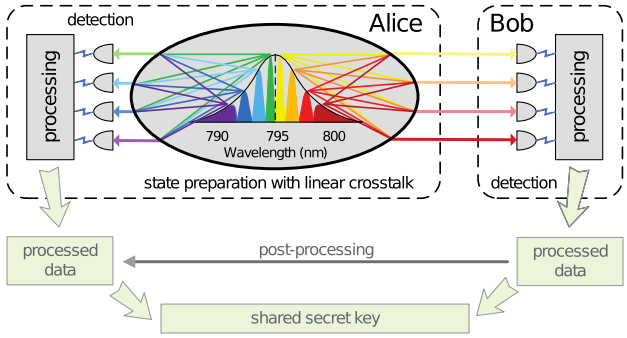

Fig. 1. Bright colors show a sketch of a CV QKD testbed for the study of the multimode entangled source at the side of the sender, Alice, with cross-talk coupling between the frequency modes in both of the two beams, leaving the source. The entangled source is based on eight pairs of modes, where only four of them are shown for clarity. We consider a scenario where half of the modes (below the central frequency) are locally measured by Alice and another half (above the central frequency) transmitted to a remote trusted party Bob (trusted devices are given in dashed blocks). Both multimode beams are detected by homodyne detectors and processed to optimally eliminate the cross talk and improve the secret key rate. The data processing corresponds to a local physical multimode symplectic transformation and was optimized to achieve higher key rate between the trusted parties. The trusted parties then can use authenticated classical channel to perform post-processing by correcting their errors and amplifying the data privacy in order to obtain quantum-secure key as the result (this part of the protocol was modeled numerically so is illustrated in pale colors).

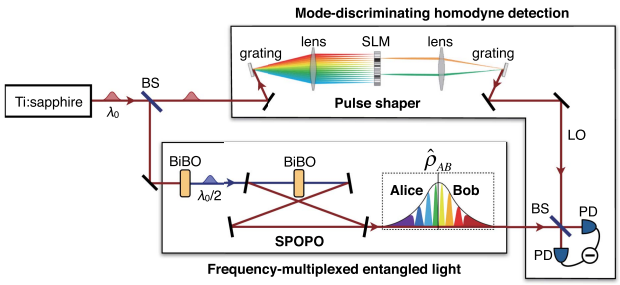

Fig. 2. Experimental setup for generation of frequency-multiplexed multimode entangled light and its measurement with mode-discriminating homodyne detection. The generated multimode light $\hat{\rho}_{AB}$ is in 16 frequency modes, where Alice (A) and Bob (B) access to the eight lower frequency modes and the other eight frequency modes, respectively. The pulse shaper is constructed in the folded configuration in actual implementation. BS, beam splitter; SLM, spatial light modulator; PD, photodiode. See main text for details.

of the main laser in a 0.2 mm thick BiBO crystal. As a result, an entangled state of femtosecond pulses of light in multiple frequency modes (centered at λ_0) is generated in a single beam, and the efficiency of the process is enhanced by the cavity constituting the SPOPO. For our purpose, we consider 16 frequency-band modes of the generated multimode light and assume that the lower half (eight) frequency modes are measured by the trusted sender Alice, while the other half frequency modes are measured by the trusted receiver Bob after a multimode channel. We stress that even if in practice this separation is not performed in the current experiment, spectrally splitting a beam in two halves can be readily done experimentally with a simple dispersive element, such as a grating, a dichroic mirror, or a prism. It is possible to use a high-efficiency grating or prism, or fiber-based wavelength-division multiplexing [31]. These dispersive elements would introduce only small additional losses, leading to the excess noise in the generated multimode states. Such noise can be however considered trusted and will only have a limited negative effect on the key distribution [32].

To measure the generated multimode state, we use homodyne detection which can discriminate different frequency modes. As the LO of homodyne detection determines the frequency mode, we control the LO based on a pulse shaping technique. For this purpose, a pulse shaper in the 4-f configuration is employed: an input beam is diffracted by an optical grating (1200 grooves/mm), which is subsequently focused by a cylindrical lens (190 mm focal length). On the Fourier plane of the lens, a reflection-type spatial light modulator having 512 × 512 pixels controls the amplitude and the phase of frequency modes. The reflected beam comes back to the lens and the grating. The overall wavelength resolution is found to be 0.1 nm. Using the pulse shaper, a covariance matrix associated with the 16 frequency modes was obtained by measuring quadrature outcomes in a sequential way from the mode-discriminating homodyne detection; in the homodyne detection, the two photodiodes have a quantum efficiency of 99%, fringe visibility is 93%–95%, and demodulation frequency is 1 MHz [33]. The obtained covariance matrix is presented in Appendix A.

Given the resolution of the pulse shaper, we consider that all the measured modes are realistically matched to the local oscillator. It also does not limit the applicability of the method which can be applied to the cross talk in the multimode detector equally well. If the unmatched modes are present, they will contribute to noise [34] and may act as a detection side channel [35] but can be compensated for by increase of the brightness of the local oscillator [36].

To extend and verify the method of decoupling following the preliminary theoretical studies [26,27] for the source depicted in Fig. 1, we assume a typical QKD scenario, where we suppose that Alice's preparation is trusted (being fully out of control by an eavesdropper Eve) and Alice is measuring her modes locally by a multimode homodyne detector, while the Bob's modes travel directly toward his detection. Bob is measuring his modes using mode-discriminating homodyne detectors, also assumed to be trusted (including the efficiency and the electronic noise of the detectors). The ability to address the individual local modes in the homodyne detection is crucial for channel multiplexing in CV QKD and the multimode structure of entangled states can be harmful for the protocols otherwise [37]. To controllably investigate the impact of lossy channel, we applied attenuation to Bob's measured results. It emulates an untrusted channel, characterized by the transmittance T, which is assumed to be fully controlled by an eavesdropper, Eve, capable of collective attacks. We assume a purely lossy (attenuating) channel as the background noise is already very small in real optical fiber channels. Such an approach allows modeling fiber as well as free-space channels, where fluctuations due to atmospheric turbulence are typically slow compared to the signal repetition rate [38]. To comply with the experimental testbed, where the multimode source was characterized, we assume that the cross talk appears in the source, but our methodology can also be directly applied also to cross talk in the channel and detectors.

Security of CV QKD is evaluated as the positivity of the lower bound on the key rate, which, in the case of collective attacks and reverse reconciliation [5], reads

$$K = \max\{0, \beta I_{AB} - \chi_{BE}\}, \tag{1}$$

where $\beta \leq 1$ is the post-processing efficiency (further we realistically take $\beta = 96\%$, which complies with the achieved post-processing efficiency [39]), I_{AB} is the mutual classical (Shannon) information between Alice and Bob, and χ_{BE} is the Holevo bound, which upper limits the information accessible to a potential eavesdropper Eve on Bob's measurement results. We address security against collective attacks for the Gaussian entanglement-based CV QKD [40,41], which can be directly extended to the finite-size regime [42,43] and implies security against general attacks [44,45]. The reverse reconciliation is used to test secret key distribution for mid-range distance with channel attenuation below –3 dB. The positivity of the lower bound [Eq. (1)] implies that the trusted parties are able to distill the secret key with at least the rate K by using classical post-processing (error correction and privacy amplification) [46]. We therefore analyze the security of frequency-multiplexed CV QKD by evaluating the lower bound on the key rate per multimode channel use K (further also referred to as the key rate). We follow the Gaussian security proofs and

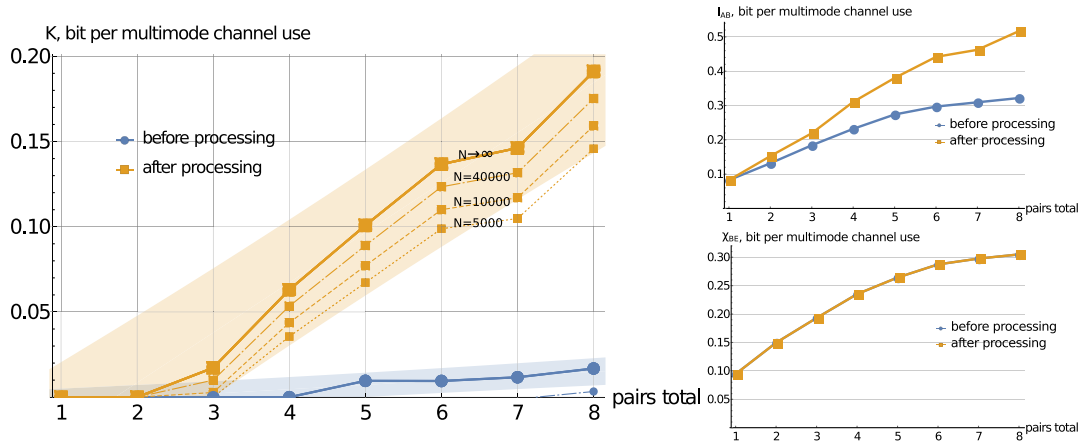

Fig. 3. Left panel: estimated key rate (in terms of bits per multimode channel use) of CV QKD based on the frequency-multiplexed entangled source in Fig. 1 for different number of pairs measured by Alice and Bob as obtained from the original data before decoupling (circles, blue lines) and after decoupling of modes involved in the multimode cross talk by optimized data processing performed by the trusted parties after the homodyne measurement (squares, yellow lines). The dotted, dotted–dashed, and dashed lines represent the pessimistic estimates that take into account standard error for the respective number of measurements $N = 5 \times 10^3$, $N = 10^4$, $N = 4 \times 10^4$, as indicated over the lines in the plots (see Appendix A for details). Note that blue non-solid lines are almost extinct on the plot. Shaded areas represent the method prediction bands with 95% confidence level in the asymptotic limit of infinitely many measurement points. Realistic reconciliation efficiency $\beta = 96\%$ taken for the processed data, perfect $\beta = 1$ taken for the original data. While multiplexing brings only small and fragile advantage when all the pairs are being used, it can be drastically improved by optimized local data manipulations, revealing power of frequency multiplexing in CV QKD. The improvement gets more pronounced as the number of data points N increases. Right panel: multimode mutual information (top) and Holevo bound (bottom) for different number of pairs measured by Alice and Bob as obtained from the original data (circles, blue line) and after optimized linear interactions performed by the trusted parties prior to the measurement (squares, yellow line). The plots illustrate the nature of improvement of frequency-multiplexed CV QKD by optimized data manipulations, which is based on increase of the mutual information, while the Holevo bound remains unchanged and, therefore, the yellow and blue points overlap.

respective security analysis methods, as described in Appendix A.

We demonstrate the power of the multimode states in CV QKD by confirming the gradual increase of the overall key rate for increasing the number of pairs of modes measured by Alice and Bob, as shown in Fig. 3 (left), assuming channel transmittance $T = 0.2$. We first rank the pairs by the key rate between the individual pairs and then add pair by pair, thereby obtaining larger key rate, as seen in Fig. 3 (left, circles and the blue solid line).

For the multimode states as shown in Fig. 1, we optimize the data processing to achieve the maximum key rate Eq. (1). The applied data processing is equivalent to local passive symplectic transformations when both the sender and the receiver separately act on their respective modes by optimized beam splitter networks [47]; see Appendix A for details. The results of the optimization are given in Fig. 3 (squares and solid yellow line) and it is evident that optimized local data manipulations lead to an almost 15-fold increase of the overall key rate for the multimode states. The optimization process can, therefore, efficiently retrieve multiple pairs of entanglement from the multimode entanglement resource, providing significant improvement for CV QKD. Moreover, the key rate becomes much more robust against statistical error in the finite data ensemble, as can be seen from the respective plots in Fig. 3 (squares and dashed yellow lines).

The improvement of multimode CV QKD by the local data processing is concerned with the increase of the multimode mutual information, as can be seen from Fig. 3 (right, top), while Holevo bound is not affected, as seen from Fig. 3 (right, bottom). Indeed, the local data processing (equivalent to symplectic transformations) does not affect the quantum entropies contributing to the Holevo bound by not changing the symplectic spectrum (i.e., thermal-state decomposition) of the multimode Gaussian state. On the other hand, redistribution of modes occupation by the local symplectic transformations increases the additive classical mutual information due to increased correlations and can be optimized to achieve the best performance. This also substantially simplifies the optimization of the method by reaching the maximum mutual information, leading to the maximum key rate. Our method is focused on maximizing mutual information (not on eliminating cross correlations) and leads to optimal improvement of the key rate. Note that our method can be advantageously combined with the protocol, in which the Holevo information, maximally accessible to Eve, is minimized [48]. In this scenario by proper multiplexing and elimination of cross talk a higher key rate can be achieved at low post-processing efficiencies, while not increasing the information leakage. This can be particularly promising for high-speed CV QKD, where fast but less efficient error correction can be otherwise a very limiting bottleneck [8,17].

3. DISCUSSION

We also analyze the robustness of CV QKD against channel attenuation (which is equivalent to channel distance) with

the full set of eight pairs of modes before and after the optimized data manipulation as shown in Fig. 4 (the eight-pair covariance matrix after optimized data processing is illustrated in Fig. 5 in Appendix A). By eliminating the cross talk, we reduce the state preparation noise in the individual channels and respectively increase the maximum tolerable channel noise. It is evident from the plot that optimized local data manipulation increases the maximum tolerable channel attenuation of the protocol from approximately 8 dB to 28 dB of loss, thus demonstrating potentially more than threefold increase of the secure distance of the multimode CV QKD protocol (assuming 0.2 dB/km loss). We extrapolate the obtained results for the cases of 25 and 50 modes, which are expected to further improve the efficiency and robustness of the CV QKD protocol up to approximately 34 and 36 dB; see Appendix A for details. We also address the efficiency of our method by comparing the achieved results to the bounds set by 8 times maximum performance of one best pair of modes (as the total number of pairs in our experiment is eight). In the way similar to maximization of the total key rate, we now run optimization to have as much as possible key in this particular pair. In terms of mutual information, the maximum in one pair is 0.28 bit per channel use, the total maximum mutual information achieved by our method is 0.517 bit per channel use, and the bound (8 times the maximum value for one pair) is 2.24 bit per channel use, which is 4.3 times larger than we achieve. For the key rate the maximum for one pair is 0.163 bit per channel use, the total achieved key rate is 0.212 bit per channel use, and the bound is 1.304 bit per channel use, which is 6.15 time larger than we achieve. We define the decoupling efficiency as the ratio between the secret key rate achieved and the secret key rate that could be achieved in a perfect setting with all eight pairs having maximal mutual Shannon information. The efficiency of our method for the secret key rate therefore reaches 0.16. This removable limitation is caused by source imperfections beyond the linear cross talk and would require development of additional advanced experimental and data processing methods to further improve practical frequency-multiplexed CV QKD. Our results show that despite drastic improvement achieved with the suggested method for cross-talk elimination, even higher performance can be achieved by larger number of frequency channels with faster data processing and by further developed experimental techniques aimed at reduction of cross talk.

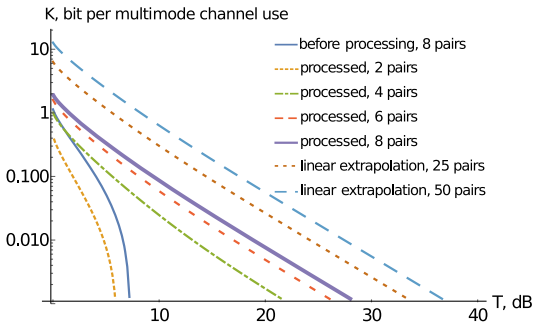

Fig. 4. Key rate of CV QKD versus channel transmittance T (in dB) as obtained from the original data on the full multimode entangled state (blue solid line), after optimized local data manipulations performed by the trusted parties for different number of used pairs of modes (non-solid lines for reduced number of pairs and thick solid violet line for the maximum number of eight pairs), linear extrapolation for larger number of modes (blue and brown dashed lines). Post-processing efficiency $\beta = 96\%$. Evidently, optimized data manipulation can drastically improve robustness to loss (and, respectively, the secure distance) of frequency-multiplexed CV QKD with entangled states.

4. SUMMARY AND OUTLOOK

By optimally applying data manipulations we were able to compensate the cross talk in the frequency-multiplexed CV QKD with femtosecond-pulsed entangled states and substantially increase the mutual information between the sets of modes, measured by the trusted parties, while the leaked information, upper bounded by a function of Gaussian quantum entropies, did not change. Thus, we can increase the achievable key rate for continuous-variable quantum key distribution or, equivalently, extend the secure distance of the protocols. The results of the optimized local data manipulations show the possibility to increase the overall key rate by almost the factor of 15 and extend the secure distance for the multiplexed entanglement-based protocol by the factor of 3. Note that while higher key rates can be as well obtained by increasing the system repetition rate, our method does not affect the information leakage and only increases the mutual information, hence drastically increasing the key. Nevertheless, our method can be further combined with the increase of the repetition rate to achieve even higher key rates. In the present demonstration, the calculations were performed on a covariance matrix obtained by mode-discriminating homodyne measurement and can be easily extended to a large number of modes [49]. Furthermore, the cross talk between the modes can also be further reduced or adapted to the measurement system manipulating the source through spectral shaping of the pump [50]. While we applied data manipulations to compensate cross talk in the multimode CV QKD source, the method can be also used to eliminate cross talk that appears in the multimode quantum channel. Our method is therefore very promising for improving key rates of continuous-variable quantum key distribution and can also be combined with the protocol based on minimization of the information leakage [48], especially with elimination of channel noise and efficient channel estimation techniques, in order to overcome the limitations imposed by realistic fast post-processing. Moreover, we can combine our method with the existing tools to eliminate correlated noise [51] and side channels [35]. We therefore open the pathway to very high-speed practical realization of quantum key distribution using continuous variables. It should be followed by a test of complete multiplexed protocol together with secret key generation and can be extended to networking entanglement-based communication settings. Furthermore, the suggested cross-talk compensation technique can be useful in other applications of continuous-variable quantum information, such as quantum imaging [52] or quantum illumination [53].

APPENDIX A

1. Security Analysis

The key rate is calculated as $K = \max\{0, \beta I_{p_{AB}} - \chi_{BE}\}$, where $I_{p_{AB}}$ is the classical information between Alice and Bob in $\hat{p} = i(\hat{a}^\dagger - \hat{a})$ quadrature (we chose it because in this experiment it gives larger key than the $\hat{x} = \hat{a}^\dagger + \hat{a}$ quadrature).

The classical mutual information for a pair of Gaussian-distributed datasets A and B with variances V_A and V_B, respectively, can be evaluated as $I_{AB} = \log_2(V_A/V_{A|B})$, where $V_{A|B} = V_A - C_{AB}^2/V_B$ is the conditional variance, which can be expressed through the correlations between the datasets, C_{AB}. It is therefore straightforward to evaluate our multimode mutual information $I_{AB} = \sum_{i=1}^{8} I_{A_iB_i}$, which is the sum of bipartite mutual information quantities between eight pairs of datasets obtained from the homodyne measurements of different frequency modes on both Alice's and Bob's sides. Note that here and further the mutual information as well as the lower bound on the key rate Eq. (1) is evaluated in bit per multimode channel use.

The calculation of the Holevo bound is more involved and is performed in the assumption that Eve is capable of collective measurement of the eight-mode state, reflected from the attenuating channel, similar to the single-mode CV QKD in purely lossy channels [54], as Eve's vacuum modes, corresponding to the loss in each of the modes, cannot be correlated. The Holevo bound is then evaluated as the difference $S(E) - S(E|B)$ between the von Neumann (quantum) entropies of the state available to Eve prior and after conditioning on the measurements of the receiving trusted party Bob. The von Neumann entropy of a state described by covariance matrix γ is calculated as $S(E) = \sum_i G\frac{\lambda_i - 1}{2}$, where λ_i are symplectic eigenvalues of γ_E and $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. Here $S(E)$ is the entropy of the eight-mode state measured by Eve, and $S(E|B)$ is the entropy of Eve's state, conditioned on the set of $\{x_{B_i}\}$, being the measurement outcomes of the homodyne detection in x-quadrature on eight modes at Bob's station (equivalently for the p-quadrature measurements). The calculation is performed in the covariance matrix formalism, within the pessimistic Gaussian state approximation (see more details on the Gaussian security analysis in Ref. [32]).

2. Error Estimation

To estimate the effects of the measurement error on the key rate, we assume that every pair of modes has bi-variate normal quadrature distributions and the covariance matrix for the i, j-pair is

$$\gamma_{ij} = \begin{pmatrix} V_i & C_{ij} \\ C_{ij} & V_j \end{pmatrix}. \tag{A1}$$

Here $V_i = \begin{pmatrix} \langle \Delta x_i^2 \rangle & 0 \\ 0 & \langle \Delta p_i^2 \rangle \end{pmatrix}$ and $C_{ij} = \begin{pmatrix} \langle x_i x_j \rangle & 0 \\ 0 & \langle p_i p_j \rangle \end{pmatrix}$, as in this experiment no correlations between quadratures were observed, hence $\langle x_i p_j \rangle = 0 \forall i,j$. The best estimate for the standard error for $\gamma_{i,j}$ after N measurements will be [55]

$$\sigma_{\gamma_{i,j}} = \frac{1}{\sqrt{N+1}} \begin{pmatrix} \sqrt{2}V_i & \sqrt{V_iV_j + C_{ij}^2} \\ \sqrt{V_iV_j + C_{ij}^2} & \sqrt{2}V_j \end{pmatrix}. \tag{A2}$$

We assume the worst case (pessimistic scenario) for different numbers of measurements and evaluate the lower bound on the secret key rate for each case. The pessimistic scenario implies that the diagonal elements of the covariance matrix (variances) are increased by the error value while the absolute values of the off-diagonal elements (correlations) are decreased [56,57]. The results are presented in Fig. 2 as dashed lines. It is evident from the plots in Fig. 2, that even multiplexing of all eight pairs can only slightly restore the nonzero key rate if the measurement results are used without any processing, and that the key rate is very sensitive to the error in the finite data samples. One can expect that the performance of the multiplexed CV QKD is strongly limited by the cross talk between the modes [27], which is likely to appear in the generation of frequency-multiplexed entangled states under study. We therefore suggest and verify the method of optimized data manipulation after the homodyne detection, performed by the trusted sides, in order to substantially compensate the cross talk and make the multimode resource more applicable for CV QKD.

3. Optimized Data Processing

Generally, all the 16 modes are getting coupled in the state preparation and such cross talk should be possible to at least partially compensate for using a global 16×16 symplectic transformation that maximizes the mutual information. The quantum communication scenario makes such global transformation impossible, but the cross talk can be significantly reduced even when we consider Alice and Bob performing only local operations independently of each other. Alice and Bob each control eight modes of the shared 16-mode state. Each of them can then introduce linear local passive operations on their respective sides in order to minimize the cross talk while preserving the security of the protocol. We are therefore looking for two 8×8 local symplectic transformation matrices equivalent to a sequence of linear optical devices.

The covariance matrix of the whole 16-mode state γ can be represented as

$$\gamma = \begin{pmatrix} V_1 & \cdots & C_{1,16} \\ \vdots & & \vdots \\ C_{16,1} & \cdots & V_{16} \end{pmatrix}, \tag{A3}$$

with V_i and $C_{i,j}$ given in Eq. (A1) and below. To model the interaction, we assume that a set of 2×2 beam splitters is introduced between all possible pairwise mode permutations on the same side, i.e., there are $(N/2 - 1)N/2 = 56$ beam splitters [58] (28 on Bob's and 28 on Alice's side). The phase convention we use for a 2×2 beam splitter acting on a 16-mode state is

$$T_{ij} = \begin{pmatrix} \mathbb{I} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \sqrt{t_{ij}}\mathbb{I} & \sqrt{1-t_{ij}}\mathbb{I} & \cdots & 0 \\ 0 & \cdots & \sqrt{1-t_{ij}}\mathbb{I} & -\sqrt{t_{ij}}\mathbb{I} & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \mathbb{I} \end{pmatrix}, \quad \textbf{(A4)}$$

where t_{ij} is the transmittance coefficient, and i, j are the modes that are interacting on the given beam splitter. Then introducing the beam-splitter network on the sender side is equivalent to Alice acting on the covariance matrix with the sequence of the beam splitter two-mode linear coupling operation: first Alice acts with $\gamma' = T_{1,2}\gamma T_{1,2}^T$, and then $\gamma'' = T_{1,3}\gamma' T_{1,3}^T$, etc. As a result, the sender (Alice) transforms the initial state with the product of 28 operators,

$$U_A = T_{7,8}T_{6,8}\ldots T_{1,3}T_{1,2} = \prod_{i=1,j=i+1}^{8} T_{i,j}, \quad \textbf{(A5)}$$

on her side and the receiver (Bob) acts in the same manner with the operation

$$U_B = T_{15,16}T_{14,16}\ldots T_{8,10}T_{8,9} = \prod_{i=9,j=i+1}^{16} T_{i,j} \quad \textbf{(A6)}$$

on his side. Their joint interaction operation is $U = U_A U_B$. After the beam-splitter network is applied to the original state, the covariance matrix becomes $\gamma_f = U\gamma U^T$.

We then calculate the mutual information $I_{x_{AB}}$ and $I_{p_{AB}}$ of the state γ_f separately in $\hat{x}$ and $\hat{p}$ quadratures and maximize the functions $I_{x_{AB}}(t)$ and $I_{p_{AB}}(t)$ numerically. Here $t = (t_{1,2}, t_{2,3}, \ldots, t_{15,16})$ is the variable vector made of transmittance coefficients of the beam splitters. There is no need to maximize the key rate, as the Holevo bound is not affected by unitary transformations (indeed, the von Neumann entropy of the states is preserved, hence the maximization of the mutual information is sufficient). The optimization was done numerically using the limited memory Broyden–Fletcher–Goldfarb–Shannon (l-BGFS) optimization algorithm with bound constraints [59] from SciPy library. The l-BGFS performs $O(d)$ computations per iteration, where d is the number of the function's variables, in this case $d = (N/2 - 1)N/2$, and the method performance scales depending on the number of the modes as $O(N^2)$. In general, l-BGFS does not converge to a global maximum if the function under maximization is not a convex one as is the case here. To find the global maximum we used the basin-hopping optimization method. Naturally there is no guarantee that each maximum we have found is indeed a global one, but the obtained results have already shown drastic improvement of quantum communication using the multimode states. The visualization of the covariance matrices before and after the optimization is given in Fig. 5, where the raw data used in the optimization are reported in Ref. [33]. It shows noticeable redistribution of correlations between the modes.

It is worth mentioning that while here we optimize the state with only passive local operations, it is also possible to use an active transformation, although it would significantly increase the computing power needed. In addition, the most general set

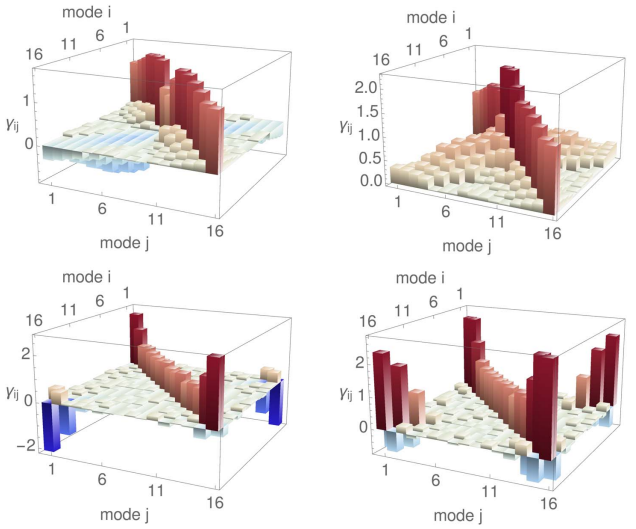

Fig. 5. Visualization of covariance matrices in $\hat{x}$ quadrature (left) and $\hat{p}$ quadrature (right) before (top) and after (bottom) the optimized linear data processing.

of passive local operations would be represented by sequence of Mach–Zehnder interferometers with beam splitters of optimized transmittance and optimized phase shifts between them. We have checked this kind of optimization setup as well, but it did not help to increase the Shannon information and the secret key rate. This is due to the fact that the correlations between $\hat{x}$ and $\hat{p}$ quadratures in the data are negligibly small.

The matrix of the optimized interaction is to be found on the parameter estimation step of the QKD protocol based on the estimation of the state, shared between the trusted parties, in terms of its covariance matrix [57]. The optimization can be performed on either the sender or the receiver side and then announced publicly. Since the optimization parameters are not related to the raw key data, no further disclosure and discarding of the key bits is needed. Eavesdropper's knowledge of the optimized interaction does not influence the security of the protocol as the security proof already assumes eavesdropper's ability to perform an optimal collective measurement on the intercepted signal [54] and the Holevo bound is not affected by the linear interactions between the signal modes on the trusted sides.

4. Results Extrapolation

We predict the efficiency of our method for larger numbers of pairs, by evaluating prediction bands, as seen in Fig. 3 (left). To do so, we first used a linear fit for the key rate results in order to predict how the key rate will behave if we add more modes. If the pairs of modes were uncorrelated (i.e., experience no cross talk) and all had the same variance, the key would grow linearly; therefore, we assume that in our case of correlated modes dependence will stay close to linear. Using the method of the least squares [60] we got a linear model for the key rate in the form $K(x) = a + bx$ (for the processed data we have $a = -0.0501$ and $b = 0.0293$). We then evaluated the prediction bands defined as $K(x) \pm t\sqrt{s^2 + X\mathrm{Cov}X^T}$, where Cov is the covariance matrix for the coefficients a and b, and s^2 is the

mean squared error for the data points, $X = \begin{pmatrix} 1 \\ x \end{pmatrix}$, t is defined from the Students distribution for 95% confidence level (resulting in $t = 2.447$).

Funding. National Natural Science Foundation of China (11904279, 12174302); European Cooperation in Science and Technology (CA 15220 QTSpace); National Research Foundation of Korea (NRF-2019R1C1C1005196)); Grantová Agentura České Republiky (19-23739S); Univerzita Palackého v Olomouci (IGA-PrF-2021-006); Ministerstvo Školství, Mládeže a Tělovýchovy (CZ.02.1.01/0.0/0.0/16_026/0008460); European Commission (708201); Horizon 2020 Framework Programme (731473 (project 8C20002 ShoQC), 820466 CIVIQ, 951737 NONGAUSS).

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data that support the findings of this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photonics **12**, 1012–1236 (2020).
2. M. Cattaneo, M. G. A. Paris, and S. Olivares, "Hybrid quantum key distribution using coherent states and photon-number-resolving detectors," Phys. Rev. A **98**, 012333 (2018).
3. Y. Chi, L. Tian, B. Qi, L. Qian, and H. Lo, *High Speed Homodyne Detector for Gaussian-modulated Coherent-state Quantum Key Distribution* (University of Toronto, 2009).
4. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).
5. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
6. 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**, 170504 (2004).
7. 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**, 238–241 (2003).
8. 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**, 042305 (2007).
9. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**, 045023 (2009).
10. 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**, 378–381 (2013).
11. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
12. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
13. N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).
14. R. García-Patrón and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," Phys. Rev. Lett. **102**, 130501 (2009).
15. X. Su, W. Wang, Y. Wang, X. Jia, C. Xie, and K. Peng, "Continuous variable quantum key distribution based on optical entangled states without signal modulation," Europhys. Lett. **87**, 20005 (2009).
16. 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**, 1083 (2012).
17. V. C. Usenko and R. Filip, "Squeezed-state quantum key distribution upon imperfect reconciliation," New J. Phys. **13**, 113007 (2011).
18. I. Derkach, V. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels," New J. Phys. **22**, 053006 (2020).
19. T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. Werner, and R. Schnabel, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," Nat. Commun. **6**, 8795 (2015).
20. N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," Optica **3**, 634–642 (2016).
21. Z. Qu and I. B. Djordjevic, "High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing," Opt. Express **25**, 7919–7928 (2017).
22. H. Ishio, J. Minowa, and K. Nosu, "Review and status of wavelength-division-multiplexing technology and its application," J. Lightwave Technol. **2**, 448–463 (1984).
23. K. Grobe and M. Eiselt, *Wavelength Division Multiplexing: A Practical Engineering Guide* (Wiley, 2013).
24. Y. Wang, Y. Mao, W. Huang, D. Huang, and Y. Guo, "Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution," Opt. Express **27**, 25314–25329 (2019).
25. R. Kumar, X. Tang, A. Wonfor, R. Penty, and I. White, "Continuous variable quantum key distribution with multi-mode signals for noisy detectors," J. Opt. Soc. Am. B **36**, B109–B115 (2019).
26. R. Filip, L. Mišta, and P. Marek, "Elimination of mode coupling in multimode continuous-variable key distribution," Phys. Rev. A **71**, 012323 (2005).
27. V. C. Usenko, O. Kovalenko, and R. Filip, "Compensating the cross-talk in two-mode continuous-variable quantum communication," in *41st International Conference on Telecommunications and Signal Processing (TSP)* (IEEE, 2018), pp. 1–4.
28. Y. Cai, Y. Xiang, Y. Liu, Q. He, and N. Treps, "Versatile multipartite Einstein-Podolsky-Rosen steering via a quantum frequency comb," Phys. Rev. Res. **2**, 032046 (2020).
29. R. Medeiros de Araújo, J. Roslund, Y. Cai, G. Ferrini, C. Fabre, and N. Treps, "Full characterization of a highly multimode entangled state embedded in an optical frequency comb using pulse shaping," Phys. Rev. A **89**, 053828 (2014).
30. G. de Valcarcel, G. Patera, N. Treps, and C. Fabre, "Multimode squeezing of frequency combs," Phys. Rev. A **74**, 061801 (2006).
31. N. Liu, Y. Liu, J. Li, L. Yang, and X. Li, "Generation of multi-mode squeezed vacuum using pulse pumped fiber optical parametric amplifiers," Opt. Express **24**, 2125–2133 (2016).
32. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: a threat and a defense," Entropy **18**, 20 (2016).
33. Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre, and N. Treps, "Multimode entanglement in reconfigurable graph states using optical frequency combs," Nat. Commun. **8**, 15645 (2017).
34. V. C. Usenko, L. Ruppert, and R. Filip, "Quantum communication with macroscopically bright nonclassical states," Opt. Express **23**, 31534–31543 (2015).

35. I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," Phys. Rev. A **93**, 032309 (2016).
36. O. Kovalenko, V. C. Usenko, and R. Filip, "Feasibility of quantum key distribution with macroscopically bright coherent light," Opt. Express **27**, 36154–36163 (2019).
37. V. C. Usenko, L. Ruppert, and R. Filip, "Entanglement-based continuous-variable quantum key distribution with multimode states and detectors," Phys. Rev. A **90**, 062326 (2014).
38. 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**, 093048 (2012).
39. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
40. R. Garcia-Patron and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
41. M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of Gaussian quantum states," Phys. Rev. Lett. **96**, 080502 (2006).
42. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
43. A. Leverrier and P. Grangier, "Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **81**, 062314 (2010).
44. R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).
45. 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**, 030502 (2013).
46. I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A **461**, 207–235 (2005).
47. 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**, 621–669 (2012).
48. C. S. Jacobsen, L. S. Madsen, V. C. Usenko, R. Filip, and U. L. Andersen, "Complete elimination of information leakage in continuous-variable quantum communication channels," npj Quantum Inf. **4**, 32 (2018).
49. V. Thiel, J. Roslund, P. Jian, C. Fabre, and N. Treps, "Quantum-limited measurements of distance fluctuations with a multimode detector," Quantum Sci. Technol. **2**, 034008 (2017).
50. F. Arzani, C. Fabre, and N. Treps, "Versatile engineering of multimode squeezed states by optimizing the pump spectral profile in spontaneous parametric down-conversion," Phys. Rev. A **97**, 033808 (2018).
51. M. Lassen, A. Berni, L. S. Madsen, R. Filip, and U. L. Andersen, "Gaussian error correction of quantum states in a correlated noisy channel," Phys. Rev. Lett. **111**, 180502 (2013).
52. M. Genovese, "Real applications of quantum imaging," J. Opt. **18**, 073002 (2016).
53. E. D. Lopaeva, I. R. Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, "Experimental realization of quantum illumination," Phys. Rev. Lett. **110**, 153603 (2013).
54. F. Grosshans, "Collective attacks and unconditional security in continuous variable quantum key distribution," Phys. Rev. Lett. **94**, 020504 (2005).
55. M. G. Kendall, A. Stuart, and J. K. Ord, *Kendall's Advanced Theory of Statistics* (Oxford University, 1987).
56. L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," Phys. Rev. A **90**, 062310 (2014).
57. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
58. M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Phys. Rev. Lett. **73**, 58–61 (1994).
59. R. H. Byrd, P. Lu, J. Nocedal, and C. Zhu, "A limited-memory algorithm for bound constrained optimization," SIAM J. Sci. Comput. **16**, 1190–1208 (1994).
60. P. R. Bevington and D. K. Robinson, *Data Reduction and Error Analysis for the Physical Sciences*, 3rd ed. (McGraw-Hill, 2003).