PALACKY UNIVERSITY OLOMOUC
FACULTY OF SCIENCE

Department of Optics

Multiplexed quantum optical communication using multimode entangled states

Olena Kovalenko

PhD Thesis

Study program: Physics, P1701
Study program: Optics and Optoelectronics, 1701V029

Supervisor: prof. Mgr. Radim Filip, Ph.D.
Consultant: Dr. Vladyslav C. Usenko Ph.D.

Olomouc 2023

Abstract

This thesis is based on the results of my PhD studies at Palacky University in Olomouc. The research deals with the task of improvement of existing quantum communication protocols with multimode entangled states. Firstly, we consider the mode-multiplexing in entanglement distribution and quantum key distribution, in this case each mode is used to carry separate quantum signal, hence it should be handled and measured separately. The other issue we study is the use of multimode bright states of light in quantum communication, in this case the modes are not discriminated in the measurement, the protocol does not use them for multiplexing, but instead multiple modes make the signal brighter and easier to work with in experimental implementation.

We study multiplexing of the entangled states of light used in quantum communication and, in particular, in quantum key distribution. Mode-multiplexing allows to improve performance and increase capacities of quantum communication protocols. Unfortunately while improving protocols capacities, the multi-mode structure of quantum states can also introduces new imperfections, that are not present in single-mode implementations of the protocols. Our work is devoted to the study of some of these imperfections. The main focus of ours is the intramode cross talk and the ways to compensate it. In the process of generation, distribution and measurement the modes can get coupled to each other due to photon exchange between them, i.e. they experience cross talk. We theoretically study deteriorating effects of the cross talk on entanglement and the secure key in a simplified 4-mode model and suggest methods that mitigate negative influence of the cross talk. The approaches we suggest can be both passive (optimization of the state during its preparation) or active (introducing network of optical elements that compensate for the cross talk). We then proceed to apply one of the active compensation methods to improve the source of frequency-multiplexed entangled light with strong coupling between the modes. We model the quantum key distribution protocol using the frequency-mode multiplexed entangled state produced experimentally by the group from Laboratoire Kastler Brossel. We show that after cross talk compensation the secret key rate of the protocol increases significantly, confirming viability of the proposed cross talk compensation method.

Lastly, we study applicability of multimode bright states for quantum key distribution. The imperfect matching of the multi-mode signal with the phase reference beam during the measurement introduces noise to the signal, negatively affecting the quantum key distribution protocol performance. We demonstrate with the experimental data from the group from Max Planck Institute for the Science of Light, that the noise introduced by unmatched modes can be suppressed by the increase of the reference beam power, hence restoring the secret key.

Key words

Quantum communication, quantum key distribution, entanglement, continuous variables, Gaussian states, entangled states of light, frequency-multiplexed entanglement.

Acknowledgement

Firstly, I wish to thank my supervisor Radim Filip for his patience and belief in me and for all his help during course of my studies. I would further like to thank Vladyslav C. Usenko for his assistance at every stage of my Ph.D. studies and his helpful comments and suggestions for my thesis. I would also extent my gratitude to collaborators from LKB and MPL for lending me their expertise and intuition to the projects we were working together on. I would also like to thank Ivan and Darren for helpful discussion and comments they contributed to my thesis. Lastly I'm grateful to Tuomas for his constant support and reassurance and to all my friends and family for their support over the past years.

Declaration

I hereby declare that this thesis titled **"Multiplexed quantum optical communication using multimode entangled states"** have been composed solely by myself under the guidance of my supervisor prof. Mgr. Radim Filip, Ph.D. and my PhD consultant Dr. Vladyslav C. Usenko Ph.D. I confirm that the thesis is based on the results of my own work, and materials and results that are not original to this work have been fully cited and referenced.

This thesis has not been previously submitted for a degree or diploma at any other higher education institution to the best of my knowledge and belief.

I agree with the further usage of this thesis in accordance with the requirements of Palacky University and the Department of Optics.

.....
Olena Kovalenko

In Olomouc, ... 2023

Contents

1 | Introduction

While quantum entanglement as a phenomenon was discovered almost a century ago, the technology employing it for quantum communication is still ongoing its development stage. One of the ways to improve communication protocols is to allow transfer of several entangled states simultaneously by multiplexing the channels. Quantum communication and, more narrowly, mode-multiplexing in quantum communication is a vast field of research, this work concentrates on several use-cases. We theoretically study application of multimode Gaussian states of light for scalability improving efficiency of quantum key distribution (QKD) and of Gaussian entanglement distribution, that has its application in QKD, in quantum teleportation and in the future, in distributed quantum computing. Mode multiplexing allows to increase channel capacities, which is essential for practical implementations of the the protocols.

Entanglement phenomenon was first introduced as EPR paradox in Einstein-Podolsky-Rosen paper [1] in 1935. It was investigated and the name "entanglement" was coined by Schrodinger in [2]. First experimental demonstration of EPR paradox and violation of Bell inequalities with polarization-entangled photon pairs were performed in [3, 4] by Freedman and Clauser, EPR experiment for continuous variable states was done with two-mode squeezed vacuum by Ou [5]. Entanglement being equivalent to inseparability was first theoretically shown in [6]. The first cryptographic protocol that used (discrete) effectively entangled quantum states for generation of classical one-time pad for unconditionally secure communication was BB84 [7]. It started a whole new field of quantum key distribution (QKD) with both discrete variables (DV) and, later, continuous variables (CV). Shortly, the task of QKD is to distribute a secret bit string between remote parties using public channel with security ensured by laws of quantum physics. DV QKD employs single photons' degrees of freedom as carriers of information, and single-photon detectors are either avalanche photo-diodes or super-conducting detectors that demand low temperatures. While the CV version of QKD employs multi-photon states and coherent homodyne/heterodyne detection. For the CV states the EPR correlations occur between continuous-variable quadratures of electromagnetic field having infinite degrees of freedom. In the experiments the CV states conveniently can be handled with well developed and easily accessible and fast optical technologies [8–10].

CV entanglement is deployed in numerous quantum technologies, in quantum teleportation [11], in quantum random number generation [12], for quantum-enhanced sensing [13], in combination with non-Gaussian resource it is also potentially useful in building scalable quantum computer [14], particularly with large cluster states [15]. QKD remains

the most practically ready among the quantum technologies. CV QKD can be implemented with existing networks in telecom fibers or in atmosphere [16], it does not need extra low temperatures, it can be integrated on chips [17, 18], and, in case of coherent state protocols, needs only classical components performing without excess thermal noise. Recently some protocols were implemented on hundreds kilometers distance (comparable to DV QKD distances) [10]. Multiple CV protocols have been developed [19] using either squeezed [20, 21] or coherent states [22], with either homodyne or heterodyne detection [23]. While new protocols and security proofs still keep developing, including twin field for DV [24], measurement-device independent [25, 26], CV protocols using thermal states [27, 28], CV protocols with non-Gaussian (discrete) modulation [29], in this thesis we keep our focus on the Gaussian protocols, for which the security proofs and techniques are well developed, and which can be available and practical test-bed for testing the multiplexing techniques.

Theoretically QKD offers unconditional security (that only relies on quantum mechanics being correct), in practice any devices used in real-life implementations does not exactly correspond to theoretical models, this creates security vulnerabilities [16,30]. The field of study that raised to investigate these vulnerabilities is often referred to as quantum hacking [16, 31–34]. Originally done in the asymptotic regime, the security proofs were made with assumption of infinitely long data blocks, afterwards they were adjusted for more realistic finite regime [35–38].

Ways to improve the performance of existing protocols can go in several directions: one approach is to increase repetition rates, currently they reach up to hundred MHz [39] (it also demands high-speed detectors [40]), another approach is source and/or channel multiplexing. Multiplexing is a well developed approach in classical signal processing with optical fibres both in frequency domain with wavelength division multiplexing [41] and, later, also in spatial domain with spatial division multiplexing [42,43], integration of CV QKD into existing telecom networks can benefit from both approaches. Wavelength multiplexing or spatial division multiplexing with multi-core (parallel channels) and/or multi-mode fibres (channels where several frequencies can be propagated simultaneously) can be applied to both DV [44] and CV QKD [45, 46]. Wavelength division multiplexing with high repetition rates demonstrated secret key rates up to 250 Mb/s for CV QKD [47]. Coexistence of classical and quantum signals in multicore cables was also studied [48, 49]. In principle multiplexing allows to achieve key rate N times (where N is the number of multiplexed channels) above the limit established by repeaterless bounds [50]. In practice significant loss occurring in the multicore fibres input and output (fan-in/fan-out) devices [51] and also cross talk between the modes can deteriorate the secret key. In multicore cables the cross talk between the classical and quantum signals is shown to be relatively low if quantum and classical signal occupy different frequency bands [45], however, even subtle effects can be crucial for quantum communication. In this thesis we theoretically study how cross talk between quantum signals influences entanglement distribution and QKD performance.

Channel multiplexed protocols demand the shared state to be multiplexed too, it is possible to achieve by using several independent sources, another approach is to use a

single intrinsically multimode frequency-multiplexed source. One way such frequency multiplexed entangled states (also referred to as frequency comb) [52] can be generated is using synchronously pumped optical parametric oscillator [53, 54], separate frequency bands of such state can be measured with mode-discriminating homodyne detection [55]. In this work we demonstrate how frequency multiplexed entangled states can be used for multiplexing of entanglement-based CV QKD protocol, after postprocessing eliminates (at least partially) cross talk between different frequency bands.

CV QKD is normally implemented with relatively weak signals, few tens of photons on average, which are difficult to control and handle on a practical level, macroscopically bright states having up to 10^6 photons per pulse [56, 57] can help to solve this practical issue. States referred to as "macroscopic" are multimode/multiparticle quantum states [56, 58]. Macroscopic entangled states were observed in experiments with bright squeezed vacuum [59] as well as with atom spin ensembles [60]. Possibility to use macroscopically bright states of light for QKD was studied theoretically [61, 62]. In our work we model a bright coherent state QKD protocol with homodyne detection based on experimental data and study possibility to reduce noise caused by imperfect matching of bight/multiple modes with local oscillator during the measurement.

This thesis aims at studying and removing the problems and limitations that can arise while implementing multiplexed CV entanglement distribution and QKD protocols using multimode entangled states, at developing methods to overcome these limitations and, to extent possible with the available experiments, at testing these methods on the experimental data. This work was conducted during my Ph.D. studies at Palacky University in Olomouc and this thesis is based on 3 articles published in peer-reviewed and impacted journals (Photonics research and Optics Express) during the course of my study.

Outline of the thesis

The thesis starts with the introduction of the theoretical tools for description of Gaussian states and operations in Chapter 2. We remind the definitions of Gaussian entanglement and the logarithmic negativity as its measure and a generic one-way entanglement distribution protocol. The chapter proceeds with description of generic CV QKD protocol, its security, assumptions about the eavesdropper. In the end we introduce a scheme of multimode protocol with linear coupling (cross talk) among the modes, we also describe a frequency-multiplexed entangled state as a possible carrier state for this protocol.

Chapters 3 to 5 contain results of our research which were published in the articles presented in Chapter 6. Chapter 3 concerns the theoretical model of the entanglement distribution in the presence of cross talk. We suggest a way to compensate the cross talk and restore entanglement with the help of optimized interference. Then we proceed comparing the suggested compensation method to another one that traces out some modes while enhances the entanglement of the other modes.

In Chapter 4 we describe a result of experimental-theoretical collaboration, where we implement the compensation method numerically to eliminate the cross talk in the experimentally measured frequency multiplexed entangled state introduced in Chapter 2. We then model the CV QKD protocol using the multiplexed state showing how optimal postprocessing successfully eliminated the cross talk and increased the secure distance of the QKD protocol.

Chapter 5 concerns another experimental-theoretical collaboration. We model CV QKD protocol with macroscopically bright coherent state, the bright state contains multiple modes that are measured with a mode-non-discriminating measurement. We consider scenario where imperfect mode matching makes the signal noisy, destroying the secure key. Using the data from the proof-of principle experiment we show how the noise coming from the imperfect mode-matching can be suppressed and the secure key restored.

Chapter 6 contains the copies of the articles published. Finally the summary of the main results, conclusions and outlook for future work are given in Chapter 7.

2 | Quantum multimode continuous-variable states

2.1 Gaussian states

States of a single mode of electromagnetic field (with defined frequency, polarisation and propagation direction) exists in infinite-dimensional bosonic Fock space $\mathcal{H}$ spanned over photon number basis $\{|n\rangle_j\}_0^\infty$. The Hilbert space of an N-mode state is then a straightforward extension $\bigotimes_{i=1}^N \mathcal{H}_i$. Multimode state in such Hilbert spaces can be described by a set of $2N$ variables: pairs of creation and annihilation operators $\hat{a}_i^\dagger$ and $\hat{a}_i$, $i \in \{1, N\}$, N is number of modes. Being bosonic operators they obey commutation relations $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$. In CV quantum optics the states of light are typically characterized by two quadratures of electromagnetic field, $\hat{x}$ and $\hat{p}$ in analogy to oscillator's position and momentum operator. These quadratures can be directly measured in the experiment by homodyne detection, as described in Section 2.1.2 . In this thesis we use convention

$$\hat{x}_i = \hat{a}_i^\dagger + \hat{a}_i \tag{2.1}$$

$$\hat{p}_i = i(\hat{a}_i^\dagger - \hat{a}_i) \tag{2.2}$$

making a vacuum shot noise equal to 1. Vacuum state is the zero-photon number state $|0\rangle$, with its noise (quadrature variance, defined as $Var(.) =< .^2 >$ for a zero-mean quadrature operator) being minimal $Var(\hat{x}) = Var(\hat{p}) = 1$ in both quadratures. The multimode state quadratures of N-mode state can be described by a vector operator $\hat{\mathbf{q}} = \{\hat{x}_1, \hat{p}_1, ...\hat{x}_N, \hat{p}_N\}^T$. Their mean values $d = \langle\hat{\mathbf{q}}\rangle$ describe the electromagnetic fields in the classical optics limit.

In Gaussian approximation, multimode quadratures allow to define the state's covariance matrix describing light fluctuations, i.e. the $2N \times 2N$ matrix of second statistical moments of symmetrically-ordered quadrature operators [63],

$$\gamma = \frac{1}{2}\langle\hat{\mathbf{q}}\hat{\mathbf{q}}^T + \hat{\mathbf{q}}^T\hat{\mathbf{q}}\rangle. \tag{2.3}$$

The commutation relation for quadrature variables can be written in form $[\hat{q}_m, \hat{q}_n] = 2i\Omega_{mn}$, where $\Omega_{mn} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the symplectic form. It leads to a multimode gener-

alisation of the Heisenberg inequality for the covariance matrix γ

$$\gamma + i\Omega \geq 0, \tag{2.4}$$

where $\Omega = \bigoplus_1^N \Omega_{mn}$ is a $2N \times 2N$ block-diagonal symplectic form.

Gaussian states are completely characterised by classical mean displacement $d = \langle \hat{q} \rangle$ and covariance matrix γ describing quantum fluctuations. They hey contain one of the most simple cases of non-classical states, the multimode squeezed states, that have wide range of application in quantum communication as they are relatively easy to generate and detect with technologically available sources, including homodyne detectors, sufficiently robust against optical loss. Moreover many standard linear or linearized optical devices preserve Gaussianity, assuming their parameters remain ideally stable.

Minimum uncertainty single-mode classical states are coherent states and, as its particular case, the vacuum state. Coherent state (being a classical state) is the closest analogue of classical light established by coherence theory by Glauber [64] with precisely defined phase and amplitude $\alpha = |\alpha|e^{i\phi}$. Crucially, the states generated by ideal shot-noise-limited monochromatic laser are coherent states, respectively to a phase reference given by the local oscillator. Vacuum state has zero displacement $(d_x, d_p) = (0, 0)$ and identity covariance matrix; coherent states $|\alpha\rangle$ have nonzero displacement $(d_x, d_p) = (2\Re(\alpha), 2\Im(\alpha))$ and identity covariance matrix (2.3). Coherent state $|\alpha\rangle$ is obtained by ideal external coherent classical drive on a linear oscillator, mathematically described by displacement operator acting on vacuum state $|\alpha\rangle = D(\alpha)|0\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle$. Uncertainties in both quadratures are equal irrespectively to α, $Var(\hat{x}) = Var(\hat{p}) = 1$ and $Var(\hat{x})Var(\hat{p}) = 1$ in vacuum noise units. Displacement operator can be generalized for many-mode states for displacement $\xi \in \mathbb{R}^{2N}$, it is then called Weyl operator [65]

$$D(\xi) = e^{i\hat{q}^T\Omega\xi}.$$

Weyl operator allows to go from formalism of Hilbert space $\mathcal{H}$ to the formalism of phase space representation. Symmetrically-ordered characteristic function of any state is given by average of Weyl operator $D(\xi)$, $\chi_s(\xi) = Tr[\rho D(\xi)]e^{\frac{s}{2}\|\xi\|^2}$ [63]. Complex Fourier transform of it is Wigner function

$$W(\mathbf{q}) = \frac{1}{(2\pi)^{2N}} \int \chi_0(\zeta) e^{i\mathbf{q}^T\Omega\zeta} d^{2N}\zeta, \tag{2.5}$$

it is a quasi-probability distribution on the phase space, it is normalised to 1 but it can take negative values. The state is Gaussian if its Wigner function in a phase space of quadratures $\hat{x}$ and $\hat{p}$ is a Gaussian function. For Gaussian states the Wigner function is always positive:

$$W(\mathbf{q}, \gamma) = \frac{1}{(2\pi)^N\sqrt{Det\gamma}} e^{-\frac{1}{2}(\mathbf{q}-d)\gamma^{-1}(\mathbf{q}-d)^T} \tag{2.6}$$

here $\mathbf{q} = \{x_1, p_1, ...x_N, p_N\}^T$ is a real vector of quadrature variables in the 2N dimensional phase space. Wigner function for single mode Gaussian states is just two-variable normal

distribution $W(X,P) = N(d,\gamma)$. In realistic cases we use the Gaussian approximation of the quantum state described by mean values and covariance matrices of the multimode states and refer to Eq. (2.6) as an approximative Gaussian state. Fortunately, for some protocols, including CV QKD ones, the Gaussian approximation is sufficient and Gaussian states are extremal [66].

Besides classical coherent states, another important case of Gaussian states are non-classical single and two-mode squeezed states. Non-classical states are the states that cannot be represented as a mixture of coherent states. For a Gaussian state to be non-classical it needs to be squeezed, a pure non-classical Gaussian state has noise below uncertainty limit (below vacuum state) for a certain phase. [65]

Several processes allow to produce squeezing [67,68]. In general squeezed states of light are obtained by strong coherent pumping of the dielectric medium with nonlinearity of second or higher order. For the first time non-classical squeezing was generated using the third order nonlinearity for four wave mixing [69], currently the best developed and most popular ways to generate squeezed states is spontaneous parametric down-conversion (SPDC) process [70,71], in an optical parametric amplifier (OPA) [69] or oscillator (OPO) [72]. SPDC process generates entangled pairs of photons in nonlinear $\chi^{(2)}$ crystal, but as nonlinear susceptibility is typically relatively weak, the squeezing achieved after a single pass of light through the crystal is not enough for many applications. Having the crystal placed in a cavity creates OPO, increasing the time of beam interacts with nonlinear medium, it produces single-mode squeezing from a degenerate process and two-mode squeezing from the non-degenerate one on the resonant frequency of the cavity. Another way is used in OPA without a cavity where an extra high power short pulse is used along with the signal beam to increase the effective nonlinear susceptibility of the crystal. Current record of single-mode squeezing is -15 dB [73] with 21 dB of anti-squeezing (anti-squeezing being higher in absolute number than squeezing due to inevitable presence of loss), on the other hand, highly pure states can reach -10 dB of squeezing with 11 dB of anti-squeezing [73].

Minimal uncertainty condition $Var(\hat{x})Var(\hat{p}) = 1 \geq 1$ puts limit on a product of quadrature uncertainties for all Gaussian states, both classical and non-classical. The pure states that have one quadrature squeezed with variance < 1 (and other quadrature antisqueezed to preserve the uncertainty) are ideal non-classical minimal uncertainty states. The squeezed states is formally obtained by action of squeezing operator on a vacuum state, the squeezing operator acting on a single mode is $S(z)|0\rangle = e^{\frac{1}{2}(z\hat{a}^2 - z^*\hat{a}^{\dagger 2})}|0\rangle$, with complex squeezing parameter $z = re^{-i\theta}$, where r gives the squeezing factor and θ gives phase of the squeezed quadrature. Single-mode squeezing is degenerate process creating photons of half frequency of the pump $\hbar\omega_0 = 2\hbar\omega$, only even Fock states $|2n\rangle$ are present. The non-degenerate process instead creates photons in pairs of different frequencies $\hbar\omega_0 = \hbar\omega_1 + \hbar\omega_2$, the generated state contains two modes, with corresponding change of creation operators $\hat{a}^{\dagger 2} \rightarrow \hat{a}^\dagger\hat{b}^\dagger$ in the interaction Hamiltonian. Two-mode squeezing operator acting on two-mode vacuum state is $S(z)|0,0\rangle = e^{\frac{1}{2}(z\hat{a}\hat{b} - z^*\hat{a}^\dagger\hat{b}^\dagger)}|0,0\rangle$. Squeezing can be generalized to multimode case [74] $\prod_{i<j=1}^{N} S(z_{ij})|0,...,0\rangle$, N is number of modes, $S(z_{ij})$ is a two-mode squeezing operator acting on modes i and j.

Two-mode squeezed vacuum (TMSV) state is an important example of many-mode Gaussian state, and it is actively used in bipartite QKD. In the photon number basis (introduced in the beginning of this chapter)

$$|TMSV\rangle = \sqrt[4]{\frac{2}{V+1}} \sum_{n=0}^{\infty} \left(\frac{V-1}{V+1}\right)^{n/2} |nn\rangle \tag{2.7}$$

with quadrature variance $V = \cosh(2r)$, here r is the squeezing parameter assumed to be real. In the quadrature picture both modes have zero displacements and corresponding covariance matrix is

$$\gamma_{AB} = \begin{pmatrix} V\ \mathbb{I} & \sqrt{V^2-1}\ \mathbb{Z} \\ \sqrt{V^2-1}\ \mathbb{Z} & V\ \mathbb{I} \end{pmatrix}, \tag{2.8}$$

here $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity matrix, $\mathbb{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is a Pauli Z matrix.

TMSV has Wigner function that is a two-mode Gaussian distribution:

$$W(\alpha, \beta) = \frac{8}{\pi^2}[-\cosh(2r)(|\alpha|^2 + |\beta|^2) + \sinh(2r)(\alpha\beta + \alpha^*\beta^*)], \tag{2.9}$$

where $\alpha = x_1 + ip_1$ and $\beta = x_2 + ip_2$, or in terms of quadrature mean values [75]:

$$W(x_1, p_1, x_2, p_2) = \frac{4}{\pi^2} \exp\left(-e^{-2r}[(x_1 + x_2)^2 + (p_1 - p_2)^2] - e^{2r}[(x_1 - x_2)^2 + (p_1 + p_2)^2]\right), \tag{2.10}$$

displaying correlations of X quadratures and anticorrelations of P quadratures of the modes of TMSV.

2.1.1 Gaussian operations

Gaussian channels map Gaussian states into other Gaussian states [76]. They allow to transform states in the Gaussian approximation using only transformations of displacement vectors and covariance matrices. Assumption of channel's Gaussianity allows to keep the calculation, data evaluation and interpretation within the Gaussian approximation. The Hamiltonians of corresponding processes are at most quadratic with regard to $\hat{a}$, $\hat{a}^\dagger$ operators, therefore, they generate linear Heisenberg equations for the dynamics. They act on quadratures, displacement vector and covariance matrix as real symplectic transformations [77] with additive normally distributed noise. In its most general form Gaussian completely positive map acts on the Gaussian state with two matrices S and Z

$$\hat{\mathbf{q}}' = S\hat{\mathbf{q}} + \mathbf{d}, \tag{2.11}$$

$$\gamma' = S\gamma S^T. \tag{2.12}$$

$$d' = Sd, \tag{2.13}$$

here Z is a symmetric matrix.

Symplectic group [78] is a set of linear operator transformations $S \in Sp(2N, \mathbb{R})$, that act on $\hat{\mathbf{q}}$ and preserve commutation relations, leading to condition $S\Omega S = \Omega$. If Wigner function in Eq.(2.6) of $\hat{\mathbf{q}}$ is Gaussian, Wigner function of $\hat{\mathbf{q}}'$ remains Gaussian, Gaussianity is preserved under symplectic transformations, (the same is also true for Gaussian approximation).

Orthogonal symplectic transformations, that preserve photon number (e.g. beamsplitters and phase plates in the experiments), are energetically passive transformations. Active transformations that add photons to the modes (for example by squeezing) are not orthogonal and require a external coherent drive, in principle. Particular case of symplectic transformations are orthogonal unitaries that present decomposition of multimode Gaussian states into single mode ones [78].

Williamson decomposition [78, 79] is a symplectic transformation of the covariance matrix into diagonal form

$$\gamma = S^T \nu S, \tag{2.14}$$

where $\nu = \mathrm{diag}[\nu_1, \nu_1, \nu_2, \nu_2, ..., \nu_N, \nu_N]$, ν_i are the symplectic eigenvalues of the state. Williamson decomposition represents any Gaussian state as a superposition of independent thermal states $\langle x_i \rangle = \langle p_i \rangle = \nu_i$ with the mean photon number in each mode $\overline{n}_i = \frac{\nu_i - 1}{2}$, and with the density matrix

$$\rho = \bigotimes_i \frac{2}{\nu_i + 1} \sum_{n=0}^{\infty} \left(\frac{\nu_i - 1}{\nu_i + 1} \right)^{n/2} |n\rangle\langle n|. \tag{2.15}$$

The uncertainty relation Eq. 2.4 simplifies into $\nu_i \geq 1$ for symplectic eigenvalues.

Bloch-Messiah decomposition [75] allows to present any symplectic transformation S as

$$S = OKO'^T, \tag{2.16}$$

where $K = \mathrm{diag}[e^{-r_1}, e^{r_1}, ..., e^{-r_N}, e^{r_N}]$ is a diagonal matrix of a multimode squeezer and O and O' are orthogonal transformations by passive elements. Combining Bloch-Messiah decomposition with Williamson decomposition Eq.(2.14) gives a general decomposition of any multimode state

$$\gamma = OKO'^T \nu \; O'KO^T. \tag{2.17}$$

Taking into account that the initial state is vacuum $\nu_0 = \mathbb{I}_{2N}$, it allows us to see transformation of any pure N-mode Gaussian state into N pure squeezed states $\gamma = OK^2O^T$, with $K^2 = \mathrm{diag}[e^{-2r_1}, e^{2r_1}, ..., e^{-2r_N}, e^{2r_N}]$. This transformation is useful in quantum optics and quantum communication with light.

Bloch-Messiah decomposition shows the way to present an (ideal, lossless) Gaussian operation as an equivalent of a network of interferometers (consisting of ideal beamsplitters and phase shifters), followed by a sequence of one-mode squeezers, followed by another interferometer network. Combining it with Williamson (symplectic eigenmodes) decomposition that transforms any Gaussian state into a set of independent thermal states, we can view any N-mode Gaussian state as N thermal modes undergoing first a basis transformation, squeezing and then another basis transformation [80].

One particular important case of the nonunitary Gaussian transformation, described in the next subsection, that is projecting multimode Gaussian state on one mode quadrature is the homodyne measurement.

2.1.2 Homodyne detection

In this thesis, any time measurement of any CV state is mentioned, the homodyne detection is assumed. Homodyne measurement is a linear and Gaussian measurement [63], i.e. it produces Gaussian probability distribution for any Gaussian state measured. In this subsection first we describe the standard two-port homodyne detection [81] that uses difference of photocurrents between two detectors to measure one of the quadratures. Then it is generalised to a four-port scheme that allows to measure any combination of quadratures [82]. To highlight the principles, we assume that both the signal and the synchronised in phase high intensity beam used as phase reference are monochromatic, and detectors are noiseless, these assumptions are realistic for currently available hodmodyne detectors.

The homodyne measurement projects a state on a quadrature $\hat{r} = \hat{a}^\dagger e^{i\phi} + \hat{a}e^{-i\phi}$ of mode K, directly giving information about the quadrature value. The signal is measured after being mixed with strong coherent phase reference beam called local oscillator on a beam splitter and the resulting intensities are measured on the outputs. The phase reference is represented by a strong classical local oscillator beam that is usually generated from the same source as the signal itself. Homodyne detection, being a continuous-variable measurement, allows no photon number resolution, the result of measurement is the difference of continuous photo-currents. In this simplest configuration (and with assumption of fast enough detection that captures separate pulses) with one beam-splitter and two detectors the homodyne observable (the difference of photo-currents intensities) is $\hat{n}_- = \hat{a}_s^\dagger \hat{a}_{LO} + \hat{a}_s \hat{a}_{LO}^\dagger$ assuming local oscillator to be a coherent state $|\alpha\rangle e^{i\phi}$.

In the regime of strong LO $|\alpha|^2 \gg \langle \hat{n}_s \rangle$ it allows to approximately measure quadrature $\hat{r}_\phi = \hat{a}^\dagger e^{i\phi} + \hat{a}e^{-i\phi}$. Depending on reference phase, the edge cases when $\phi = 0$ and $\phi = \pi/2$ are the quadratures $\hat{x}$ and $\hat{p}$. Both the local oscillator and the signal may acquire extra noise while passing through the channel, any phase noise acquired by both beams travelling through the same channel should be almost the same, these phase fluctuations synchronise on the detectors and cancel out, the phase fluctuations that are not synchronised bring extra noise to the quadratures measured. Local oscillator also suppresses any noise occurring in all the modes other than the reference mode.

The homodyne measurement of one mode r_k of the multimode state transforms the remaining state. Assuming the state being measured is Gaussian N-mode state, its many-mode covariance matrix $\gamma_{A_1 \ldots A_N}$ is transformed by homodyne measurement of one of the quadratures of mode K [83]:

$$\gamma_{A_1 \ldots A_N | r_K} = \gamma_{A_1 \ldots A_N} - \sigma_{A_1 \ldots A_N, K} \left(R \cdot \gamma_K \cdot R \right)^{MP} \sigma^T_{A_1 \ldots A_N, K}, \tag{2.18}$$

where γ_K is the single-mode covariance matrix of the mode K, $\sigma_{A_1 \ldots A_N, K}$ is the correlation

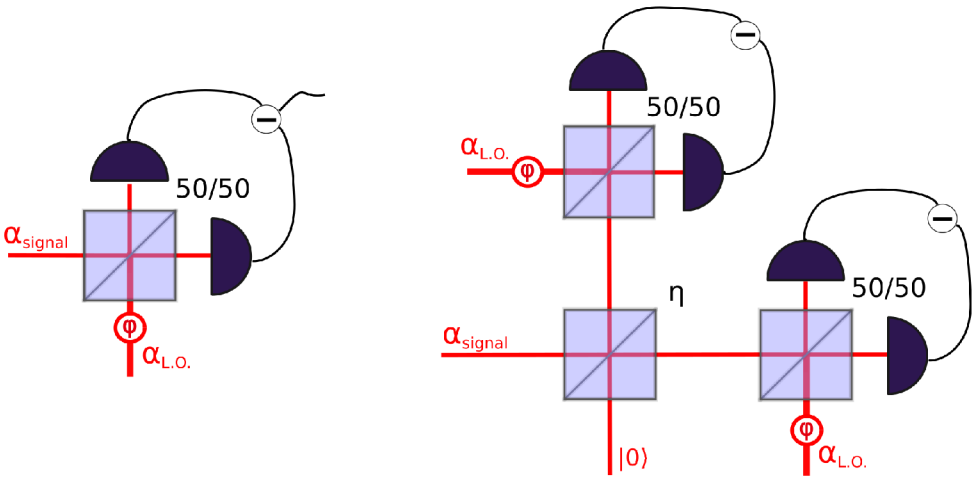

Figure 2.1: Left: Standard homodyne detection. Signal and high intensity phase reference are mixed on the beam-splitter, intensities of output photocurrents are subtracted allowing to measure quadrature $\hat{r}$. Adding a variable phase shift ϕ to the LO beam allows to switch between quadratures. Right: generalized homodyne detection. Allows to measure linear combination of both quadratures while adding extra vacuum noise from the state $|0>$.

matrix between modes $A_1...A_N$ and K, matrix R is a diagonal matrix, being $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ for an x-quadrature measurement or $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ for a measurement of p-quadrature (can be generalized to any r_k quadrature measurement), and MP stands for Moore-Penrose pseudo-inverse of a matrix, applicable to singular matrices.

First moments (displacements) of a many-mode state are transformed as

$$d_{A_1...A_N|r_K} = d_{A_1...A_N} + \sigma_{A_1...A_N,K} \left(R \cdot \gamma_K \cdot R\right)^{MP} (Q_K - d_K), \tag{2.19}$$

here $d_{A_1...A_N} = \{\langle x_{A_1}\rangle, \langle p_{A_1}\rangle ..., 0_K, 0_K, ..., \langle x_{A_N}\rangle, \langle p_{A_N}\rangle\}$ is mean values of displacement before measurement, in the basic case when either X or P complementary quadrature is measured, $Q_K = \{X_K, 0\}$ or $Q_K = \{0, P_K\}$ is the result of measurement of the mode K, $d_K = \{x_K, p_K\}$

To measure both quadratures at the same time the heterodyne measurement, that projects the state onto a coherent state $|\alpha\rangle$, can be used. It allows to measure simultaneously both $\hat{x}$ and $\hat{p}$ while adding extra vacuum noise, by dividing the signal on a 50/50 beam-splitter (where vacuum noise enters) and then measuring the opposing quadratures with two separate homodyne measurements at the beam-splitter outputs. It is required for detection of off-diagonal elements of the covariance matrix, describing inter-mode correlations. A slightly generalised version of heterodyne measurement where the beam-splitter is allowed to not be 50/50 but to have varied transmittance η is depicted on the Fig. 2.1. This generalised homodyne measurement projects the state on an arbitrary chosen linear combination of quadratures $\sin\theta\hat{x} + \cos\theta\hat{p}$ depending on the choice of the beam-splitter transmittance.

Generalised homodyne measurement of a single mode K of a multimode state with modes $A_1...A_N$ transforms the covariance matrix of the remaining state as

$$\gamma_{A_1...A_N|K_{r_\phi}} = \gamma_{A_1...A_N} - \sigma_{A_1...A_N,K} \left(\gamma_K + \gamma_\theta\right)^{-1} \sigma^T_{A_1...A_N,K}, \tag{2.20}$$

where $\sigma_{A_1...A_N,K}$ is the correlation matrix between modes $A_1...A_N$ and K, and

$$\gamma_\theta = \begin{pmatrix} \frac{1-\eta}{\eta} & 0 \\ 0 & \frac{\eta}{1-\eta} \end{pmatrix} = \begin{pmatrix} \tan^2\theta & 0 \\ 0 & \tan^{-2}\theta \end{pmatrix}$$

is a covariance matrix of the linear combination of quadratures the state is projected on. For the balanced heterodyne measurement $\gamma_\theta = \mathbb{I}$. The displacement of the remaining state becomes

$$d_{A_1...A_N|r_K} = d_{A_1...A_N} + \sigma_{A_1...A_N,K} \left(\gamma_K + \gamma_\theta\right)^{-1} \left(Q_K - d_K\right), \tag{2.21}$$

here $Q_K = \{X_K, P_K\}$ is the result of measurement (either of quadratures) of the mode K.

In reality homodyne detection is always nearly perfect, however, to be safe from overestimating results we need to consider that the detectors efficiency is limited, there is loss on the beam-splitter, the beam-splitter is not perfectly balanced, electronic noise is added on detectors, small phase shifts between the signal and LO can happen in the channel. The multimode local oscillator can be imperfectly matched with the modes of the state.

Usually the local oscillator comes from the same laser that is used to generate the entangled signal state and is sent together with the state through the same channel. Longer channels can introduce phase and intensity fluctuations to the local oscillator that destroy perfect phase-matching necessary for homodyne detection. Generally noise in homodyne detection can arise from different (assumed to be statistically independent) sources: state preparation, Raman scattering, relative intensity noise, residual phase noise [84]. Fluctuations of the local oscillator intensity can lower the calibration of vacuum variance, affecting correctness of covariance matrix evaluation and security of CV QKD protocols [85, 86]. To avoid this, a local-local oscillator can be generated by a separate laser at a receiver station that is phase-locked with the signal phase [87].

2.2 Gaussian entanglement

For the multimode states entanglement is a complicated issue, even narrowing down to Gaussian states only, as different partitions can be considered. In this thesis, devoted mainly to bipartite CV QKD, we consider only bipartite entanglement and the task of multiplexing of bipartite entanglement. It is necessary, although not sufficient, resource for many of quantum communication applications, in particular for QKD. We are interested in the communication protocols where two parties A and B aim to distribute a multimode entangled state, however, our considerations can be generalized to any two-parties in more complex communication scenario. To compare behaviour of entanglement and secure key

rate, we have to discuss the distribution of Gaussian entanglement in more details.

Phenomenon of entanglement overcomes limits of of separability of quantum states. Separability of a state means that it can be generated with only local operations and classical communication. The composite system is entangled if and only if it is not separable. To define separability of pure states, consider Schmidt decomposition $|\psi\rangle = \sum_i a_i \ |u_i\rangle \otimes |v_i\rangle$, then separability of a given pure state means it can be written as $|\psi\rangle = |u_A\rangle \otimes |v_B\rangle$ and its Schmidt rank is 1.

The entanglement for mixed states is defined generalizing this concept. The two-party system is separable if it's density operator can be presented as $\hat{\rho} = \sum_i a_i \ \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2}$. However, without exact and complete knowledge of full density matrix it is hard to conclusively estimate if the state is entangled or not. In [88, 89] Simon and Duan et al. showed that negative partial transpose is a sufficient and necessary criterion of entanglement for a bipartite Gaussian state (as well as for the Gaussian approximation of the bipartite state). For general system with arbitrary number of parties the negativity of partial transpose is only a sufficient condition [6,90]. Operational entanglement measures are numerous and they continue to develop: entropy of entanglement (von Neumann entropy), distillable entanglement, entanglement of formation, entanglement cost, etc. [91]. Particular case of Gaussian states entanglement is investigated far better than more general case for both bipartite and multipartite systems [92, 93].

Transposition for continuous variables means complex conjugation of the density operator, the time evolution operator changes sign, as $i\frac{\partial}{\partial t} \to -i\frac{\partial}{\partial t}$, effectively for Gaussian states only relevant change is in signs of momentum operators $\hat{p}_i \to -\hat{p}_i$. Negativity of partial transpose of a bipartite system AB means time reversal for one party can make the joint state unphysical, no longer satisfying inequality Eq.(2.4)

$$\Gamma_A \oplus \mathbb{I}_B \ \gamma \ \Gamma_A \oplus \mathbb{I}_B + i\Omega < 0,$$

where Γ_A is a transpose operator for partial state A.

As an operational measure of bipartite Gaussian entanglement that quantifies negativity of partial transpose we use logarithmic negativity (LN).

$$LN_i = \max\{0, \log_2 ||\rho^{\Gamma_p}||_1\}, \tag{2.22}$$

where $||\rho||_1 = \mathrm{Tr}\sqrt{\rho\rho^\dagger}$ is a trace norm. ρ^{Γ_p} signifies partial transpose of the state ρ.

The logarithmic negativity of Gaussian states can be expressed in terms of symplectic eigenvalues. Before any partial transpose Williamson's decomposition of covariance matrix γ decomposes the initial state with density matrix ρ into superposition of independent thermal states with average photon numbers $\{\nu_i\}$, e.g. TMSV is decomposed into two thermal states. Each of these states has the density matrix $\rho_i = \frac{2}{\nu_i+1}\sum_n^\infty (\frac{\nu_i-1}{\nu_i+1})^n |n\rangle\langle n|$. The states ρ_i are normalized and the respective eigenvalues are positive $\nu_i \geq 1$. This way before partial transpose the trace of each state in decomposition is equal to, 1 $||\rho_i||_1 = 1$, as well as the trace of the total state $||\rho||_1 = 1$. After partial transpose the new state ρ^{Γ_p} can be transformed by Williamson decomposition into superposition of different thermal

states with mean photon numbers $\{\tilde{\nu}_i\}$. If the state is entangled one of its eigenvalues is to be $\tilde{\nu}_- < 1$ and for this eigenvalue the trace norm is $||\rho_-||_1 = \frac{1}{\tilde{\nu}_-}$, for all other non-negative eigenvalues the trace continues to be $||\rho_i||_1 = 1$. This way for TMSV the trace $||\rho^{\Gamma_p}||_1 = \frac{1}{\tilde{\nu}_-}$ and the Eq. (2.22) simplifies to [94]

$$LN_i = \max\{0, -\log_2 \nu_-\}, \tag{2.23}$$

Logarithmic negativity, being an entanglement monotone [95], is a widely used operational entanglement measure for Gaussian states.

Similarly to separability of states, separability of channels can be defined. Operational equivalent to a very formal mathematical idea of separability of channels as CPTP maps is local operations and classical communication (LOCC). All LOCC are separable but there exist separable channels that are not LOCC [96]. A real world implementation would be two distant labs that can process quantum information inside each lab only locally (through CPTP maps) and can communicate outcomes of local operations through a classical channel.

Figure 2.2: Basic one-way entanglement distribution protocol

The simplest Gaussian entanglement distribution protocol is described by the scheme given in Fig. 2.2. One party (Alice) possesses a source of TMSV states, she shares it with the remote party (Bob) through a quantum channel that introduces loss and adds noise to the shared state. The parties have additional free access to classical communication channel and can perform other operations locally in each lab (including Gaussian measurements), i.e. only LOCC can be performed on the shared state. The noiseless channel (either free space of fiber) with constant transmittance T can be modeled as a simple beam-splitter interaction that couples one of the modes of the signal to a vacuum state. The channel also adds excess noise ε to the second quadrature moments, transforming TMSV (2.8) into:

$$\gamma'_{AB} = \begin{pmatrix} V\,\mathbb{I} & \sqrt{T(V^2-1)}\,\mathbb{Z} \\ \sqrt{T(V^2-1)}\,\mathbb{Z} & [T(V-1)+1+\varepsilon]\,\mathbb{I} \end{pmatrix} \tag{2.24}$$

Both attenuation and excess noise make entanglement to deteriorate from

$$LN = -\frac{1}{2}\log_2(2V^2 - 1 - 2V\sqrt{V^2-1})$$

for TMSV to

$$LN = -\frac{1}{2}\log_2\frac{1}{2}\Big[1 + 2T(V^2-1) + T^2(V-1)^2 + V^2 - [1+V+T(V-1)]\times \sqrt{(T^2+1)(V-1)^2 + 2T(V-1)(V+3)}\Big] \tag{2.25}$$

for TMSV after pure loss channel.

An asymptotic limit for entanglement that can be distributed with one maximally entangled state is given by the fundamental repeaterless bound [50]. The bound on entanglement shared through a pure loss channel of transmittance T with an ideal TMSV state in the limit of infinite squeezing $r \to \infty$ is

$$LN(T) = -\log \frac{1-T}{1+T}. \tag{2.26}$$

Entanglement is deteriorated by channel loss, but in idealised case of pure loss channel no attenuation ($T > 0$) can fully destroy entanglement. For channels with additive noise ε the repeaterless bound is lowered to

$$LN(T) = -\log \frac{1-T(1-\varepsilon)}{1+T}, \tag{2.27}$$

giving the fundamental limit on maximal tolerable the excess noise added by two vacuua, above this noise level entanglement of any Gaussian state is destroyed.

2.3 QKD

The goal of cryptography, to securely encrypt a message shared among the remote parties, can be accomplished with algorithms that are either computationally secure or information theoretic secure. The majority of currently wide spread algorithms ensure secure encryption by computation complexity (like RSA algorithm that relies on impossibility to factorize product of prime numbers in polynomial time with classical computers). But the quantum Shor's algorithm [97] does allow to solve the factorisation problem by quantum computer in polynomial time. The one-time pad is free from this problem [98]; it assumes that the key is as long as the message; it is random (genuinely not pseudo-random). The key is added to message (bit-wise addition modular two – exclusive or – XOR); the resulting cipher-text is sent through a public authenticated channel; the receiver on the other side has a copy of the same key, the receiver adds the key modular two to the cipher-text once more and gets the original message. The key can be used only once.

The task QKD is to generate information-theoretic secure one-time pad for two distant trusted authenticated parties in presence of malicious eavesdropper with unlimited abilities bounded only by laws of physics. Traditionally the parties are referred to as Alice (sender) and Bob (receiver), and Eve (the eavesdropper). Alice and Bob share quantum states through a quantum channel that is considered to be fully controlled by the eavesdropper, and classical communication is happening openly through an authenticated classical channel. The goal of eavesdropper is to get a copy of the key while not bringing in enough noise into state for trusted parties to notice and terminate the protocol. Assumptions about Eve as follows:

- fully controls the quantum channel;

- knows everything Alice and Bob share through public channel (but the channel is authenticated, Eve cannot "impersonate" either side);
- can perform any measurement physically possible (including ones that require quantum memory)
- has unlimited computational power.
- Alice's and Bob's labs are secure. Eve has no access to measurement devices used by Alice and Bob.

In practice a lot of device imperfections make attacks possible for eavesdropper, different levels of trust can be assigned to the measurement devices and ability to characterise the preparation noise.

QKD protocol is to be secure (ε_s-secure), correct (ε_c-correct) and robust [99–101]. Correctness means that barred some small probability ε_c Alice's key and Bob's key are the same $P(K_A \neq K_B) \leq \varepsilon_c$. Robustness means that with some (reasonably large even in presence of noise) probability $(1 - p_{abort})$ the protocol produces secure key and is not terminated. Security is conceptualised as distance between the bit string generated by given QKD protocol and ideal perfectly randomly distributed bit string [99]. Let's assume that Alice and Bob ended up with (identical) key strings $S_A = S_B$ that belong to the key space $\mathcal{S}$, the key has (classical) probability distribution P_S. Although obviously at the start of the CV protocol the state is infinite-dimensional, when the key is discretized the equivalent state becomes a discrete one. To represent the key's state as a joint state with eavesdropper's (quantum) state ρ_E, it can be written as an operator $\rho_S = \sum P_S(s)|s\rangle\langle s|$ in orthonormal basis $|s\rangle$ on Hilbert space $\mathcal{H}_\mathcal{S}$. Then the condition on distance between the key state and ideal fully mixed state being less than arbitrary small ε_s is

$$\frac{1}{2}\|\rho_{SE} - \rho_U \otimes \rho_E\|_1 \leq \varepsilon_s \tag{2.28}$$

with $\rho_U = \frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}} |s,s\rangle\langle s,s|$ is an operator representation of randomly uniformly distributed key (which is equivalent to a finite-dimensional fully mixed state) and $\rho_{SE} = \sum P_S(s)|s,s\rangle\langle s,s| \otimes \rho_E^s$ is a tripartite state operator of whatever key was actually obtained [99]. Eve can prepare any global state and make it interact with all the modes in all the pulses shared by trusted parties and measure resulting many-mode state collectively, she is allowed to perform any global unitary transformation on her many mode-state prior to measurement. Even if the state prepared by Alice was optimal independent and identically distributed one, Eve can meddled with it and change the distribution.

Variety of one-way CV protocols exist using different source states, either single-mode states (coherent, squeezed, even thermal states) or two-mode entangled states. Protocols in CV QKD can be either entanglement based (EB) or prepare-and-measure (PM). In PM protocol one side has a source of single-mode carrier states and encodes normally distributed random variables (independent ones in x and p quadratures) into them by applying (truly random) displacements to the state. In EB protocols each party measures one mode of a shared bipartite entangled state.

PM protocols can employ both Gaussian [22, 23] and non-Gaussian modulation [29], we only concentrate on Gaussian modulation ones. Any Gaussian PM protocol has an EB equivalent, assuming ideal modulation they are indistinguishable from the point of view of the eavesdropper. To prove security of PM protocol it is sufficient to prove security of the equivalent entanglement based one [83].

Prior using any QKD protocol Alice and Bob authenticate themselves using classical channel, decide on the postprocesing stage (which error correction code, hash functions to use for reconciliation and privacy amplification, how to discretize the measured data into the alphabet etc.)

Stages of a generic one-way Gaussian protocol:

1. State preparation. For PM protocol state generation: Alice prepares a set of single-mode states (either coherent or squeezed states are used in different protocols [20, 22, 23]), then applies Gaussin modulation displacing the states according to i.i.d. two-dimensional random distribution with 0 mean and variance V. The modulated states are sent to Bob.
   For EB protocol Alice prepares many copies of TMSV state, keeps one mode to herself, and sends the second mode and the local oscillator to Bob through the channel. The channel can be free space or fiber, for the security proofs without loss of generality it can be assumed to be Gaussian due to the proofs relying on extremality of Gaussian sates [66].

2. State measurement. In PM protocol Bob only, in EB protocol both sides use homodyne detection. We assume that the devices are trusted, i.e. their imperfections are reliably accounted for in the device's theoretical model, Eve has no access to either of the measurement devices and no imperfection can be attributed to her tampering. In protocols with homodyne detection Bob measures a randomly chosen quadrature and informs Alice of his quadrature choice, or, in protocol with heterodyne detection, both quadratures are measured. Discretization of continuous variables according to agreed alphabet gives both sides two strings of measured results $\{a_1, ..., a_N\}$ and $\{b_1, ..., b_N\}$.

3. Information reconciliation. The string that belongs to one of the trusted side is treated as a raw key, the other side has to correct their string to match the raw key. If the reference side is Alice the reconciliation is called direct, if the reference side is Bob the reconciliation is reverse, (in practice it is almost always beneficial to use reverse reconciliation for better robustness against loss [83]). Both sides apply pre-agreed linear error correction code [102] to their strings and the reference side (Bob) sends error syndrome to Alice, who uses a co-set error correction code (depending on error syndrome received) to correct her data string to match the raw key. Then they both calculate predetermined hash function and compare results, if the results coincide with probability $1 - \varepsilon_{err}$ the error correction was successful, both sides now share same raw key $\{b_1, ..., b_N\}$, otherwise this attempt failed and the raw key has to be discarded.

4. Parameter estimation. Evaluation of the upper bound on the eavesdroppers information: At this step the sides disclose some portion of data to estimate the bounds on covariance matrix of the shared state [103–105]. Depending an amount of information available to the eavesdropper they determine length of the key l that is secure from Eve. If the estimated parameters are above certain threshold, meaning too much of shared state leaked to the eavesdropper, the protocol is aborted.

5. Privacy amplification. Alice chooses hash function [102], a one-way function that maps a data string to a shorter string of fixed length, and declares the function to Bob. They both apply the hash function to their data strings to obtain shorter uniformly distributed data sets $S_A = S_B$ of length l that is uncorrelated to Eve's data [106].

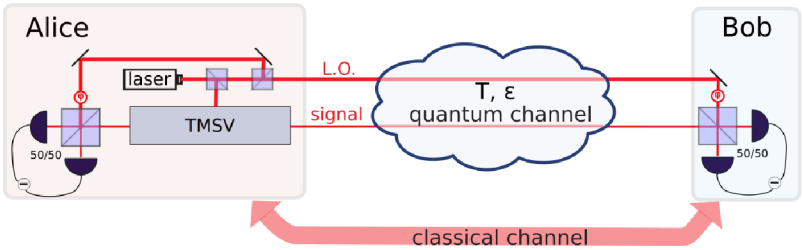

Figure 2.3: Basic scheme of one-way entanglement-based CV QKD protocol with homodyne detection [20] using real local oscillator generated from the same laser as the TMSV state. The sender Alice generates a TMSV state, she shares one of the modes together with the phase reference through attenuating noisy quantum channel with the receiver Bob. Both sides measure their respective modes with homodyne detectors and proceed to postprocessing of the measurement results using classical channel to generate the secret key. The quantum channel is assumed to be controlled by the eavesdropper, the classical channel is authenticated and public, while Alice's and Bob's labs, where the measurements and the state preparation happen, are secure from eavesdropper. This simplified protocol scheme is similar to ones implemented in the experiments [107–109]

The entanglement distributed as in Fig. 2.2 can be used to generate the secret key in EB QKD protocol, if several additional assumptions, about eavesdropper's abilities and about security of the state preparation and homodyne measurement, being met. The operational scheme of such entanglement-based protocol is given in Fig. 2.3. In her lab, secure from eavesdropper's interference, Alice prepares the TMSV state with covariance matrix given by Eq.(2.8), she measures one of the modes of TMSV with a homodyne detector and sends the other mode together with the local oscillator through the quantum channel of transmittance T to Bob. In his secure lab Bob measures the state by homodyne detection randomly switching between the quadratures. The parties proceed to information reconciliation and privacy amplification as described above in the protocol outline using authenticated public classical channel. The covariance matrix of the shared state γ_{AB} Eq. (2.24) after Bob measures one of the quadratures (here, without

loss of generality, quadrature $\hat{p}$ is chosen) becomes

$$\gamma'_{A|B} = \begin{pmatrix} V & 0 \\ 0 & V - \frac{T\left(V^2-1\right)}{TV-T+1+\varepsilon} \end{pmatrix}. \tag{2.29}$$

The secret key per channel use is calculated as difference between the information between Alice and Bob, and the information between Eve and the reconciliation side (the side that discloses information about their state). While generating the key in the postprocessing stage of the protocol Alice and Bob access classical information contained in their shared state. Classical information is Shannon entropy $S(X) = \sum_{x\in X} -p(x)\log p(x)$ [98]. Taking into account that the state is Gaussian, their mutual classical information is calculated using the covariance matrix $S(\gamma_{AB}) = I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}$. When assessing how much the information leaked to the eavesdropper, we must estimate upper bound on quantum information available to her. The quantum analogue of Shannon entropy of quantum state ρ is von Neumann entropy $S(\rho) = -Tr[\rho\log\rho]$. For a Gaussian state von Neumann entropy can be expressed in terms of symplectic eigenvalues (2.14), it is computed as $S(\nu) = \sum_{k=1}^{N} G(\nu_k)$, where $\mathrm{G}(x) = (x+1)\log_2(x+1) - x\log_2 x$ [63]. Upper limit on information that can be shared using quantum system ρ which contains subsystems ρ_x is given by the Holevo bound

$$I(\rho) \leq S(\rho) - \sum_i p_x S(\rho_x), \tag{2.30}$$

here p_x is conditional probability to find the measured system in state ρ_x [110].

Assuming that sides can use protocol infinite number of times (infinite key length), Devetak-Winter bound [111] gives the asymptotic secret key rate.

$$K = \max\left\{0, \beta I_{AB} - I_{AE/BE}\right\} \tag{2.31}$$

$\beta \in [0,1]$ is postprocessing efficiency, it depends on error correction algorithm used in classical postprocessing, in practice it can be close to 0.96 [112] for Gaussian (or nearly Gaussian) data sets. $I_{AE/BE}$ is information among either Alice or Bob chosen as a reference side and Eve. Historically the first approach introduced in CV QKD was direct reconciliation [22], where Alice is the reference side in the reconciliation step. In this direct reconciliation virtually all loss occurs between the signal source and the remote side, and the channel attenuation of more than T=0.5 (3 dB) means information between Alice and Bob is less than information between Alice and Eve, the security is destroyed and the protocol is to be aborted. Reverse reconciliation with the remote side as the reference does not have 3 dB attenuation threshold [113]. Any practical one way QKD protocols use only reverse reconciliation and in this work we always assume Bob to be the reference side.

The states employed in the protocol don't necessary need to be Gaussian. A security proof for Gaussian states is sufficient, due to their extremality among all other quantum

states [66]. Gaussian states are the minimally entangled states among all CV states with same displacement and covariance matrix as given Gaussian state: for any state ρ there is a "Gaussified" state ρ_G (a Gaussian state that has same first and second moments) for which $f(\rho) \geq f(\rho_G)$. Here f is a continuous functional acting on bounded linear operators on the Hilbert space $\mathcal{H}$, which is invariant and strongly super-additive under local unitaries $f(U^{\otimes N}\rho U^{\dagger\otimes N}) = f(\rho)$ [66]. This leads to Gaussified state giving a lower bound on some entanglement measures (but not logarithmic negativity Eq. (2.23) [114]) for a non-Gaussian state and also the upper bound on quantum information and Holevo number (Gaussian states maximize von Neumann entropy allowing to estimate the lower bound of secure key rate).

Attack strategies for eavesdropper. Eve having control of the channel implies that she can replace the real channel with a simulated one, that will be indistinguishable for the trusted parties from the real channel only with different level of noise. Any kind of attack happening in the channel can be modeled with Eve preparing probe states that interact with the signal states in the channel, the probe states are then stored and subsequently measured by Eve. Eavesdropper can perform attacks of different levels of generality depending on how Eve's probe state are prepared and measured: individual, collective [22, 115, 116] and coherent attacks [36, 117]. It in turn gives restrictions on how Eve can prepare her probe states and how they can be stored and measured by her.

1. Individual attacks [118]: during each round of protocol Eve's probe state interacts with each signal state separately, all the probe states , and the are stored in quantum memory and, after post-processing step of the protocol is finished, each probe state is measured by her separately in the correct basis.

2. Collective attacks [115, 116, 119]: Eve performs independent attack in each round, her probe states are prepared individually each time and stored in a quantum memory after the interaction with the signal, after the protocol is finalized Eve accesses all probe states collectively performing optimal global measurement. The protocol is secure if the signal states prepared by Alice are known to be i.i.d. [19].

3. Coherent attacks [36, 37, 120]: there are no limitations on the probe states Eve can prepare and on correlations between her probe states, we have to assume that before protocol begins she prepares an optimal entangled state, this global probe state interacts with the signal states in each round of protocol and after she measures the probe state collectively. Proven security against coherent attacks guarantees that the protocol is secure independently of what actual signal states were prepared by Alice, signal states used in each round of protocol can have arbitrary correlations with each other.

Gaussian attacks, using Gaussian probe states, are optimal for Eve on any level of generality [116]. In most cases the more general attacks are the more information eavesdropper gets, the coherent attacks are the optimal ones for eavesdropper. There are some special cases where less general attacks are proven to also be optimal. Taking into account realistic expectation, that Eve's probe states stored in quantum memory experience some

decoherence, individual attacks can be optimal [121]. In more general case, assuming infinitely long blocks (asymptotic regime) and symmetric parameter estimation and privacy amplification algorithms (which is practically always the case), the secret key rate for coherent attacks is shown to converge to collective attacks key [115]. Gaussian de Finetti reduction [122, 123] together with extremality of Gaussian states [66] allows to only consider Gaussian collective attacks instead of general attacks for certain entanglement-based protocols and the corresponding PM protocols. It has been proven only for protocols with squeezed states and heterodyne detection (randomly switching between quadratures) or homodyne detection [37, 104, 115, 116]. Nevertheless security against Gaussian collective attacks is a useful benchmark for any protocols.

To prove security against collective attacks in the asymptotic limit of infinitely long key, taking into account extremality of Gaussian states, we assume that the initially pure Gaussian state ρ_{AB} prepared by the sender is coupled to Eve's probe state while passing through the noisy channel, becoming a three-party state ρ_{ABE}. We assume that in each use of the protocol, Eve has access to and is able to perform any collective measurement of the rest of the three-party pure state (Eve holds purification of the state shared between Alice and Bob). The upper bound on her information is given then by the Holevo bound (2.30). Using the fact that the total ρ_{ABE} state is pure, the von Neuman entropy of the state available to Eve is equal to the entropy of the state shared by Alice and Bob $S(\rho_E) = S(\rho_{AB})$. The secure key rate against collective attacks is [124]:

$$K = \max\{0, \beta I_{AB} - \chi_{BE}\} \tag{2.32}$$

here $\chi_{BE} = S(\gamma_E) - S(\gamma_{E|B})$ is Holevo bound (2.30) for Gaussian state with covariance matrix γ, difference of von Neumann entropy in the state available to Eve and the same state conditioned after measurement by the remote party. It gives the upper bound on information contained in the parts of state that can be available to Eve, due to channel loss and the protocol implementation imperfections. While the most conservative assumption to prove security against collective attacks is that Eve purifies the state, in the case if it can be certified that part of noise and loss that occur during state generation or on the detectors, indeed occurred inside the secured laboratories, the purification assumption assigning all the noise present in the state shared between Alice and Bob to the meddling by the eavesdropper can be relaxed, then $S(\rho_E) \neq S(\rho_{AB})$.

2.4 One-way Gaussian communication protocol with multimode states. Model of the cross talk

Multiplexing can increase robustness of quantum information protocols, allow parallel processing of information, increase transmittance capacities of channels. Source used for multiplexing can be intrinsically multimode source, for example a frequency comb, used in the following analysis and experiment, or it can be a set of single mode sources. Channel multiplexing in CV can be done with already accessible technologies, such as deterministic

squeezing sources, multicore fibers and mode discriminating homodyne detection. to increase capacity of quantum communication protocol.

We consider multiplexing of the two-mode protocols in Sections 2.2 and 2.3, where to increase capacity N protocols are implemented in parallel. The basic protocol with two parties sharing a TMSV state (i.e. two signal modes) through a lossy and noisy channel of attenuation T, with the excess noise ϵ, is extended to the case of N replicas of TMSV states (2N modes) and N channels. Ideally the pairs of modes do not interact between themselves and the modes are perfectly discriminated at the measurement stage. Then adding multiple modes becomes simply a question of scalability, scaling up the number of separate entangled pairs of modes shared times N and increasing the secret key rate of QKD protocols N-folds.

Due to imperfections in the process of the state generation, sharing through channels and measuring, the modes can get coupled to each other. We refer to this extra coupling as inter-mode cross talk. We apply linear cross talk model to initially independent TMSV states: multiplexed source starts as N independent two-mode states that are coupled to each other either in the channel, during measurement or the state preparation. Fig. 2.4 shows the simplest possible case: a two-fold multiplexed entanglement distribution protocol, where two TMSV sources start independently and linear cross talk occurs in the receiver before the modes enter the channel [45, 51]. Our model assumes that the sender possesses two sources of TMSV states (making the four-mode total state $A_1A_2B_1B_2$), the modes B_1B_2 are shared with the remote party through an attenuating channel with excess noise ε (the channel attenuation is considered unbalanced, being different for each mode). On the senders side the modes B_1B_2 get coupled to each other, experiencing the cross talk. We model cross talk as linear beam-splitter-like interaction between the signal modes, in Fig. 2.4 it is depicted as a beam-splitter of transmittance t_c. Of course in reality modes can experience more complicated interaction between each other, but the goal of our work is to only study the basic cross talk that is most likely to occur through linear coupling and can be compensated by the trusted parties applying LOCC.

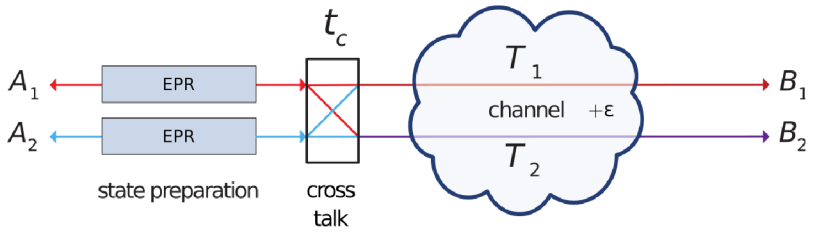

Figure 2.4: Entanglement distribution scheme with two pair of TMSV states, where cross talk is modeled as a beam-splitter of transmittance t_c

The initial state is a product of two TMSV states given by (2.8), assuming that the states squeezing parameters are identical and their variances are both V, their joint covariance matrix is $\gamma_{A_1A_2B_1B_2} = \gamma_{A_1B_1} \oplus \gamma_{A_2B_2}$. After the linear cross talk mixes signal

modes and the channel attenuates them, the covariance matrix becomes

$$\gamma_{A_1A_2B_1B_2} = \begin{pmatrix} V\ \mathbb{I} & \sqrt{t_cT_1}\sqrt{V^2-1}\ \mathbb{Z} & 0\ \mathbb{I} & -\sqrt{r_cT_2}\sqrt{V^2-1}\ \mathbb{Z} \\ \sqrt{t_cT_1}\sqrt{V^2-1}\ \mathbb{Z} & [T_1(V+\varepsilon-1)+1]\ \mathbb{I} & \sqrt{r_cT_2}\sqrt{V^2-1}\ \mathbb{Z} & 0\ \mathbb{I} \\ 0\ \mathbb{I} & \sqrt{r_cT_1}\sqrt{V^2-1}\ \mathbb{Z} & V\ \mathbb{I} & \sqrt{t_cT_2}\sqrt{V^2-1}\ \mathbb{Z} \\ -\sqrt{r_cT_1}\sqrt{V^2-1}\ \mathbb{Z} & 0\ \mathbb{I} & \sqrt{t_cT_2}\sqrt{V^2-1}\ \mathbb{Z} & [T_2(V+\varepsilon-1)+1]\ \mathbb{I} \end{pmatrix}, \tag{2.33}$$

here $r_c \equiv 1 - t_c$.

We study the multimode protocols theoretically, not bounding the model we use to any particular experimental implementation. In practice mode multiplexing can be implemented in either spatial or frequency domain. The spatial modes can use similar frequencies, as in the wavelength division multiplexing with multicore fibers [45, 48, 125] where the cross talk occurs between neighbouring cores. Then each core has to be treated as a separate channels with linear cross talk between closest neighbouring channels (the experiment in [45] was designed in a way that quantum signal could only experience cross talk with classical signals in neighbouring cores, but for the goal of large-scale mode multiplexing more cores would be used for quantum signal with cross talk occurring between them). Another approach to multiplexing is using frequency domain, examples of frequency-multiplexed states can be several independent TMSV states with different frequencies that experience cross talk while being shared through multimode fiber channel or a frequency-multiplexed state generated by synchronously pumped optical parametric oscillator [53,126–128] where different frequency modes can become coupled to each other during measurement.

Important example of a device that produces the multimode Gaussian state for this thesis is a synchronously pumped optical parametric oscillator (SPOPO). It is an intrinsically multimode source that produces many entangled photon-pairs in all frequencies, some of these can be accessed by mode-discriminating homodyne measurement. SPOPO is an optical parametric oscillator, in which sequence of very short (and broad in spectrum) pulses is sent to the cavity containing a nonlinear crystal in such a way, that the pulses travelling between mirrors inside the cavity and new arriving pump pulses are synchronised. As in normal OPO bellow threshold that is pumped with single frequency, each spectral component resonant with the SPOPO cavity undergoes parametric downconversion process $\omega_{p_i} = \omega_{1_i} + \omega_{2_i}$ and if pump is centered around ω_0 the output state is centered around $\omega_0/2$. In the same time its output is not equal to just sum of all possible downconversion processes as the phase matching and momentum conservation conditions allow several processes to scatter into the photons of the same frequencies. The state generated by the SPOPO is Gaussian entangled state that is basically a frequency comb but with each frequency in given spectrum present. The state is entangled in frequency domain, which corresponds to a set of squeezed states in domain of Hermite-Gaussian modes. While the generated states contains huge number ($\sim 10^5$) of frequency modes, such a big number of modes cannot be accessed individually, but it can be sliced into narrow frequency bands which then can be measured separately with multipixel homodyne detection. Further these narrow frequency bands (and not single frequencies) will be referred to as spectral modes. Multipixel detection allows to measure all the modes

simultaneously, it is fully analogous to the single-mode homodyne detection described earlier but both multimode signal and multimode oscillator are dispersed on gratings into spectra that is then focused on two photodiode arrays [128].

Frequency multiplexed multimode state generated by SPOPO according to Eq. (2.17) can be from the point of view of theory treated as a result of mixing of N independent thermal modes that undergo basis change and each mode is then squeezed in this new basis (these are the squeezed Hermite-Gaussian modes), then the modes are mixed again with another basis change to the frequency basis. The frequency modes can be (to certain extend) experimentally accessed by multiplexed homodyne detection. The measured spectral modes are imperfect, they create an incomplete basis. It only approximates the orthonormal basis that can be transformed into Hermite-Gaussian basis of squeezed supermodes. The experiment [129] showed that it is possible to get sufficiently good access to the supermodes, proving that the measurement captured most of the SPOPO frequency range, and the measured state is close to its theoretical model. In this experiment all the frequency modes were measured simultaneously, while switching between quadratures $\hat{x}$ and $\hat{p}$, and the covariance matrix was estimated had negligible intramode $\hat{x} - \hat{p}$ correlations. Although the SPOPO generates multipartite entanglement, for the purpose of the two-party QKD the frequency modes are shared between two sides and in the very end only bipartite correlations shared among the trusted parties contribute to the key generation. The parties can only access classical information carried by the modes in frequency domain, while the eavesdropper has access to the state "leaked" through the channel as a whole and the Holevo bound on Eve's information is calculated from the states thermal decomposition (2.17).

In general any practical implementations of CV sources contain multiple modes, in either frequency spectrum or any other degree of freedom. In the use-case we described above the multiple modes are a resource for mode multiplexing. In another possible case if extra modes appearing due to imperfections in the state generation, then some modes will inevitably be non-signal ones, they add noise or they can be abused by eavesdropper as side channels [34, 130, 131]. In this thesis besides mode multiplexing scenario we also consider another many-mode scenario where extra modes are generated all in the same state and are used in a QKD protocol to increase signal's brightness, making it easier to handle in the experimental setting. An obstacle to use these macroscopically bright states in QKD can appear when the modes of the bright states don't perfectly match with the local oscillator while being measured with mode-non-discriminating homodyne detection [62].

3 | Cross talk compensation for multi-mode entanglement distribution

This Chapter mainly overviews the results of the published paper (see [1] Chapter 6). The paper is concerned with effects of a linear cross talk in an entanglement distribution scheme in Fig. 2.4 of Section 2.4. Preparing and distributing multiplexed entangled states with significant number of modes almost inevitably leads to cross talk between the modes [132–134]. We use a significantly simplified model of linear cross talk in distribution of two TMSV states to demonstrate possibility to compensate its negative effects with local manipulations of data on one of the sides of communication protocol. This data processing uses advantageous properties of continuous variable states and measurements that has no known analogy with single photon DV QKD.

3.1 Theoretical model

In the entanglement distribution scheme with cross talk in Fig. (2.4) the initial logarithmic negativity of one TMSV state Eq.(2.8), before any cross talk and the channel loss occurs, is

$$LN_0(V) = -\frac{1}{2}\log_2\Big(2V^2 - 1 - 2V\sqrt{V^2-1}\Big), \tag{3.1}$$

After taking into account the cross talk, the channel attenuation and the excess noise, the logarithmic negativity of the first mode A_1B_1 of the shared state with the covariance matrix $\gamma_{A_1A_2B_1B_2}$ in Eq. (2.33) becomes

$$\begin{aligned} LN = -\frac{1}{2}\log_2\frac{1}{2}\Big(1 + 2T_i[\varepsilon + (V-1)(t_cV + t_c + 1)] + \\ T_i^2(\varepsilon + V - 1)^2 + V^2 - [1 + V + T_i(\varepsilon + V - 1)]\times \\ \sqrt{T_i^2(\varepsilon + V - 1)^2 + (V-1)^2 - 2T_i(V-1)[\varepsilon - 2t_c(V+1) + V - 1]}\Big). \end{aligned} \tag{3.2}$$

In the Section 2.2 Eq. (2.25) shows how entanglement in a single pair of modes is reduced by the channel attenuation. The presence of the cross talk reduces the entanglement even further and also makes it more sensitive to the destructive influence of the excess noise. These effects are plotted in Fig.(3.1) for the modes pair A_1B_1. In the left panel the shared logarithmic negativity is plotted versus the initial logarithmic negativity of a single TMSV state demonstrating how presence of the cross talk suppresses the shared entanglement

and creates a maximal limit for it. The right panel illustrates how the presence of the cross talk makes the $\varepsilon = 2$ SNU limit on the maximal tolerable excess noise tighter.

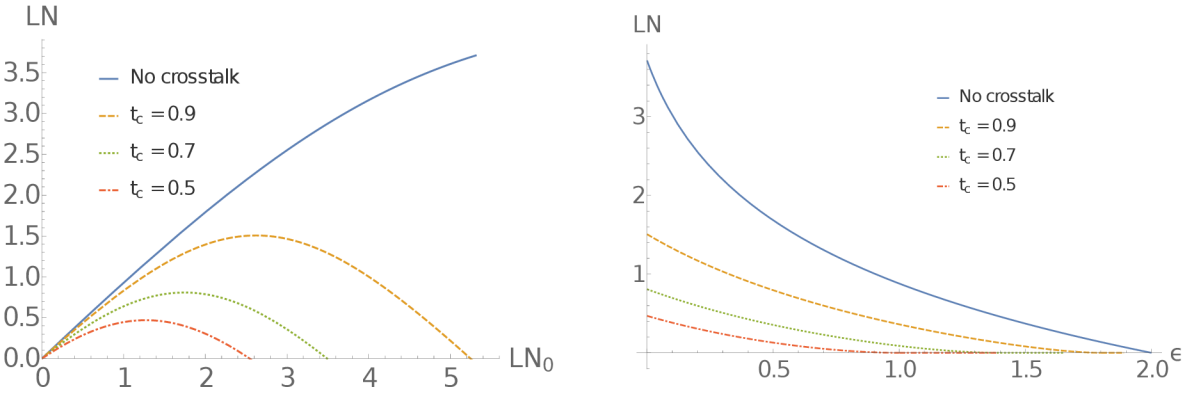

Figure 3.1: Gaussian logarithmic negativity of the pair of modes A_1, B_1 after cross talk t_c and after passing through a quantum channel versus the initial logarithmic negativity of the state (left) and versus the channel noise (right). The channel transmittance for both the modes is $T = 0.9$. Left: no excess noise $\varepsilon = 0$. Right: fixed signal state variance $V = 5$.

Without the cross talk the shared entanglement increases monotonously with the state variance and, in principle with the squeezing being unlimited, it can grow up to the repeaterless bound Eq.(2.26) of the entanglement distribution. In the limit of infinite state variance ($V \to \infty$) and no cross talk in the attenuating channel with excess noise the repeaterless bound Eq.(2.26 depends not only on on T but also ε and becomes

$$\lim_{V\to\infty} LN = -\log_2 \frac{1 - T_i(1-\varepsilon)}{1+T_i}. \tag{3.3}$$

In the presence of cross talk with increase of the initial entanglement (or, equivalently, the state variance), the shared entanglement reaches its maximum and vanishes if the initial variance exceeds

$$V_{max} = \frac{1 + t_c - \varepsilon}{1 - t_c}. \tag{3.4}$$

As an example of application for the multiplexed entanglement distribution scheme in Fig. 2.4, we consider a scenario where each mode of the 4-mode entangled state shared by the remote parties is measured with balanced homodyne detectors, and then the parties proceed to establish the secret key among themselves, implementing multiplexed version of the protocol described in Fig. 2.3. The mutual information distributed between Alice and Bob by two pairs of modes is additive and the secure key rate Eq. (2.32) becomes

$$K = \max\left\{0, \beta(I_{A_1B_1} + I_{A_2B_2}) - \chi_{B_1B_2E}\right\}. \tag{3.5}$$

Taking into account the assumption that eavesdropper holds purification of the total state, here $\chi_{B_1B_2E} = S(\gamma_{A_1A_2B_1B_2}) - S(\gamma_{A_1A_2B_1B_2|B_1B_2})$.

By reducing or destroying the state's entanglement, cross talk also negatively influences

the secure key rate. The analogy between the cross talk effects on the secure key and entanglement can be seen comparing Fig. 3.2 to Fig. 3.1. In both cases cross talk introduces limitations on the initial state variance and enhances destructive influence of the excess noise.

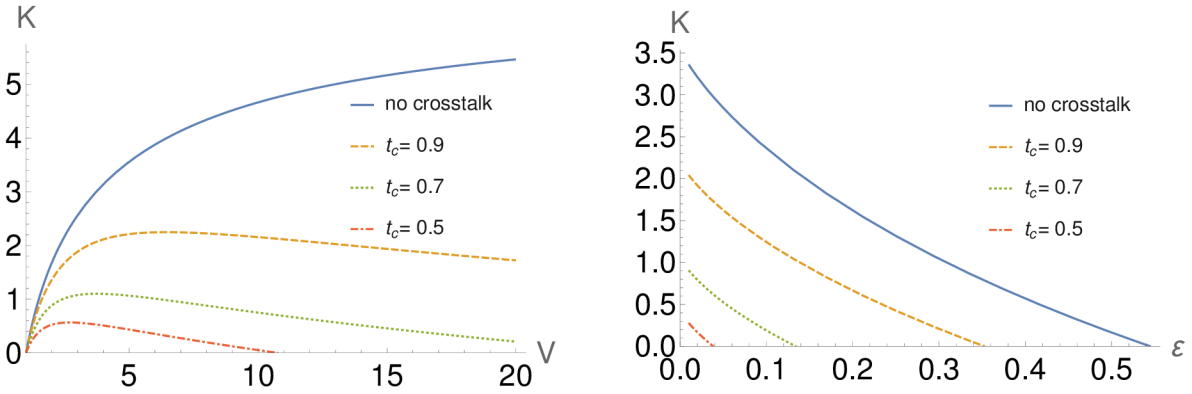

Figure 3.2: Secret key rate for multiplexed state γ_{A_1,A_2,B_1,B_2} with cross talk t_c after attenuation by channel with transmittance $T = 0.9$ versus the initial state variance V of the state (left) and versus the channel noise (right). Left: no excess noise $\varepsilon = 0$. Right: fixed signal state variance $V = 5$. Postprocessing efficiency $\beta = 0.96$.

The initial state variance could be optimized with respect to cross talk t_c and channel parameters T and ε. Depending if the goal is to maximize the logarithmic negativity or the secure key rate, the optimal initial state variance in general would differ. But even with the optimization, the damage done by the cross talk remains significant. As an alternative to the initial state optimization we further proposed two passive optical schemes to eliminate the cross talk and restore entanglement at least partially.

3.2 Cross talk compensation

Linear cross talk we consider in our model should be possible to compensate by the linear interactions, combination of phase shifts and beam-splitters. In a more complicated case with higher number of modes the most general compensating scheme would consist of a sequence of Mach-Zender interferometers, but for a simpler case of two TMSV states we only need a sequence of a phase shift by π on one mode with the modes B_1, B_2 then interacting on a beam-splitter with transmittance t_r, here t_r is the parameter to be optimized.

Applying this decoupling interaction changes the covariance matrix of a pair A_1, B_1 to

$$\gamma_{A_1B_1} = \begin{pmatrix} V\,\mathbb{I} & \left(\sqrt{T_2 r_c r_r} + \sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\,\mathbb{Z} \\ \left(\sqrt{T_2 r_c r_r} + \sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\,\mathbb{Z} & \left[1 + T_1 t_r (V-1) + T_2 r_r (V-1)\right]\mathbb{I} \end{pmatrix}, \tag{3.6}$$

here $r_r \equiv 1 - t_r$. The pair of modes A_2, B_2 has similar covariance matrix up to the

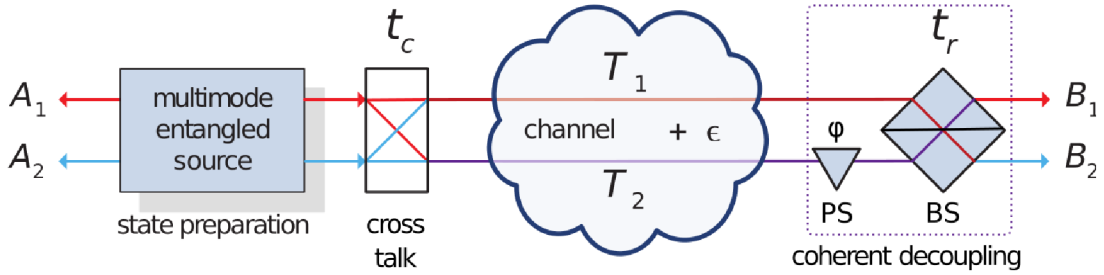

Figure 3.3: Compensating cross talk with optical interference, when the remote side optimally applies phase shift (PS) by π to one of the modes and couples the signal modes on a variable coupler t_r.

replacement of T_1 with T_2.

For a noiseless channel with balanced transmittance (same transmittance for both modes $T_1 = T_2 \equiv T$) it is straightforward to see that putting $t_r = t_c$ turns covariance matrix in Eq. (3.6) into the covariance matrix of a TMSV Eq. (2.24) fully eliminating the cross talk.

In general case the channel transmittance is unbalanced, i.e. it is different for different pairs of modes $T_1 \neq T_2$ (without loss of generality we assume $T_1 > T_2$), then the optimal t_r has to be found numerically. Its value is bound from below and above by two important edge cases of very weak and infinitely strong initial entanglement for the mode pair A_1, B_1

$$t_r^1 = \frac{T_1 t_c}{T_1 t_c + T_2(1 - t_c)}, \quad V \sim 1 \tag{3.7}$$

and

$$t_r^\infty = \frac{T_2 t_c}{T_2 t_c + T_1(1 - t_c)}, \quad V \to \infty. \tag{3.8}$$

For the second pair A_2, B_2 the limits are similar up to $T_1 \leftrightarrow T_2$ substitution, no choice of t_r can maximize entanglement in both pairs simultaneously, it is up to our decision if either pair's entanglement or the average of their entanglement values is to be maximized. Nevertheless any t_r in the interval $[t_r^1, t_r^\infty]$ increases the logarithmic negativity in both pairs compared to the case before compensation.

Applying optimal coupling t_r allows to significantly restore entanglement and to remove the limitations on the maximal initial variance V_{max} in Eq.(3.4). For optimally chosen t_r the logarithmic negativity is an increasing function of V. In Fig. 3.5 the logarithmic negativity restored by optimal decoupling (purple line) grows similarly, albeit being slightly lower, to the logarithmic negativity without any cross talk (given in Eq. 2.25, blue line in the plots). For infinitely large initial state variance and t_r given by (3.8) the logarithmic negativity approaches the limit:

$$\lim_{V\to\infty} LN_{rev} = -\log_2 \left[\frac{t_c T_2 + T_1(1 - t_c - T_2)}{t_c T_2 + T_1(1 - t_c + T_2)} \right]. \tag{3.9}$$

The proposed decoupling method allows to almost fully restore the entanglement and

eliminate the cross talk in both pairs of modes, but it depends on numerical optimization with respect to the generally unknown parameter t_r.

Further we consider an alternative way to compensate for entanglement loss (see Fig. 3.4), that relies on the conditional measurement of one pair of modes (here a more attenuated pair A_2, B_2 is chosen) with feeding forward the measurement result to displace another pair of modes A_1, B_1. This approach allows to increase entanglement in one pair of modes at the expense of completely losing the other pair, but it does not need any prior estimation of the cross talk strength.

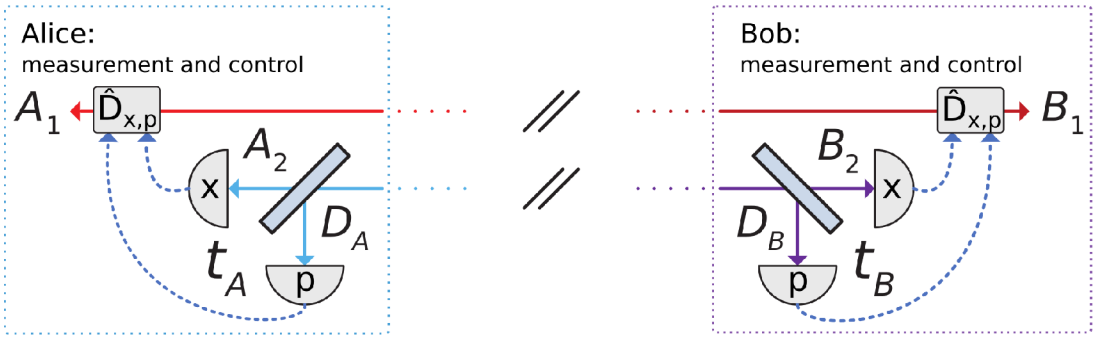

Figure 3.4: Measurement and feed-forward control scheme to compensate the cross talk in the pair of modes A_1, B_1. The two parties perform generalized Gaussian measurements by splitting modes A_2, B_2 on variable beam-splitters t_A, t_B and measuring x-quadratures on the modes A_2, B_2 and p-quadratures on the auxiliary detection modes D_A, D_B. The measurement outcomes are then used to feed-forward modes A_1, B_1. The rest of the scheme (source, cross talk and channel) is as in Fig. 3.3. The scheme allows increasing entanglement in modes A_1, B_1 at the cost of tracing out modes A_2, B_2.

On both sides Alice and Bob perform generalised homodyne measurement dividing the pair A_2, B_2 on beam-splitters of variable transmittances t_A and t_B respectively and then measuring both quadratures. The measurement transforms the state $\gamma_{A_1A_2B_1B_2}$ as given by Eq. (2.20) and (2.21). t_A and t_B are the parameters to be optimized to maximize the logarithmic negativity. The covariance matrix of the first pair of modes $\gamma_{A_1B_1}$, becomes $\gamma_{A_1B_1}^{gen.meas} = \begin{bmatrix} \tilde{\gamma}_{A_1}(t_A,t_B) & \tilde{C}_{A_1B_1}(t_A,t_B) \\ \tilde{C}_{A_1B_1}(t_A,t_B) & \tilde{\gamma}_{B_1}(t_A,t_B) \end{bmatrix}$, in the the explicit form it is given in the paper [1] in Chapter 6. $\gamma_{A_1B_1}^{gen.meas}$ allows to calculate the logarithmic negativity $LN(t_A,t_B)$ from Eq. (2.23 and to maximize it. The optimal measurement of Bob's side does not depend on the state or channel parameters, it is always a homodyne measurement of either of the quadratures, the optimal t_B is either $t_B = 1$ for measurement of $\hat{x}$ or $t_B = 0$ for measurement of $\hat{p}$. Without loss of generality we further put $t_B = 1$. Optimal measurement on Alice's side does depend on the state variance V and the cross talk t_c, channel transmittance T_1 and T_2 and excess noise ε and in general case optimal t_A can only be found numerically. Independently of what kind of the generalized measurement is applied to the pair of modes A_2B_2 (and what t_A and t_B are chosen), the measurement with feed forward always improves the entanglement in the pair A_1B_1.

In the limit of a very short channel with low loss $T_{1,2} \to 1$ the optimal measurement

by Alice is the homodyne detection of a quadrature opposite to the one measured by Bob (e.g. if Bob measures $\hat{x}$, Alice measures $\hat{p}$ with $t_A = 1$). Then the logarithmic negativity of the state in modes A_1, B_1 in the limit of $V \to \infty$, for a noiseless channel ($\varepsilon = 0$) tends to

$$\lim_{V\to\infty} LN_{hom} = -\frac{1}{2}\log_2\left[\frac{(1-T_1)[T_1(1-t_c-T_2)+t_cT_2]}{t_c(1+T_1)^2T_2}\right] \tag{3.10}$$

which may turn to zero for certain (albeit unrealistically strong) cross talk t_c. In the opposing case in the limit of a very long channel with extremely high loss $T_{1,2} \to 0$ the optimal measurement is the balanced heterodyne detection with $t_A = 1/2$. The logarithmic negativity of the pair A_1, B_1 LN_{het} is a growing function of the state variance and in the limit of $V \to \infty$ and no excess noise ($\varepsilon = 0$) it asymptotically approaches

$$\lim_{V\to\infty} LN_{het} = -\frac{1}{2}\log_2\left[\frac{(1-t_cT_1)[1-t_c(T_1-T_2)-T_2]}{(1+t_cT_1)^2-(1-t_c)T_2(1-t_cT_1)}\right]. \tag{3.11}$$

In Fig. 3.5 yellow line illustrates how applying combination of balanced heterodyne detection on sender side together with homodyne on the receiver side allows to restore entanglement in the remaining modes and avoid the limit V_{max} on the initial entanglement.

All the proposed compensation methods are compared in Fig. 3.5 for the cases of longer (left panel) and shorter (right panel) channels. It demonstrates that all the compensation methods allow to significantly restore the Gaussian entanglement. Comparison of the behaviour of yellow and green curves in the left and right panels shows how in case of the feed forward control method for low loss channels superiority belongs to a combination of homodyne detection in opposing quadratures, while for channels with higher loss the combination of homodyne with balanced heterodyne detection gives superior results. But both implementations of the measurement and feed forward approach are less efficient in cross talk compensation than the optimal interference approach. For any realistic values

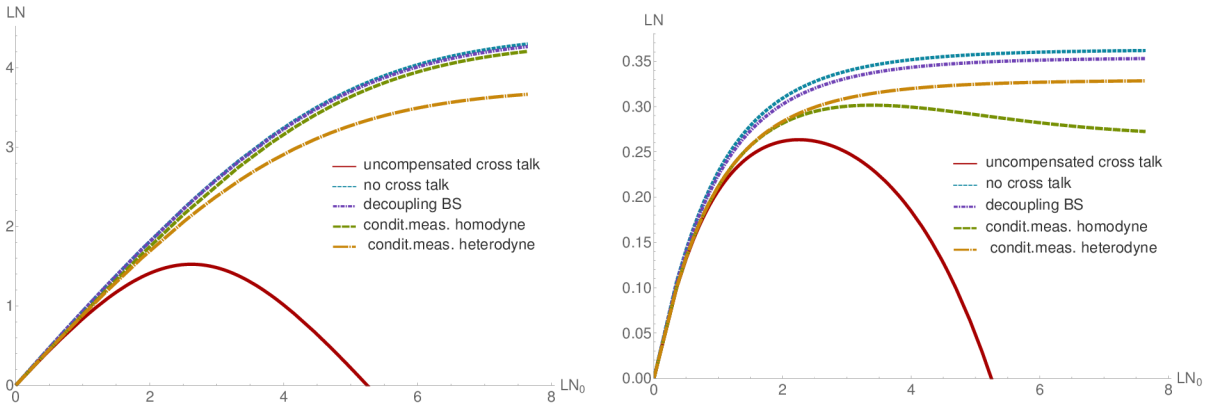

Figure 3.5: Logarithmic negativity in the pair A_1, B_1 after applying optical interference method or measurement of the pair A_2, B_2 and feed-forward control, as indicated in the plots. cross talk is $t_c = 0.9$, decoupling beam-splitter transmittance t_r is given by eq.(3.8), no excess noise ($\varepsilon = 0$). Left: low loss unbalanced channels ($T_1 = -0.4dB$, $T_2 = -0.5dB$), right: high loss unbalanced channels ($T_1 = -9dB$, $T_2 = -10dB$).

the parameters of the state V, the cross talk t_c and channel transmittance $T_{1,2}$ can take, the entanglement restored in the pair A_1, B_1 by optimal feed forward measurement (LN_{hom} orLN_{het}) is always lower than the entanglement after compensating interference method LN_{rev} in Eq.(3.9). The exception is a quite unrealistic situation where the transmittance for each pair modes is drastically different $T_1 >> T_2$.

3.3 Main results

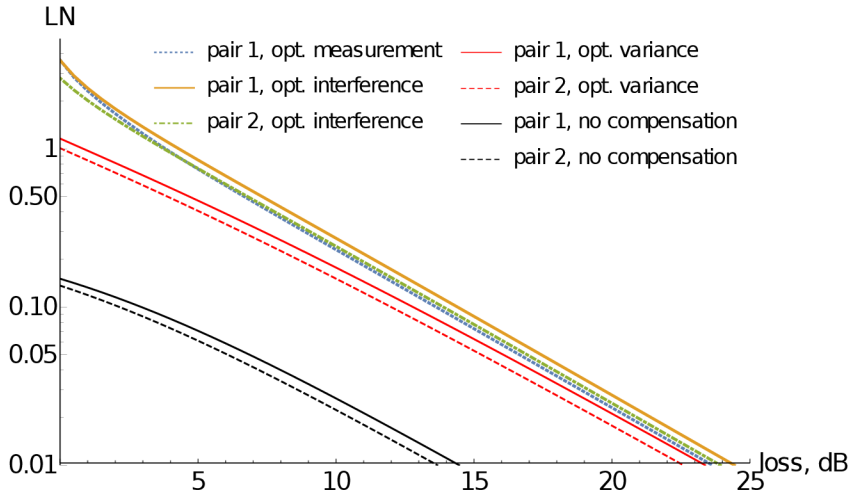

Figure 3.6: Comparing different ways of cross talk compensation: optical interference using a decoupling beam-splitter, and entanglement concentration by optimized conditional measurement and feed-forward control. Plot shows the logarithmic negativity in a pair of modes after each respective method is applied. Initial entanglement is fixed $LN_0 = 4.$, cross talk is $t_c = 0.8$, and transmittance ratio is $T_1/T_2 = 1.2$, parameters t_r and t_A are optimized. The ideal case without any cross talk is not shown, but would be indistinguishable from the optimized interference method for given parameters.

Comparison, how the entanglement in both pairs of modes restored by the different ways to compensate for cross talk, depending on the channel attenuation is given in Fig. 3.7. The passive method that implies the initial state variance optimization is the easiest to implement, it gives comparable results to the active methods, but only for high attenuation, it also does depend on the knowledge of the cross talk coupling t_c. The active compensation schemes always perform better, in particular the optimal interference, in case of its ideal implementation, beats all the other methods. The optimal interference also preserves all the modes intact, while relying on the correct choice of the parameter t_r, which can be challenging. While the measurement with the feed forward control halves the number of modes successfully distributed, but can be implemented without any knowledge of the strength of the cross talk t_c. Depending on the applications this disadvantage can be crucial. In QKD, where the mutual information in the pairs of modes is additive, the entanglement concentration method that traces out one of the mode pairs does not help to increase the key rate, but only deteriorates it further (except for the case

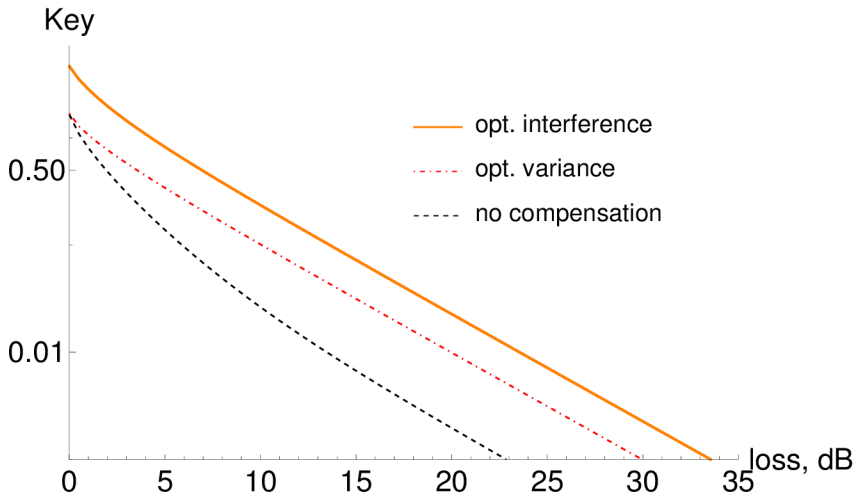

Figure 3.7: Different ways of cross talk compensation influencing the secret key rate for total state. Initial entanglement is fixed $LN_0 = 4.0$, cross talk is $t_c = 0.8$, and transmittance ratio is $T_1/T_2 = 1.2$, t_r is optimized. The compensation method using optimal measurement with feed forward is not applicable for QKD.

of unrealistically strong cross talk). In Fig. 3.6 we demonstrate how the proposed optimal interference compensation method allows to restore the secret key rate in the multiplexed entanglement-based QKD scenario.

Summary. In the entanglement distribution scheme presence of the cross talk deteriorates entanglement and the secret key rate. Depending on channel parameters and cross talk strength the initial state variance could be optimized to maximize entanglement shared. The negative effects of cross talk can be at least partially compensated by either of two methods we suggest and compare here. Depending on the purpose of entanglement distribution, e.g. for entanglement-based QKD protocols, the physical implementation of the cross talk compensating schemes could be substituted with numerical data processing. In the following Chapter 4 we demonstrate applicability of numerical implementation of the optimal interference method to compensate the cross talk in the experimental source with significantly more modes.

4 | Compensating cross talk in frequency multiplexed entangled QKD source

In this Chapter we present the main results of the published paper (see [2] in Chapter 6), where we study a way to increase the performance of the entanglement based CV QKD protocol by mode-multiplexing of optical transmission channel in the frequency domain. We test the method on the experimental data, obtained using the SPOPO as a source of entangled states and the mode-discriminating homodyne detection. Using the experimental data we then model a multimode version of the entanglement-base CV QKD with homodyne detection shown in Fig 2.3. The cross talk between signal modes appears to be very strong, it deteriorates the secret key rate and negates benefits of multiplexing. We apply the multimode cross talk compensation method based on data manipulation, equivalent to linear state manipulations, similar to the optimized interference method suggested in Chapter 3. We evaluate security of resulting CV QKD protocol, confirming the efficiency of cross talk compensation.

4.1 Experimental source

We model an EB CV QKD protocol using data from the experiment [54] with SPOPO as a source of frequency multiplexed entanglement and mode-discriminating homodyne detection that distinguishes 16-frequency bands. The source of multimode entanglement used in the experiment is described in Fig.4.1. In the actual experiment all 16 modes are generated in a single beam, when we suggest the way to use it in the QKD protocol, we have to model situation where half of the frequency modes are measured by Alice and the other half are distributed to Bob.

To generate the entangled light, a synchronously pumped optical parametric oscillator (SPOPO) including a 2-mm-thick BiB_3O_6 (BiBO) crystal, which operates below the threshold, was employed. The main laser is a Ti-sapphire pulse laser, with pulse 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 LO for mode-discriminating homodyne detection. The pump laser for the SPOPO (centered at $\lambda_0/2$) is prepared by second-harmonic

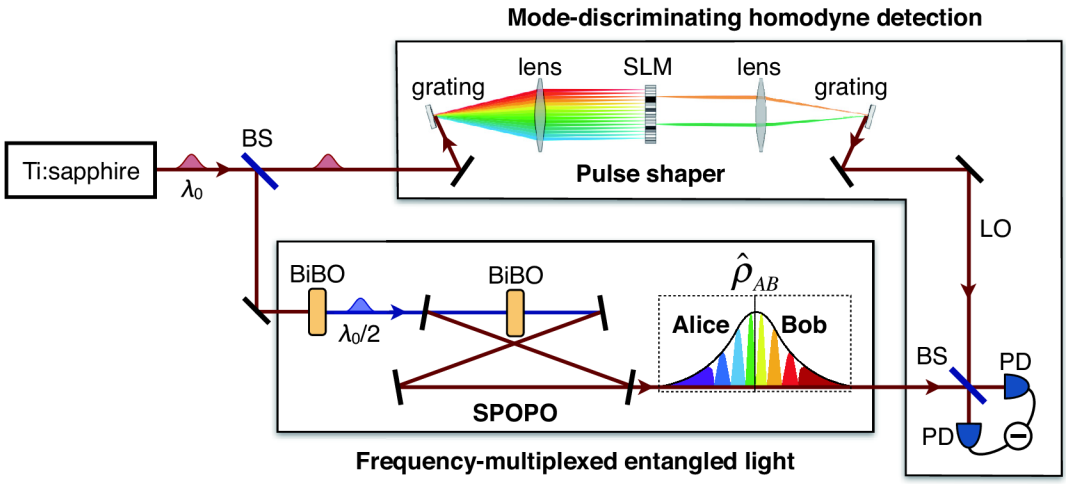

Figure 4.1: Experimental setup for generation of frequency-multiplexed multimode entangled light and its measurement with mode-discriminating homodyne detection. The pulse shaper is constructed in the folded configuration in actual implementation. BS: beam splitter; SLM: spatial light modulator; PD: photodiode.

generation of the main laser in a 0.2-mm-thick BiBO crystal.

4.2 QKD protocol

We consider a scenario, as shown in Fig. 4.2, where half of the modes (below the central frequency) is 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) through a pure loss channel. 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.

Optimized symplectic transformation we applied is equivalent to set of passive local operations on each side. The most general case would be a set of Mach-Zehnder interferometers acting on each possible combination of modes [135]. However, due to absence of the correlations between $\hat{x}$ and $\hat{p}$ quadratures no phase shifts can increase correlation (and, consequently, the mutual information) and a sequence of Mach-Zehnder interferometers simplifies to a sequence of beam-splitters between all possible pairwise mode permutations on each side.

The model of local passive symplectic transformation between modes introduces a set of beam-splitters on each side. In total there is $(N/2-1)N/2 = 56$ beam splitters (28 on Bob's and 28 on Alice's side), each beam-splitter in the sequence having transmittance coefficient t_{ij}, with the modes i, j interacting on the given beam-splitter. The joint

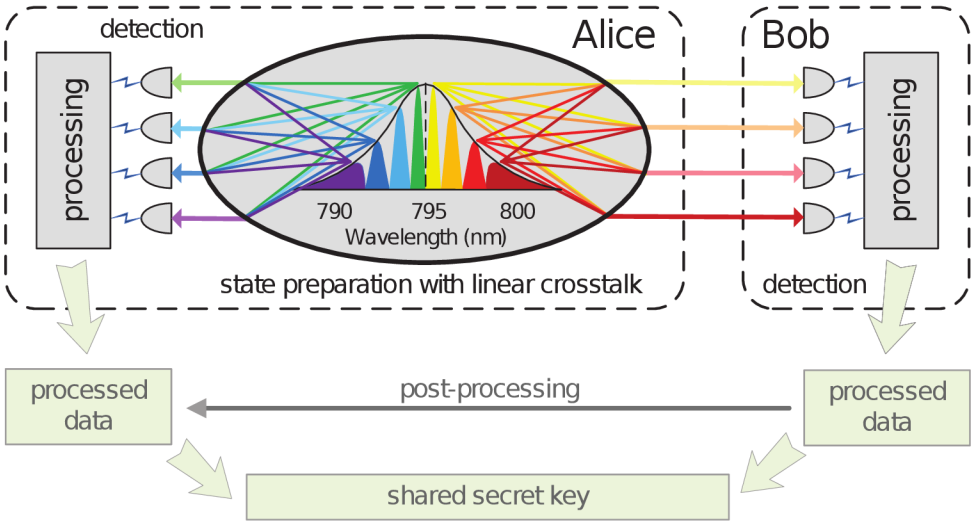

Figure 4.2: Bright colors show a sketch of a CV QKD test-bed for study of the multi-mode entangled source at the side of sender, Alice, with cross talk coupling between the frequency modes in both of the two beams, leaving the source. The entangled source is based on eight pairs of modes, here only four of them are shown for simplicity. The part of the CV-QKD protocol tested experimentally (as shown in Fig.4.1) is given in bright colors, while the part, that is modelled theoretically, is given in dim colors.

operation performed by Alice is

$$U_A = T_{7,8}T_{6,8}...T_{1,3}T_{1,2} = \prod_{i=1,j=i+1}^{8} T_{i,j}, \tag{4.1}$$

the operation Bob performs is

$$U_B = T_{15,16}T_{14,16}...T_{8,10}T_{8,9} = \prod_{i=9,j=i+1}^{16} T_{i,j}. \tag{4.2}$$

Their joint operation acts on the 16×16 covariance matrix γ of the state $\gamma_f = U_A U_B \gamma U_B^T U_A^T$. Symplectic unitary operation $U_A U_B$ is equivalent to a basis change and it cannot influence information that leaked to eavesdropper. Basis change does not influence symplectic eigenvalues in Eq. (2.14) and Holevo bound Eq.(2.30) on Eve's information remains unchanged. To maximize the key rate Eq.(2.32) it is therefore enough to maximize the mutual information. The mutual information between the sides is additive $I_{AB} = \sum_{i=1}^{8} I_{A_i B_i}$. Two functions we seek to maximize are mutual information values (calculated in each quadrature separately) $I_{x_{AB}}(\mathbf{t})$ and $I_{p_{AB}}(\mathbf{t})$, here $\mathbf{t} = (t_{1,2}, t_{2,3}...t_{15,16})$ is the variable vector made of transmittance coefficients of the beam splitters. They are maximized numerically with respect to vector $\mathbf{t}$ using limited memory Broyden–Fletcher–Goldfarb–Shannon (l-BGFS) optimization algorithm with bound constraints [136] and basin hopping. As the function $I_{AB}(\mathbf{t})$ is not convex, the l-BGFS method (even with basin hopping) doesn't guarantee that the maximum we found is a global one, but the results obtained show significant

increase in mutual information in both quadratures, more in $\hat{p}$ quadrature with increase from 0.28 to 0.517 bit per channel use. In the CV QKD protocol with homodyne detection only one quadrature can be chosen for the quantum key generation, we therefore consider $\hat{p}$ quadrature for the key.

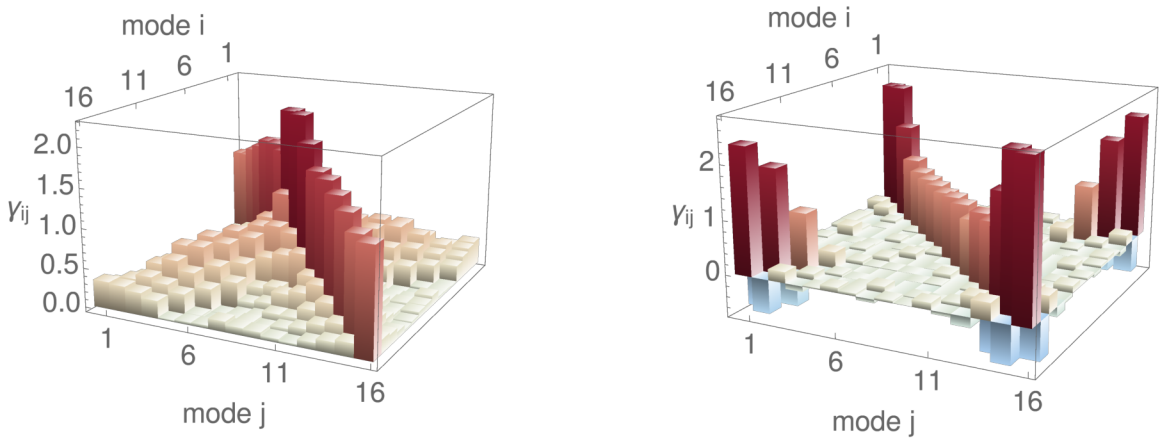

Figure 4.3: Visualization of covariance matrices in $\hat{p}$ quadrature before γ (left) and after γ_f (right) the optimized linear data processing.

The effect of optimal basis change on the covariance matrix is shown in Fig. 4.3.

4.3 Main results

We compare the secure key rate robustness to channel loss with the original experimental data and the data after optimal processing in Fig. 4.4. The optimized data manipulation has noticeably improved robustness to loss (and, respectively, increased the secure distance) of frequency-multiplexed CV QKD protocol, the tolerable loss increased from 7.5 dB before processing (blue) to 28 dB (orange). To show how multimode nature of the source increases the key rate we also calculated the key rates for reduced states with only some modes used for the key generation and extrapolated it to the cases with significantly larger numbers of modes (dashed lines). The extrapolation for a larger number of pairs was done with the method of the least squares [137], with linear model for the key rate in the form $K(x) = a + bx$ ($a = -0.0501$ 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 $t = 2.447$). Comparing the results for different number of modes and extrapolations suggests that increasing the number of frequency bands measured with mode-discriminating homodyne detection can further increase performance of the QKD protocol.

Summary. This work suggests SPOPO in prospect can be a useful source for implementation of frequency multiplexed entanglement-based CV QKD protocols. During

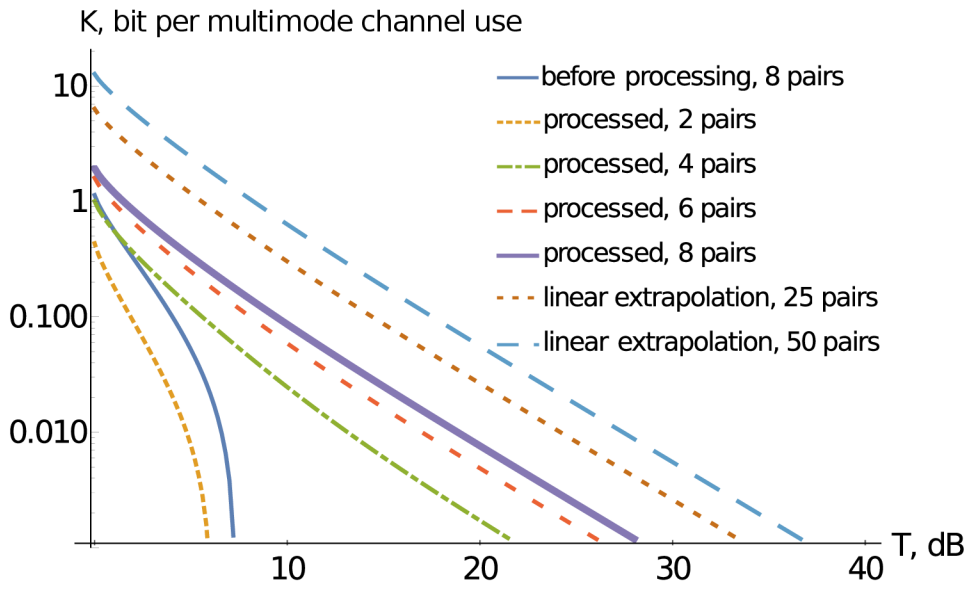

Figure 4.4: Key rate of CV QKD versus channel transmittance T (in dB) as obtained from the original data on the full multimode entangled state (blue solid line), after optimized local data manipulations performed by the trusted parties for different number of used pairs of modes (non-solid lines for 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 $\beta = 96\%$.

generation and measurement this source suffers from cross talk between different frequency modes that can be compensated by optimally applying data manipulations in the postprocessing stage of the protocol. The optimal data processing allowed to increase the mutual information between the sets of modes on both sides, while the leaked information is not affected. We observed increase of protocol robustness to channel attenuation from about 7.5 dB to 28 dB.

5 | QKD with macroscopically bright coherent states of light

Besides channel multiplexing, when each mode carriers signal individually and has to be measured individually, multimode states can be used even in quantum communication scenarios without mode-discriminating measurement. E.g. bright squeezed vacuum states (BSV) containing multiple squeezed modes can be treated in an experiment as single-mode states of higher intensity. The possibility to implement entanglement-based QKD protocol with BSV was proposed earlier [62]. Here we present the main results of the published paper (see [3] in Chapter 6) that considers a prepare-and-measure CV QKD protocol with bright coherent states, based on the results of the experimental test of their generation and detection. Bright states are called so in the sense that they consist of multiple modes, making them easier to handle in practical QKD implementations. The downside of having multiple signal modes is that not all of them overlap successfully with the local oscillator during the homodyne measurement, hence creating additional noise. This paper tests the possibility to reduce the resulting noise and estimates the applicability of the bright nonclassical states for CV QKD.

5.1 Experiment

In regular homodyne detection in Fig. 5.1 (left) single-mode signal beam is mixed with single-mode local oscillator on the balanced beam-splitter, while in homodyne detection of bright states it is necessary to mix all modes of the signal state with the multi-mode local oscillator. In case the mode matching is imperfect, some signal modes do not match with the local oscillator modes, these unmatched modes mix with vacuum on the beam-splitter, adding extra noise to measurement results [62]. In Fig. (5.1 (right) we show the case with only two signal modes, one of which does not overlap with the local oscillator.

The measured quadrature variance gains extra noise from the unmatched modes registered by the detector, variance of quadrature $\hat{x}$ becomes

$$Var\,(x)_{meas} = Var(x) + \varepsilon_{tot}^2 \overline{n}, \tag{5.1}$$

where $Var(x)$ is the quadrature variance of the matched signal modes (being $Var(x) = 1$ for pure coherent states), $\overline{n}$ is the mean number of photons in an unmatched signal mode

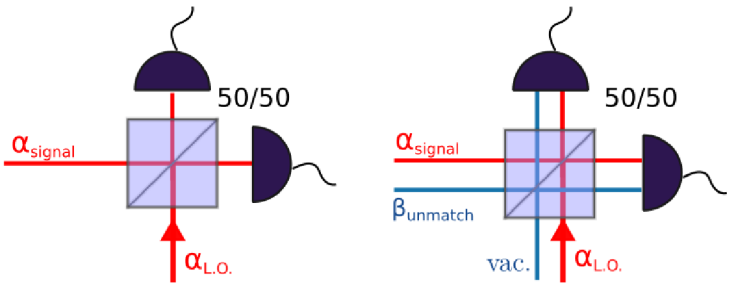

Figure 5.1: The standard scheme for homodyne detection (left) and the scheme with uncompensated modes in the multimode signal beam (right).

and

$$\varepsilon_{tot}^2 \equiv \frac{N\varepsilon^2}{M\left|\alpha_{LO}\right|^2}, \tag{5.2}$$

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. In the experiment and the QKD protocol model described bellow $\varepsilon = 1$ everywhere.

In the experiment homodyne detection was performed on coherent states. Let's name the matched mode $|\alpha\rangle$ and the unmatched one $|\zeta\rangle$ so that Eq. (5.1) becomes

$$Var\left(x\right)_{meas} = 1 + \frac{|\zeta|^2}{|\alpha_{LO}|^2}, \tag{5.3}$$

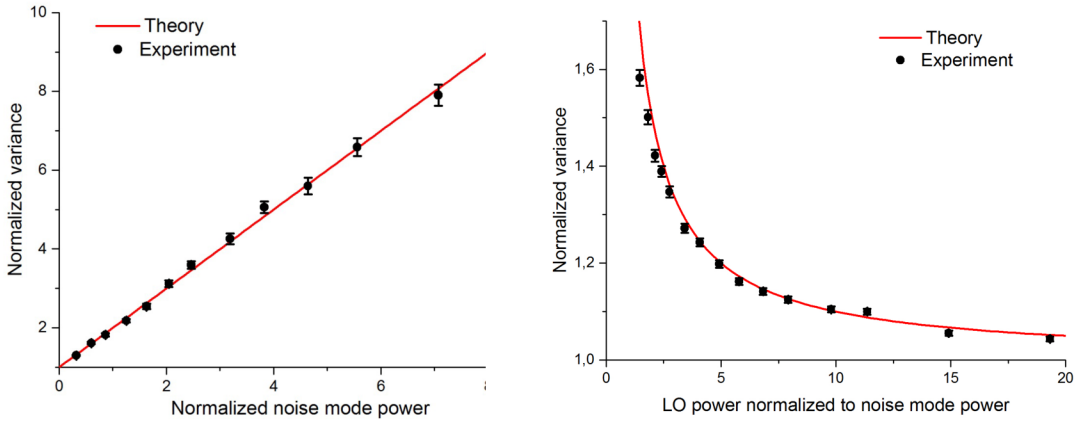

Figure 5.2: Measured normalized variance in shot-noise units as a function of the normalized photon number in the unmatched mode (left) and in the local oscillator (right). The mean photon number in a signal mode of BSV is 10^5

The results of the experimental test is given in Fig. 5.2, the variance measured has linear dependence on the photon number in the unmatched mode and inverse dependence on the mean photon number in local oscillator. By increasing the local oscillator intensity ten times the additional noise is reduced from 1.6 SNU to 0.16 SNU, which well matches the theory.

5.2 Bright coherent-state QKD protocol

Based on the experimental data, we consider a coherent state prepare-and-measure protocol described in Fig.5.3. Coherent-state protocols differ from entanglement-based ones described in the Section 2.3 only in the ways Alice prepares the state by displacing a coherent state in the phase space. We assume that Alice possesses a source of the multimode

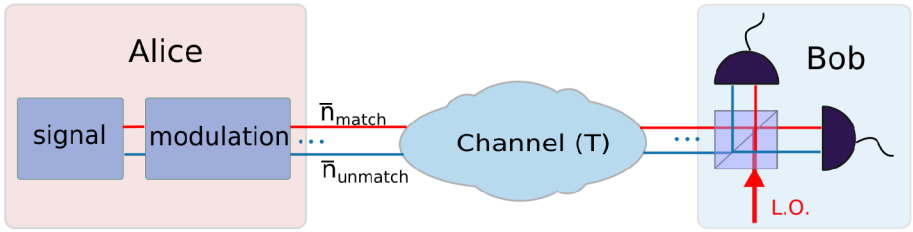

Figure 5.3: Operational scheme of prepare-and-measure CV QKD protocol using bright coherent states. Alice prepares bright coherent states and applies Gaussian modulation to them. She sends them (and local oscillator) through the attenuating quantum channel to Bob, who measures the signal with homodyne detection. The detection is assumed to be imperfect.

bright coherent light and applies Gaussian modulation to a signal preparing the thermal state. Initially Alice posses a bright coherent state with covariance matrix $\gamma^B_{coh} = \mathbb{I}$. After Alice applies modulation according to random variables she draws from two Gaussian distributions with zero mean, the covariance matrix of the state becomes that of a thermal state:

$$\gamma^B_{coh} = \begin{pmatrix} V^x_m + 1 & 0 \\ 0 & V^p_m + 1 \end{pmatrix}. \tag{5.4}$$

The signal then travels through a quantum channel to a remote party Bob, who measures one of the signal quadratures with homodyne detection. The variance of the modulation has to be optimized depending on the channel parameters, attenuation T and excess noise V_N, here both optimal modulations are equal and we redefine the variance as $V^x_m + 1 = V^p_m + 1 = V$. The security proof for this protocol relies on the proof for an equivalent entanglement-based protocol described in the Section 2.3. The covariance matrix of the state shared through a channel for the the equivalent protocol is

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & \left[T(V+V_N)+1-T+\varepsilon^2_{tot}\overline{n}\right]\mathbb{I} \end{pmatrix}, \tag{5.5}$$

The secret key rate is calculated from the covariance matrix γ_{AB} using Eq. 2.32. The presence of unmatched modes brings extra noise to the results of Bob's homodyne measurement. The security proof assumes that the eavesdropper purifies the state, forcing to attribute any noise to the eavesdropper's interference and lowering the secure key rate.

5.3 Main results

In the prepare-and-measure protocol while Alice applies the Gaussian modulation to bright coherent states, she can either successfully displace in the phase space all the modes present, so that all the unmatched modes will arrive to Bob's detector in thermal state, or else displacement can happen to only to some of them, the unmodulated modes then will stay in coherent state. In the first scenario both number of unmatched modes and their mean photon number $\overline{n} = V_m/2$, in the second scenario all the modes that arrived to Bob's detector can be effectively treated as a single bright mode with a higher average photon number. In practice some combination of the scenarios will appear. These scenarios are different in the experimental implementation (the failure to successfully match modulated modes brings more noise to the measurement), but in this theoretical model we only deal with total unmatched photon number $N\overline{n}$.

The asymptotic secure key rate versus increase in LO brightness for different channel transmittance is given in the left panel of Fig. 5.4. The key rate grows with the larger LO photon number, the maximal key rated is obtained with the maximum LO brightness of 10^6 photons reached in the experiment. In practice it is impossible to indefinitely rise LO brightness due to detectors limitations, in the right panel of Fig. 5.4 the theoretical prediction of the key rate vs mean photon number in unmatched modes is given for different fixed LO mean photon numbers for a mid-range 3 dB channel is plotted, showing how the key rate is destroyed by the noise the unmatched modes create.

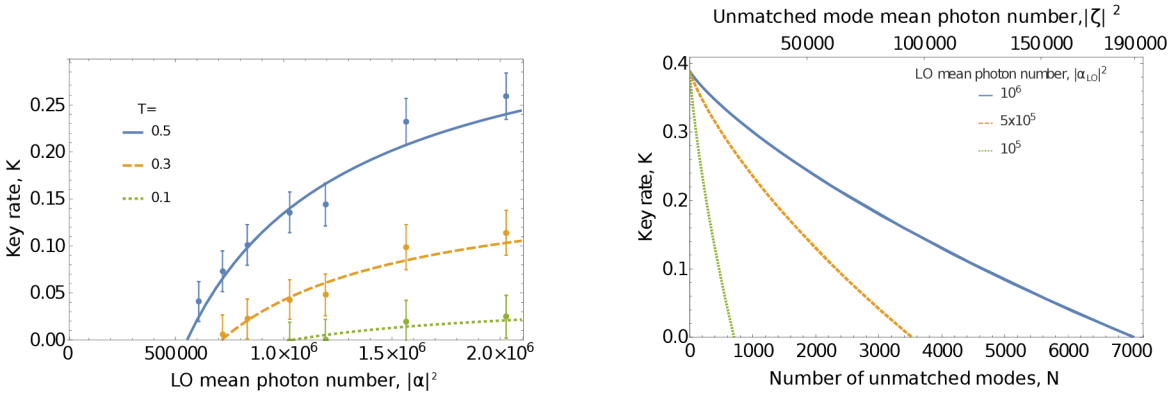

Figure 5.4: Left: the key rate for multimode coherent-state CV QKD in the presence of mode mismatch versus the LO brightness at different values of the channel transmittance T, obtained from the experimentally measured noise (points with error bars) and from the calculated quadrature variance (5.1), $N/M = 1$ (lines). Right: the key rate for multimode coherent-state CV QKD in the presence of mode mismatch (theoretically evaluated using (5.1) for the given parameters) versus the unmatched mode brightness, $|\zeta|^2$, 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 brightness is varied, $T = 0.5$. In both plots, the modulation variance is optimized, $\beta = 0.96$ and $\epsilon^2 = 1$ as confirmed in the experiment.

Summary. Presence of bright unmatched modes can undermine the security of coherent-state CV QKD with multimode states by leading to the excess noise in homodyne measurement results, which has to be assumed untrusted. The proof-of principle experiment demonstrated that this noise can be suppressed by increase of the power of the local oscillator. Further we used experimental parameters to model a prepare and measure CV QKD protocol using multimode coherent states showing the possibility to perform CV QKD with bright states using optimal modulation and proper mode matching.

6 | Publications

The following chapter contains copies of publications prepared and published/submitted during PhD studies. The author contributions are stated for each work, and can be found prior to respective publication copy.

Cross talk compensation in multimode continuous-variable entanglement distribution

Olena Kovalenko, Vladyslav C. Usenko, and Radim Filip

Published: *Optics Express* Vol. 29, Issue 15, pp. 24083-24101 (2021)

Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic

Following is an exact copy of the published article.

Cross talk compensation in multimode continuous-variable entanglement distribution

OLENA KOVALENKO,[1,*] VLADYSLAV C. USENKO,[1] AND RADIM FILIP[1]

[1] *Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*
[*] *kovalenko@optics.upol.cz*

Abstract: Two-mode squeezed states are scalable and robust entanglement resources for continuous-variable and hybrid quantum information protocols at a distance. We consider the effect of a linear cross talk in the multimode distribution of two-mode squeezed states propagating through parallel similar channels. First, to reduce degradation of the distributed Gaussian entanglement, we show that the initial two-mode squeezing entering the channel should be optimized already in the presence of a small cross talk. Second, we suggest simultaneous optimization of relative phase between the modes and their linear coupling on a receiver side prior to the use of entanglement, which can fully compensate the cross talk once the channel transmittance is the same for all the modes. For the realistic channels with similar transmittance values for either of the modes, the cross talk can be still largely compensated. This method relying on the mode interference overcomes an alternative method of entanglement localization in one pair of modes using measurement on another pair and feed-forward control. Our theoretical results pave the way to more efficient use of multimode continuous-variable photonic entanglement in scalable quantum networks with cross talk.

1. Introduction

Photonic quantum entanglement [1] is not only a puzzling physical phenomenon, but as well a resource for quantum information processing and quantum communication tasks, in particular for quantum key distribution (QKD) [2, 3], quantum metrology [4] or quantum computing [5]. Continuous-variable (CV) entanglement, using generally multiphoton states of light, has experimentally enabled quantum communication and information processing with large information capacity [6–14]. It can be quantified using logarithmic negativity (LN) [15], being a measure of negativity of a state's partial transpose [16, 17]. Advantageously, CV entanglement can be deterministically generated reaching two-mode squeezing bellow $-10dB$ (corresponds to logarithmic negativity up to $LN = 4.3$) [18]. In CV quantum communication, one of the possible ways to simultaneously transfer many entangled states during the same period of time is to use frequency or spatial multiplexing of quantum states residing in different modes [19–22]. Such an approach was in particular used to improve quantum communication with multiplexed QKD [23] or with multiplexed quantum teleportation using frequency pulse modes [24]. The techniques for preparation and detection of multimode quantum states of light were drastically improved in the past years, which enabled generation of highly multimode frequency comb states [25, 26] with the focus on quantum networks [27, 28] or cluster states, which are multiplexed in the time domain [29–32].

In a massive mode multiplexing, it is challenging to avoid cross talk between the modes during preparation and distribution [33–35], which can reduce or even destroy logarithmic negativity of entangled pairs and undermine applicability of shared entanglement. It was, in particular, shown that cross talk effects in the multimode homodyne detection can undermine security of mode-non-discriminating CV QKD [36–38]. However, the cross talk already in the state preparation before the distribution may substantially influence also other entanglement-based protocols, especially, if they are implemented over attenuating (lossy) channels [26, 27].

In the current paper, we theoretically study the role of linear cross talk between the signal modes on the state preparation side in distribution of multimode CV entangled states of light through an imperfect (lossy and noisy) channel (differently from the recent study of cross talk from the co-propagating classical signals in multimode CV QKD [39]). We consider Gaussian bipartite two-mode squeezed vacuum states (TMSV) [40], also known as twin beams, and show that even a small cross talk substantially degrades Gaussian entanglement contained in the mode pairs and makes the states more sensitive to excess noise in quantum channels used for entanglement distribution. Importantly, amount of initial two-mode squeezing should be optimally adjusted to maximize its transmission in the presence of cross talk. To overcome this basic passive method, we suggest active control of phase between the modes and controllable linear coupling of the output modes prior to their use on a remote side in order to compensate the cross talk, inspired by the method used to remove correlations in quantum memory channels [41] and in the squeezed state generation [42]. We show that such an active method, if used optimally, can completely eliminate the negative effect of cross talk once the noiseless channel transmittance is the same for all the modes. For a realistic case of asymmetrical quantum channels with slightly different transmittance for different modes, the cross talk can be still largely compensated for. To demonstrate the advantage we compare our method of active cross talk elimination to a deterministic entanglement localization scheme [43, 44] using homodyne detection on one pair of modes and feed-forward control on another pair. We show that the active scheme provides better results in a wide range of realistic parameters, particularly, at relatively small cross talk and similar channel transmittance values for different modes, while remarkably preserving multimode structure of the signal. We also address stability of our method and show that it is robust against deviations of the linear coupling used to compensate the cross talk.

2. Effect of cross talk on multimode continuous-variable entanglement distribution

We consider multimode entangled idler and multimode entangled signal beams constituting TMSV emitted by a source [40]. Such states are entangled so that quadratures $\hat{x} = \hat{a}^\dagger + \hat{a}$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, defined for a given mode, are strongly respectively correlated and anti-correlated within a pair of modes belonging to the signal and the idler beams. To verify the entanglement, a sender (Alice) is performing homodyne quadrature measurement on each of the modes of a respective beam (e.g., signal) and a receiver (Bob) is measuring quadratures of each of many modes of another twin beam (e.g, idler) using another homodyne detector, after the modes experience cross talk and travel through generally attenuating and noisy quantum channels. In the relevant experimental examples [26, 27, 45] the crosstalk appears already in the source prior to the lossy and noisy channel.

We assume the most common linear cross talk between two neighbouring modes, which can be represented by a beamsplitter coupling t_c between the modes, as it is schematically shown in Fig. 1. Changing t_c from 0 to 1 then means a transition from very strong inter-mode coupling (hence strong cross talk) to the absence of cross talk. Here we analyse weak nearest-neighbour coupling, although in general case multimode coupling is more complex, the model allows us to obtain necessary conditions for improvement to further numerically apply these methods to a more complex multiple mode cross talk. We parametrize the quantum channel with transmittance T_i for a given i-th mode and with the amount of phase-insensitive excess noise ε added to the quadrature variance, which is assumed (and typically is) the same for all the modes. Excess noise in general depends on properties of the channel , but can be also concerned with unaccounted detection noise or imperfect state generation. For the fiber channels the observed excess noise is typically below 1 % shot noise unit (SNU), being the level of vacuum quadrature fluctuations, at the channel output [46, 47]. We first analyse the role of cross talk in a basic case of two entangled mode pairs (so that the overall number of modes in signal and idler beams is four), then extend

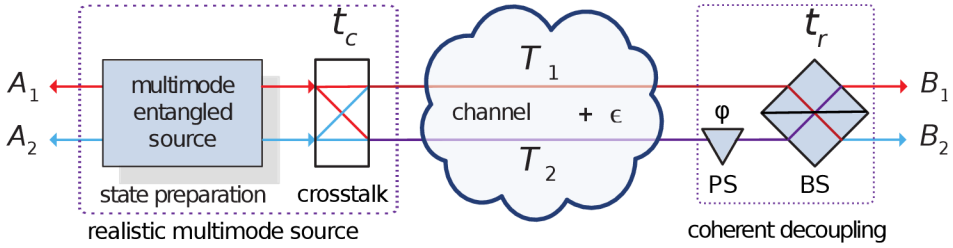

Fig. 1. Four-mode CV entanglement distribution scheme in the presence of cross talk characterized by the linear coupling t_c between the signal modes, performed over lossy and noisy channels with transmittance T_i for an i-th mode and with channel excess noise ε added to all the modes. In order to decouple the entangled modes after the channel, we use optical interference, when the remote side optimally applies variable relative phase shift (PS) φ between the modes to one of the modes and couples the B_1 and B_2 modes on a variable beam-splitter (BS) type of interaction with transmittance t_r. We maximize entanglement in pairs of modes A_1, B_1 and A_2, B_2 over BS transmittance t_r and phase φ.

the results to three pairs.

We describe the Gaussian multimode TMSV states [40] by covariance matrices with elements $\gamma_{ij} = \langle r_i r_j \rangle$, where $r_i = \{x_i, p_j\}$ is a set of quadratures of a given i-th mode, taking into account their zero mean values, $i \in [1, 2N]$, here $2N$ is the overall number of modes (hence, N is the number of mode pairs, or, equivalently, the number of modes in each signal and idler beams). Then the system of four pairwise perfectly entangled modes $A_{\{1,2\}}, B_{\{1,2\}}$, shown in Fig. 1, each having quadrature variance $V \geq 1$, is described by the 8x8 covariance matrix of the form

$$\gamma_{A_1A_2B_1B_2} = \begin{pmatrix} V\,\mathbb{I} & \sqrt{V^2-1}\,\mathbb{Z} & 0 & 0 \\ \sqrt{V^2-1}\,\mathbb{Z} & V\,\mathbb{I} & 0 & 0 \\ 0 & 0 & V\,\mathbb{I} & \sqrt{V^2-1}\,\mathbb{Z} \\ 0 & 0 & \sqrt{V^2-1}\,\mathbb{Z} & V\,\mathbb{I} \end{pmatrix}. \tag{1}$$

Here $\mathbb{I} = diag[1, 1]$ is the unity matrix, $\mathbb{Z} = diag[1, -1]$ is a Pauli matrix. Quadrature variance V is related to the squeezing parameter r of TMSV, which defines the amount of two-mode squeezing applied to the two-mode vacuum in both quadratures $\mathrm{Var}[(x_{A_i} + x_{B_i})/\sqrt{2}] = e^{-2r}$ and $\mathrm{Var}[(p_{A_i} - p_{B_i})/\sqrt{2}] = e^{-2r}$, and $V = \cosh(2r)$, so that the larger r, the stronger is quadrature correlations between the modes, given by $\langle (x_{A_i} + x_{B_i})(p_{A_i} - p_{B_i}) \rangle = \sinh r$. After a linear cross talk t_c and lossy and noisy quantum channel, the covariance matrix changes to

$$\gamma_{A_1A_2B_1B_2} = \begin{pmatrix} V\,\mathbb{I} & \sqrt{t_c\,T_1}\sqrt{V^2-1}\,\mathbb{Z} & 0 & -\sqrt{r_c\,T_2}\sqrt{V^2-1}\,\mathbb{Z} \\ \sqrt{t_c\,T_1}\sqrt{V^2-1}\,\mathbb{Z} & [T_1(V+\varepsilon-1)+1]\,\mathbb{I} & \sqrt{r_c\,T_2}\sqrt{V^2-1}\,\mathbb{Z} & 0 \\ 0 & \sqrt{r_c\,T_1}\sqrt{V^2-1}\,\mathbb{Z} & V\,\mathbb{I} & \sqrt{t_c\,T_2}\sqrt{V^2-1}\,\mathbb{Z} \\ -\sqrt{r_c\,T_1}\sqrt{V^2-1}\,\mathbb{Z} & 0 & \sqrt{t_c\,T_2}\sqrt{V^2-1}\,\mathbb{Z} & [T_2(V+\varepsilon-1)+1]\,\mathbb{I} \end{pmatrix} \tag{2}$$

Here $r_c \equiv 1 - t_c$. We characterize the bipartite Gaussian entanglement using LN [15] of a state ρ is defined as

$$LN(\rho) = -\log_2 ||\rho^\Gamma||_1, \tag{3}$$

where ρ^Γ is a partial transpose of ρ, $||\rho||_1$ is the trace norm of the operator ρ, that is equal to the sum of the absolute values of the negative eigenvalues of ρ^Γ, quantifying the degree to which a partially transposed state fails to be positive [16, 17]. For a Gaussian states with covariance matrix γ the eq. (3) becomes the sum of all symplectic eigenvalues of the partially transposed that are less than one: $LN(\gamma) = \sum_k \max\{0, -\log_2 \nu_k\}$. For the TMSV states with the symplectic eigenvalues $\{\nu_+, \nu_-\}$ the larger eigenvalue is $\nu_+ \geqslant 1$ [48]. This way the LN of the i-th pair of

modes simplifies to

$$LN_i = \max\{0, -\log_2 \nu_{i-}\}, \tag{4}$$

where ν_- is the smallest symplectic eigenvalue of the covariance matrix of the partially transposed state of either the first or the second pair. We limit our study to the Gaussian TMSV states as the typical case of bipartite quadrature-entangled states of light. As the task is to deterministically transmit all pairs through the channel, we evaluate logarithmic negativity for each pair of modes separately. We also define the *initial logarithmic negativity* of a TMSV state (1), before the cross talk and before sharing the state over a noisy and lossy channel, see Fig.1, as

$$LN_0(V) = -\frac{1}{2}\log_2\left(2V^2 - 1 - 2V\sqrt{V^2-1}\right), \tag{5}$$

which is the same for the both pairs of modes. It represents the maximum of Gaussian entanglement in the pairs of modes, which can be shared in the perfect case of no cross talk and ideal (lossless and noiseless) channels. In the limit of small state variance ($V \to 1$), it behaves as $LN_0 \sim \frac{1}{\log 2}\sqrt{2(V-1)}$. In the limit of large $V \to \infty$, $LN_0 \sim \log_2(2V)$.

In the absence of cross talk ($t_c = 1$) the logarithmic negativity monotonously grows with increasing TMSV quadrature variance V, but its limit depends on the channel parameters as

$$\lim_{V\to\infty} LN = -\log_2 \frac{1 - T_i(1-\varepsilon)}{1+T_i} \tag{6}$$

For noiseless channels ($\varepsilon = 0$) the entaglement never vanishes for any $T_i > 0$. For lossless channels ($T_i = 1$) entanglement is lost at $\varepsilon > 2$. In the presence of cross talk between the signal modes and after a lossy and noisy channel, as shown in Fig. 1, the logarithmic negativity becomes

$$LN = -\frac{1}{2}\log_2\frac{1}{2}\Big(1 + 2T_i[\varepsilon + (V-1)(t_c V + t_c + 1)] + T_i^2(\varepsilon + V - 1)^2 + V^2 - \\ [1 + V + T_i(\varepsilon + V - 1)]\sqrt{T_i^2(\varepsilon + V - 1)^2 + (V-1)^2 - 2T_i(V-1)[\varepsilon - 2t_c(V+1) + V - 1]}\Big) \tag{7}$$

For channels with high loss ($T_i \ll 1$), expanding (7) around $T_i = 0$ gives

$$LN \approx \frac{T_i[2 - \varepsilon - (1-t_c)(V+1)]}{\log(2)}\left(1 + \frac{T_i}{2}[2 - \varepsilon - (1-t_c)(V+1)] - \frac{T_i t_c (V+1)}{V-1}\right) \tag{8}$$

For a very small transmittance, $T_i \to 0$, LN is well described by the first term in (8), $LN \sim \frac{T_i[2-\varepsilon-(1-t_c)(V+1)]}{\log(2)}$. In this limit, the shared entanglement has linear dependence on the transmittance T_i. Provided that the cross talk is absent ($t_c = 1$), the entanglement is independent on the initial variance V and is destroyed by the excess noise $\varepsilon = 2$. The presence of cross talk introduces a new term $-T_i(1-t_c)V$ that reduces the shared entanglement, which then monotonically decreases with the increase of V.

Beyond the limit of small initial entanglement ($V \to 1$), sensitivity of Gaussian entanglement of TMSV to cross talk can be seen in Fig. 2, left, where logarithmic negativity is plotted versus the initial entanglement at different cross talk coupling t_c values and compared to the case when the cross talk is absent ($t_c = 1$). It is numerically evident from (7) and from the plots in Fig. 2, left, that the amount of entanglement shared over the noiseless channel in the presence of cross talk becomes sensitive to the initial entanglement even for weak channel attenuation $T_i = 0.9$ and can be broken once the initial entanglement is too strong. This is concerned with the fact that due to cross talk the signal from an adjacent mode is coupled to the signal in another mode and thus effectively acts an uncorrelated noise appearing in one of the beams if all modes are treated independently. Amount of such a noise is larger for the higher state variance, i.e., for a larger

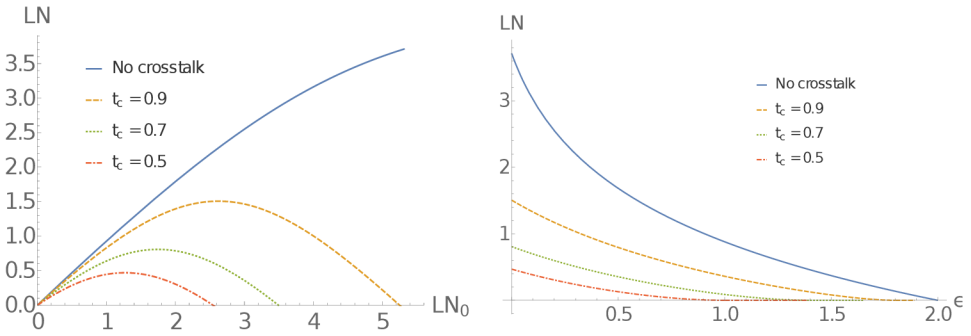

Fig. 2. Gaussian logarithmic negativity of the pair of modes A_1, B_1 after cross talk t_c and after passing through a quantum channel versus the initial logarithmic negativity of the state (left) and versus the channel noise (right). The channel transmittance for both the modes is $T_{1,2} = 0.9$. Left: no excess noise ($\varepsilon = 0$). Right: fixed state variance $V = 5$. Entanglement is evidently reduced and made more sensitive to the excess noise even by a small cross talk, and is destroyed completely by the excess noise reaching the threshold (9). The initial entanglement can be optimized as in (11) to reach the maximum shared entanglement.

initial entanglement. This destructive extra noise effect from the crosstalk is also dominant for channels with excess noise. Moreover, the presence of cross talk degrades robustness of the shared entanglement to the channel noise, as can be seen from Fig. 2, right. The shared entanglement is then destroyed by the level of noise, which is independent of the channel transmittance T_i (hence being valid for any $T_i > 0$), and is given by

$$\varepsilon_{max} = 1 + t_c - (1 - t_c)V. \tag{9}$$

Equivalently, the bound on the shared entanglement (variance V for which entanglement turns to 0) is the same for any $T_i > 0$, and it reads

$$V_{max} = \frac{1 + t_c - \varepsilon}{1 - t_c} \tag{10}$$

Importantly, the maximum tolerable initial variance given by V_{max} (or, equivalently, maximum tolerable initial entanglement) also does not depend on the channel transmittance and, for a purely attenuating channel, depends only on the cross talk coupling t_c. The necessary condition $V < V_{max}$ therefore simplifies optimization if the cross talk is present only in the source. Note that if the channel is present also before the crosstalk, optimization becomes more complex and involves the channel transmittance values, however, the limitation $V < V_{max}$ remains.

The above given results were obtained in the assumption that the cross talk occurs between two modes. In the case, when each of the multiple TMSV modes interacts with two neighbouring modes, i.e., the cross talk dominantly occurs between three modes, the equations (7, 10) hold up to the substitution $t_c \to t_c^2$, which leads to stronger sensitivity of the shared entanglement to the linear cross talk between the signal modes. In this case, V_{max} is even more limited and therefore less entanglement can be transmitted.

The shared entanglement, in the presence of cross talk, can be maximized by optimizing the initial entangled resource. The optimal state variance V, which maximizes the shared entanglement, reads

$$V_{opt} = \frac{(1 - t_c)(1 - T_i)(1 - T_i + \varepsilon T_i) + (T_i + 1)\sqrt{(1 - t_c)t_c T_i[4t_c - \varepsilon(2 - 2T_i + \varepsilon T_i)]}}{(1 - t_c)[1 + T_i(4t_c + T_i - 2)]} \tag{11}$$

By optimizing the initial TMSV variance as in (11) we both reduce the negative influence of the cross talk, and rise tolerance to the excess noise. The maximal tolerable level of excess noise then becomes $\varepsilon_{max} = 2t_c$ SNU.

For a small cross talk $t_c \to 1$ the optimal variance can be approximated as

$$V_{opt} \approx \frac{(1-T_i)(1-T_i+\varepsilon T_i)}{(1+T_i)^2} + \frac{\sqrt{(2-\varepsilon)T_i(2+\varepsilon T_i)}}{(1+T_i)\sqrt{1-t_c}}. \tag{12}$$

If we neglect the excess noise, the expression (12) simplifies to

$$V_{opt} \approx \left(\frac{1-T_i}{1+T_i}\right)^2 + \frac{2\sqrt{T_i}}{(1+T_i)\sqrt{1-t_c}}. \tag{13}$$

Putting $T_i = 1$ in (13) allows to easily demonstrate the existence of the upper bound on the optimal state variance $V_{opt}(T=1) = \frac{1}{\sqrt{1-t_c}}$. It illustrates the fact that for any cross talk, even without noise and attenuation, the maximal possible shared entanglement is rather limited. For a strongly attenuating channel ($T_i \to 0$) together with excess noise ε, the optimal variance V_{opt} is approximately

$$V_{opt} \approx 1 + \frac{\sqrt{2T_i t_c(2t_c-\varepsilon)}}{\sqrt{1-t_c}} - (4t_c-\varepsilon)T_i \tag{14}$$

which means that the optimal initial quadrature variance of TMSV is rather small (close to one) when channel is strongly attenuating even if the cross talk is small ($t_c \to 1$). Therefore, amount of entanglement, which can be shared over lossy channels in the presence of even small cross talk, is then strongly limited. Note, that (14) explicitly shows the condition on excess noise ε for the optimized V being $\varepsilon < 2t_c$ SNU.

For a channel with strong attenuation ($T_i \to 0$), the optimized entanglement can be then approximated as

$$LN(V_{opt}) \approx \frac{2T_i\left[t_c - \frac{\varepsilon}{2} - 2\sqrt{t_c(1-t_c)(t_c-\frac{\varepsilon}{2})T_i} + [3t_c(1-t_c) + \frac{\varepsilon}{2}(1-\frac{\varepsilon}{2})]T_i\right]}{\log(2)} \tag{15}$$

or, in the absence of excess noise,

$$LN(V_{opt}) \approx \frac{2t_c T_i\left(1 - 2\sqrt{(1-t_c)T_i} + 3(1-t_c)T_i\right)}{\log(2)}. \tag{16}$$

In the limit of a very small cross talk ($t_c > 0.98$) for relatively strong excess noise ($\varepsilon > 0.2$ SNU) it is possible to find better approximation expanding optimized entanglement $LN(V_{opt})$ into series for a very low cross talk ($t_c \sim 1$) in the the limit of strongly attenuating channel ($T_i \to 0$), then the optimized entanglement can be better analytically approximated as

$$LN(V_{opt}) \approx -\log_2\left(\frac{1-T_i+\varepsilon T_i}{1+T_i}\right) - \frac{2T_i\sqrt{(2-\varepsilon)T_i(2+\varepsilon T_i)}}{(1+T_i)(1-T_i+\varepsilon T_i)\log(2)}\sqrt{1-t_c} \tag{17}$$

Figs. 2 – 3 illustrate that although optimization of the state variance during the state preparation helps to somewhat mitigate the negative effects of cross talk (allowing to reach maximal logarithmic negativity for given cross talk and excess noise that corresponds to the maximums in Fig. 2), nevertheless such optimization fails to fully compensate for the cross cross talk especially in the presence of a stronger excess noise. Comparison of the left and the right panel in the Fig. 3 and the eqs. (15-17) show that in the strongly attenuating channel while for a weak cross talk logarithmic negativity decreases as $LN \sim -\sqrt{1-t_c}$ (eq. (15) and dashed lines), very soon it gets

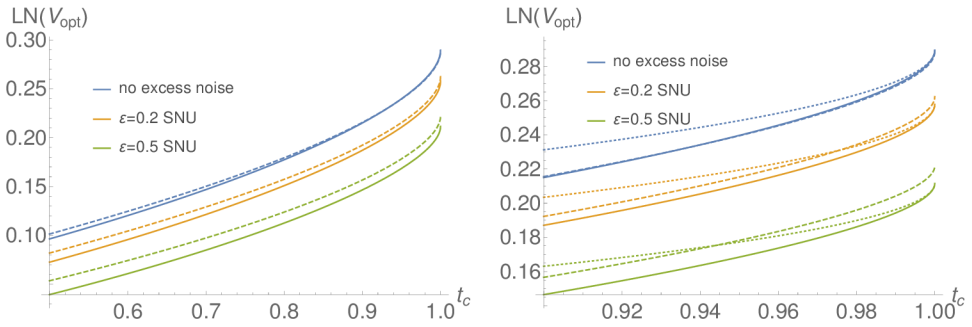

Fig. 3. Optimized logarithmic negativity in one pair of modes versus cross-talk coupling t_c after passing through the attenuating channel of transmittance $T_i = 0.1$ for different levels of excess noise. The initial variance of the state is optimized. Solid lines correspond to the exact results, dashed lines – to the approximation (15), dotted lines – to the approximation (17). Entanglement is reduced by cross-talk quite strongly even when the state is optimized before sharing.

suppressed more by higher orders of t_c (eq. (15-17) and dotted lines). Thus, even though initial entanglement can be optimized to achieve the maximum shared entanglement in the presence of cross talk, the shared entanglement will be still largely reduced by the cross talk, especially if combined with the channel loss and/or noise.

We therefore consider the local active manipulations on either sender or receiver side in order to improve and possibly fully restore the shared entanglement by compensating the cross talk. If the mode coupling happens only in the source during the state preparation, it can be compensated by manipulating either the modes A_1 and A_2, or B_1 and B_2 on the sender side or the modes B_1 and B_2 on the remote side after the states are shared through an imperfect channel. If an additional mode coupling also happens in the channel, manipulations on the receiver side are needed in addition to the manipulations at the sender side in order to simultaneously compensate both cross talk in the state preparation and in the channel. Generally both, the cross talk and the losses, can occur on both sender and receiver side and also in the source itself during the state preparation and distribution. In our study we assume that the shared part of the states (hence, modes B_1 and B_2) is the subject to cross talk. We then consider the manipulations on the receiver side, i.e., after the imperfect channel, in order to compensate the cross talk. The case of an ideal cross talk compensation on the sender side would be equivalent to the absence of cross talk, as can be seen in the next section.

3. Cross talk compensation by optical interference

We consider the feasible state operations prior to using the entangled states in order to compensate the cross talk, i.e., to reduce or completely eliminate its negative effect on the entanglement distribution. Since the cross talk is typically caused by an energetically passive photon exchange between the signal modes, we consider the beam-splitter type interaction based on a variable coupling t_r between the signal modes. The compensating interaction can in principle be performed on either sender or receiver side. If no signal loss occurs on the sender side, it is sufficient to implement the beam-splitter with $t_r = t_c$ coupling the modes A_1 and A_2 at the sender. To take into account the effects caused by the lossy channels we further concentrate on the case where the compensation is implemented on the modes B_1 and B_2 by the remote party of the entanglement distribution scheme. In this case the beam splitter needs to be preceded by an optimal phase shift (in the case of linear cross talk between two modes it is given by π) on one of

the modes (e.g., mode 2), as shown in Fig. 1. Then for a pair A_1, B_1 the covariance matrix reads

$$\gamma_{A_1B_1} = \begin{pmatrix} V\,\mathbb{I} & \left(\sqrt{T_2 r_c r_r} + \sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\,\mathbb{Z} \\ \left(\sqrt{T_2 r_c r_r} + \sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\,\mathbb{Z} & \left[1 + T_1 t_r (V-1) + T_2 r_r (V-1)\right]\mathbb{I} \end{pmatrix}, \tag{18}$$

where $r_c \equiv 1 - t_c$, $r_r \equiv 1 - t_r$, and similarly for A_2, B_2 up to the replacement $T_1 \leftrightarrow T_2$. It follows from the expression (18), that for the perfectly balanced noiseless channels $T_1 = T_2 \equiv T$ putting $t_r = t_c$ turns the correlations into $\left(\sqrt{T_2 r_c r_r} + \sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1} = \left(\sqrt{T}(1-t_c) + \sqrt{T}t_c\right)\sqrt{V^2-1} = \sqrt{T}\sqrt{V^2-1}$ and the variances into $1 + T t_r (V-1) + T(1-t_r)(V-1) = 1 + T(V-1)$ so that the covariance matrix turns into the one without any cross talk:

$$\gamma_{A_1B_1} = \begin{pmatrix} V\,\mathbb{I} & \sqrt{T}\sqrt{V^2-1}\,\mathbb{Z} \\ \sqrt{T}\sqrt{V^2-1}\,\mathbb{Z} & \left[1 + T(V-1)\right]\mathbb{I} \end{pmatrix}, \tag{19}$$

similarly for A_2, B_2, which fully restores entanglement and other Gaussian characteristics, affected by the cross talk. This can be generalized to a pair of arbitrary pure two-mode states in modes A_1, A_2 and B_1, B_2, considered as the product of $\iint d^2\bar{\alpha} d^2\alpha\; P(\bar{\alpha}, \alpha) |\bar{\alpha}\rangle_{A1} |\alpha\rangle_{B1}$ and $\iint d^2\bar{\beta} d^2\beta\, P(\bar{\beta}, \beta) |\bar{\beta}\rangle_{A2} |\beta\rangle_{B2}$ in the coherent-state overcomplete basis. This overcomplete basis decomposing unity allows to straightforwardly calculate the result for any pure two-mode state in equally lossy channels. Indeed, if two coherent basis states $|\alpha\rangle_{B_1}$ and $|\beta\rangle_{B_2}$ experience a linear cross talk t_c and pass through the attenuating channels T_1 and T_2 and through the decoupling scheme with a phase shift and coupling t_c as shown in Fig. 1, disregarding normalization and general phase they are transformed as

$$|\alpha'\rangle_{B_1} = \left|\left(\sqrt{T_1 t_c t_r} + \sqrt{T_2 r_c r_r}\right)\alpha + \left(\sqrt{T_2 t_c r_r} - \sqrt{T_1 r_c t_r}\right)\beta\right\rangle_{B_1} \tag{20}$$

and

$$|\beta'\rangle_{B_2} = \left|\left(\sqrt{T_1 r_c r_r} + \sqrt{T_2 t_c t_r}\right)\beta + \left(\sqrt{T_2 r_c t_r} - \sqrt{T_1 t_c r_r}\right)\alpha\right\rangle_{B_2}. \tag{21}$$

Choosing $t_r = \frac{T_2 t_c}{T_2 t_c + T_1 r_c}$ the states change to

$$|\alpha''\rangle_{B_1} = \left|\frac{\sqrt{T_2 T_1}}{\sqrt{T_2 t_c + T_1 r_c}}\alpha\right\rangle_{B_1} \tag{22}$$

$$|\beta''\rangle_{B_2} = \left|\sqrt{T_2 t_c + T_1 r_c}\beta + \frac{(T_2 - T_1)\sqrt{t_c r_c}}{\sqrt{T_2 t_c + T_1 r_c}}\alpha\right\rangle_{B_2}. \tag{23}$$

We have therefore eliminated the contribution of the second mode B_2 to the first one B_1, but not vice versa. If, on the other hand, we chose $t_r = \frac{T_2 t_c}{T_2 t_c + T_1 r_c}$, the cross talk will be eliminated from the second mode, but not from the first one. It is easy to see, that if $T_1 = T_2 \equiv T$, (22) and (23) turn into $|\alpha''\rangle_{B_1} = \left|\sqrt{T}\alpha\right\rangle_{B_1}$ and $|\beta''\rangle_{B_2} = \left|\sqrt{T}\beta\right\rangle_{B_2}$ as it should be for two independent modes attenuated by a channel. Therefore for the perfectly balanced channels ($T_1 = T_2$) the cross talk is fully eliminated for a pair of arbitrary pure two-mode state.

When the channel transmittance values T_1, T_2 for modes B_1, B_2 are different, the cross talk cannot be fully compensated in both modes and entanglement cannot be fully restored in both transmitting channels. While transmittance values for different modes are typically similar in fiber channels [49], they can vary, e.g. for frequency modes in atmospheric channels [50]. We therefore consider the efficiency of the cross talk compensation in the unbalanced channels. In order to maximally reconstruct entanglement, one has to optimize the coupling t_r, as shown

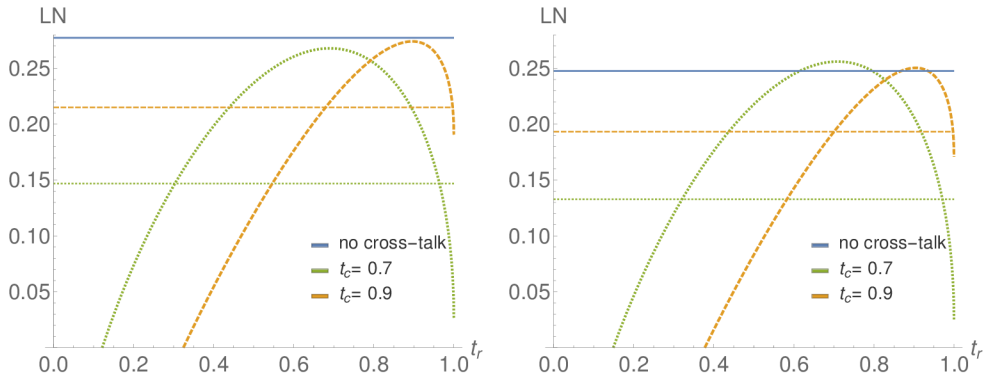

Fig. 4. Logarithmic negativity versus reverse coupling t_r aimed at compensating the cross talk after the unbalanced channels with the imbalance $T_1 = -10dB$ and $T_2 = -10.5dB$ of the first pair of modes (A_1B_1, left), the second pair (A_2B_2, right). The uppermost (blue) horizontal line shows the logarithmic negativity of the respective pair without the cross talk, the upper (orange) and the lower (green) curves show the result of applying compensating beam-splitter of transmittance t_r on Bobs's side at the same cross talk parameter t_c. Initial state variance is $V = 5$, no excess noise ($\varepsilon = 0$). The dotted horizontal lines (orange and green) correspond to the logarithmic negativity without the cross talk compensation but with the initial entanglement optimization.

in Fig. 4. It is evident from the plots, that entanglement can still be largely compensated for weaker crosstalk ($t_c \to 1$) between asymmetrical lossy channels and that the method of optical interference is stable to the setting t_r. There is a difference between the optimal t_r for the first pair and for the second one (it corresponds to the maximums of the curves on the left and right plots in Fig. 4), although, as it noticeable from the plots, their maximums are very close. In the second pair A_2B_2 we even can overcome the entanglement before the cross talk because we get stronger signal in the pair A_2B_2 that is taken from the pair A_1B_1 due to the cross talk.

In a general case, t_r should be optimized numerically to result in the maximally restored entanglement. However, the optimal setting can be derived analytically in the relevant limits of small and large initial entanglement (or, equivalently, small and high large initial state variance V). For a purely lossy channel ($\varepsilon = 0$), the optimal transmittance, that maximizes the entanglement in the first pair of modes A_1B_1, reads

$$t_r = \frac{T_1 t_c}{T_1 t_c + T_2(1 - t_c)}, \quad V \approx 1 \tag{24}$$

and

$$t_r = \frac{T_2 t_c}{T_2 t_c + T_1(1 - t_c)}, \quad V \to \infty \tag{25}$$

And vice versa ($T_1 \leftrightarrow T_2$) for another pair. It is important to note that the optimal t_r for any value of the state variance V always lies between the bounds given by (24-25) and, for realistically close T_1 and T_2, this interval is quite narrow. For t_r defined by (25) the logarithmic negativity is an increasing function of V and for large initial state variance it approaches the limit:

$$\lim_{V\to\infty} LN_{t_r} = -\log_2\left[\frac{t_c T_2 + T_1(1 - t_c - T_2)}{t_c T_2 + T_1(1 - t_c + T_2)}\right]. \tag{26}$$

Note, that the above given equations (24-26) are applicable for maximization of the enanglement for the pair A_1, B_1. If, on the other hand, the goal is to maximize the logarithmic negativity in

the second pair A_2, B_2 , the same equations (24-26) can be applied with replacement $T_1 \leftrightarrow T_2$. This also implies, that in the case of unbalanced channels $T_1 \neq T_2$, the entanglement cannot be optimally restored in both modes. While applying the optical interference method to compensate the cross talk in the channels with different transmittance for each mode ($T_1 \neq T_2$), one has to chose one mode in which to maximize the entanglement at the expense of the rest of the modes. The equations (24-26) refer to the first pair of modes A_1B_1. However, since in practical situations strong unbalancing between transmittance values for different modes is unlikely, i.e. T_1 is typically close to T_2, optimal settings for t_r are also close and choosing t_r in between the optimal settings for either of the pairs will give nearly optimal results in terms of entanglement for both the pairs.

Advantage of the decoupling by interference is that cross talk from *all* entangled pairs can be nearly perfectly removed. Moreover, technical imperfections, as the modes match imperfectly at the decoupling BS, can be incorporated to the full optimization. Despite such a principal advantage, one may be interested in maximizing entanglement in only one pair of modes. In this case entanglement localization [43, 44] can be applied by performing only an optimized measurement on one pair and feed-forward control on another pair of modes based on the measurement outcomes, which we consider in the next Section and compare it to the above suggested method of reversed coupling.

4. Entanglement localization by measurement and feed-forward control

In order to compensate the negative effect of cross talk in *only one* entangled pair in the scheme given in Fig. 1, we now consider a possibility to apply optimized Gaussian measurement of one pair of modes and feed-forward control of the other pair on the receiving sides and thus to increase the shared entanglement at the cost of losing one of the mode pairs. This method relies on the highly efficient and low-noise homodyne measurement and the high fidelity feed-forward control and coherent displacement [9, 51]. Similarly as in the previous Section, we theoretically consider a simple two-mode case with the feed-forward control applied by Alice and Bob on the first pair of modes A_1, B_1 after the measurement on the second pair of modes A_2, B_2, as shown in Fig. 5. Instead of a direct interference of multimode signals on a coupler with variable t_r, we interfere the signal modes A_2, B_2 with the local oscillator beams in a generalized Gaussian measurement [52] on both Alice and Bob sides of the scheme, as shown in Fig. 5. Photocurrents from this detection control the modulation units in the other pair of modes A_1, B_1. We therefore assume that both the sender and the receiver perform a general Gaussian measurement [52] on the second pair of modes (A_2, B_2), i.e., a generalized heterodyne (also known as double-homodyne) measurement, using unbalanced beam-splitters with transmittance values t_A and t_B in Alice's and Bob's sides respectively. The beam-splitters divide each of the measured modes A_2, B_2 (into auxiliary detection modes denoted as C_A, C_B, D_A, D_B) and the outputs are then measured in conjugate quadratures using two homodyne detectors (with no loss of generality we assume x-quadrature measured on C_A, C_B and p-quadrature measured on D_A, D_B). It is advantageous to optimize the measurement shown in Fig. 5, we are therefore searching for optimal t_A and t_B that maximize the logarithmic negativity of the conditional state in the first pair of modes A_1, B_1. We evaluate conditional matrix of the state in modes A_1, B_1 after a homodyne measurement of a quadrature r (being either x or p) in mode K (being one of C_A, C_B, D_A, D_B). The covariance matrix of the modes A_1, B_1 and K before the measurement is $\gamma_{A_1B_1K} = \begin{pmatrix} \gamma_{A_1} & c_{A_1B_1} & c_{A_1K} \\ c_{A_1B_1} & \gamma_{B_1} & c_{B_1K} \\ c_{A_1K} & c_{B_1K} & \gamma_K \end{pmatrix}$. The measurement resulting in an outcome r_K transforms the covariance matrix as [53]

$$\gamma_{A_1B_1|r_K} = \gamma_{A_1B_1} - \sigma_{A_1B_1,K} \left(R \cdot \gamma_K \cdot R\right)^{MP} \sigma^T_{A_1B_1,K}, \tag{27}$$

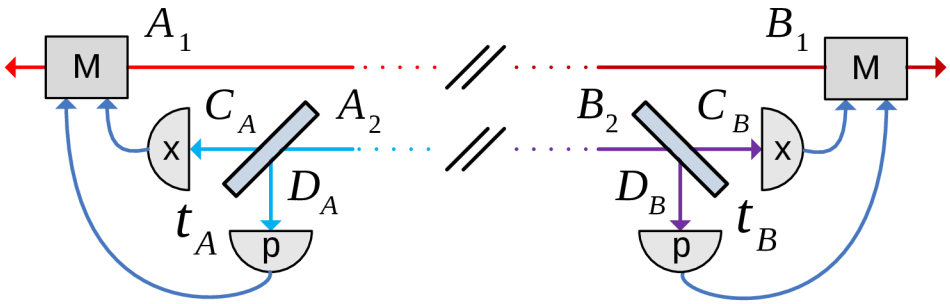

Fig. 5. Measurement and feed-forward control scheme aimed at compensating cross talk and localizing maximum of entanglement in the pair of modes A_1, B_1. The two parties perform generalized Gaussian measurements by splitting modes A_2, B_2 on variable beam-splitters t_A, t_B and measuring x-quadratures on the modes C_A, C_B and p-quadratures on the auxiliary detection modes C_A, C_B, D_A, D_B. The measurement outcomes are then used to modulate A_1, B_1. The rest of the scheme (source, cross talk and channel) is as in Fig. 1. The scheme allows increasing entanglement in modes A_1, B_1 at the cost of tracing out modes A_2, B_2.

where $\sigma_{A_1B_1,K} = \begin{pmatrix} c_{A_1K} \\ c_{B_1K} \end{pmatrix}$ is the correlation matrix between modes A_1, B_1 and K, matrix R is a diagonal matrix, being either $\frac{1}{2}(\mathbb{I}+\mathbb{Z})$ for an x-quadrature measurement or $\frac{1}{2}(\mathbb{I}-\mathbb{Z})$ for a measurement of p-quadrature, and MP stands for Moore-Penrose pseudo-inverse of a matrix, applicable to singular matrices. The state in equation (27) can be obtained either by an optimal feed-forward control of the state in modes A_1, B_1 or by post-selecting the states in modes A_1, B_1 based on a condition on the measurement outcomes in modes A_2, B_2. While the first strategy is deterministic, but requires optimization of feed-forward, the second one does not rely on optimization, but is probabilistic. It only asymptotically approaches the result of feed-forward control, and while the probability of success greatly reduces while approaching this result due to reduction of the post-selection interval. On the other hand, it does not require gain optimization and optical modulation as the deterministic method does. Repeating the conditioning (27) generally for each of four measurements, we arrive at the general conditional matrix $\gamma_{A_1B_1|x_{C_A},x_{C_B},p_{D_A},p_{D_B}}$, which reads $\begin{pmatrix} \tilde{\gamma}_{A_1} & \tilde{C}_{A_1B_1} \\ \tilde{C}_{A_1B_1} & \tilde{\gamma}_{B_1} \end{pmatrix}$ with sub-matrices

$$\tilde{\gamma}_{A_1} = \begin{pmatrix} \frac{T_2 r_B (V-1)[V-t_A(t_c V+t+[V-1])]+V[t_A(V-1)-V]}{t_c T_2 r_A r_B (V^2-1)+[t_A(V-1)-V][T_2 r_B (V-1)+1]} & 0 \\ 0 & \frac{T_2 t_B (V-1)[t_A(V-1)+1-t_c r_A (V+1)]+V(t_A-t_A V-1)}{t_A(V-1)(T_2 t_B[1+t_c-r_c V]-1)-T_2 t_B (V-1)-1} \end{pmatrix}, \tag{28}$$

$$\tilde{\gamma}_{B_1} = \begin{pmatrix} 1+T_1(V-1)-\frac{r_c T_1 r_A (V^2-1)}{t_A+r_A\left[V-\frac{t_c T_2 r_B (V^2-1)}{1+T_2 r_B (V-1)}\right]} & 0 \\ 0 & 1+T_1(V-1)-\frac{r_c T_1 t_A (V^2-1)}{r_A+t_A\left[V-\frac{t T_2 t_B (V^2-1)}{1+T_2 t_B (V-1)+1}\right]} \end{pmatrix} \tag{29}$$

and

$$\tilde{C}_{A_1B_1} = \begin{pmatrix} \frac{\sqrt{t_c T_1}\sqrt{V^2-1}[(T_2(1-2t_A)r_B+t_A)(V-1)-V]}{t_c T_2 r_A r_B (V^2-1)+[t_A(V-1)-V][1+T_2 r_B (V-1)]} & 0 \\ 0 & \frac{\sqrt{t_c T_1}\sqrt{V^2-1}[1+(t_A(1-2T_2 t_B)+T_2 t_B)(V-1)]}{t_A(V-1)[T_2 t_B(1+t_c+r_c V)-1]-T_2 t_B (V-1)-1} \end{pmatrix}, \tag{30}$$

where $r_A \equiv 1-t_A$, $r_B \equiv 1-t_B$. From this two-mode matrix we can evaluate Gaussian entanglement of the conditioned state in terms of logarithmic negativity, which we do numerically.

First, we observe that the best possible result for any given channel transmittance values and any cross talk level is achieved by using homodyne measurement on the receiver side. It corresponds to $t_B = 1$ or $t_B = 0$, i.e. measuring either only C_B (homodyne measurement of x-quadrature) or only D_B (homodyne measurement of p-quadrature) mode in Fig. 5. We further assume with no loss of generality that $t_B = 1$, which is equivalent to Bob measuring x-quadrature of the mode A_2 with a homodyne detector. On the other hand, an optimal t_A on the receiver side generally depends on the TMSV state variance V, channel parameters (transmittance values and excess noise) and the cross talk coupling t_c. In the general case t_A can be found only numerically, but in the limit of large V and noiseless channels, we can find the t_A that maximizes the logarithmic negativity in $\gamma_{A_1B_1|x_{C_A},x_{B_2},p_{D_A}}$ analytically. Then for $V \to \infty$ and $\varepsilon = 0$ in the limit of the weak cross talk $t_c \lesssim 1$ the optimal t_A on the sender side is independent of the TMSV variance and can be approximated as

$$t_{A_{opt}} = \max\left[0, 1 - \frac{(1+T_1)(1-T_2)}{2+2T_1(1-T_2)-4T_2} + O(1-t_c)\right] \tag{31}$$

In the case, when additionally losses are low ($T_1 \to 1, T_2 \to 1$), the optimal setting at the sender side is $t_A = 0$. This means that for the highly transmitting channels or low cross talk the best strategy for the feed-forward method of cross talk compensation is to use homodyne measurement on Alice's side and measure complementary quadrature to the one that the receiver (Bob) measures. This phenomena can be explained using continuous-variable quantum erasing, where Alice by measurement prepares a squeezed state in front of the cross talk which, using homodyne measurement of antisqueezed variable and feed-forward control, can be used to eliminate beam-splitter type of cross talk [54, 55]. The covariance matrix for a noiseless channel then turns to

$$\gamma_{A_1B_1|p_{A_2},x_{B_2}} = \begin{pmatrix} V - \frac{r_c T_2(V^2-1)}{1+T_2(V-1)} & 0 & \sqrt{t_c T_1(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{t_c T_1(V^2-1)} \\ \sqrt{t_c T_1(V^2-1)} & 0 & 1+T_1(V-1) & 0 \\ 0 & -\sqrt{t_c T_1(V^2-1)} & 0 & \frac{V+T_1(V-1)(Vt_c+t_c-1)}{V} \end{pmatrix} \tag{32}$$

In a simple case of a perfect channel ($T_i = 1$ and $\varepsilon = 0$), the logarithmic negativity of the state in modes A_1, B_1 (conditioned on homodyne measurement outcomes on both sides) can be expressed analytically as

$$LN_{hom} = -\log_2\left[\sqrt{1+t_c\left(V^2-1\right)} - \sqrt{t_c\left(V^2-1\right)}\right]. \tag{33}$$

It is always larger than the logarithmic negativity in the same pair of modes after the crosstalk and in the same perfect channels, but without conditioning, which reads $LN = -\log_2\left[V - \sqrt{t_c\left(V^2-1\right)}\right]$. The latter equation reaches maximum when $V_{opt} = \frac{1}{\sqrt{1-t_c}}$, while (33) is a constantly growing function of V. It illustrates the fact that the conditional measurement overcomes the limit on the initial entanglement given by (10) and generally any need to optimize the initial state. Therefore it allows to use as high initial entanglement as it is experimentally achievable. When the state is conditioned on the optimal homodyne measurement in a highly transmitting channel, the logarithmic negativity of the state in modes A_1, B_1 is not bounded and in the limit of arbitrarily strong TMSV variance $V \to \infty$, assuming a noiseless channel ($\varepsilon = 0$) tends to

$$\lim_{V\to\infty} LN_{hom} = -\frac{1}{2}\log_2\left[\frac{(1-T_1)[T_1(1-t_c-T_2)+t_cT_2]}{t_c(1+T_1)^2T_2}\right] \tag{34}$$

which may eventually for large initial variance turn to zero if the condition $t_c < \frac{(1-T_1)(1-T_2)}{1-T_1(1-T_2)+3T_2}$ is met. However, for realistic values of relatively weak cross talk ($t_c > 0.5$), it happens only for very low T_2. i.e. in channels with high loss. For such channels the homodyne measurement on the sender side is not the optimal one. As the losses in the channel increase, the optimal measurement gets closer to the balanced heterodyne, i.e., to $t_A = 1/2$. Moreover, in the most practical cases, i.e. when T_1 is close to T_2, and the cross talk is small, finding the optimal t_A gives little improvement. In this case it is enough for sender to use homodyning for the highly transmitting (short) channels and heterodyning for the highly attenuating (long) ones, while receiver shall use homodyning in both cases. This result contrasts with the previous results [56] for recovering quantum information by conditional measurement of the modes leaked into environment, where heterodyne measurement on the receiver side is optimal.

In the case, when the channels are strongly attenuating ($T_{1,2} \to 0$), the optimal t_A given by (31) turns to $1/2$, i.e., the balanced heterodyne detection on the sender side becomes the optimal measurement. In this case, when we also chose the optimal $t_B = 1$, the conditional covariance matrix of the state in modes A_1, B_1 becomes (assuming no excess noise, $\varepsilon = 0$)

$$\gamma_{A_1B_1|x_{A_2},p_{D_A},x_{B_2}} = \begin{pmatrix} \frac{V-T_2(V-1)r_c}{1-T_2r_c(V-1)} & 0 & \sqrt{t_cT_1(V^2-1)} & 0 \\ 0 & V & 0 & \frac{-\sqrt{t_cT_1(V^2-1)}}{1-T_2r_c(V-1)} \\ \sqrt{t_cT_1(V^2-1)} & 0 & \frac{1+T_2(V-1)+t_c(T_1-T_2)(V-1)}{1-T_2r_c(V-1)} & 0 \\ 0 & \frac{-\sqrt{t_cT_1(V^2-1)}}{1-T_2r_c(V-1)} & 0 & 1+t_cT_1(V-1) \end{pmatrix} \tag{35}$$

The logarithmic negativity is then as well not bounded and the optimization of the initial entanglement (11) is not needed. In the limit of very strong initial entanglement $V \to \infty$ (assuming no excess noise, $\varepsilon = 0$) it tends to

$$\lim_{V\to\infty} LN_{het} = -\frac{1}{2}\log_2\left[\frac{(1-t_cT_1)[1-t_c(T_1-T_2)-T_2]}{(1+t_cT_1)^2-(1-t_c)T_2(1-t_cT_1)}\right] \tag{36}$$

which is always positive, contrary to the logarithmic negativity before conditioning, which vanishes at (10). Eq. (34) and (36) show that by optimized conditional measurement one can beat the limit on the maximal initial entanglement given by (10) and recover the entanglement degraded or destroyed by the cross talk, although such strong initial squeezing and/or cross talk are not very likely in practical applications.

In the general case of intermediate channel attenuation and level of cross talk an optimized heterodyne measurement on the sender side should be chosen by evaluating the respective logarithmic negativities, but entanglement in the remaining pair of modes after the measurement and feed-forward control is always no less, than before these operations. Therefore, optimized measurement and feed-forward can always improve (and fully restore in the case of almost perfectly balanced channels) entanglement in a single pair of modes at the cost of loosing another pair. We illustrate the efficiency and stability of the method with respect to the sender measurement settings in Fig. 6 and show that it can largely restore the entanglement in the remaining pair of modes and is stable with respect to the measurement setting t_A. As it is evident from Fig. 6, any kind of Gaussian measurement on the pair A_2, B_2, even not an optimized one, largely restores entanglement in the pair A_1, B_1. The best result is achieved with the homodyne measurement of the x-quadrature on the sender side ($t_A = 1$) in the low loss channels and with the heterodyne measurement ($t_A = 1/2$) in the strong loss channels, which agrees with approximate analytical results given above in (31). Remarkably, the optimized measurement allows to recover entanglement that was completely destroyed by the cross talk.

We also compare the method of optimized measurement and feed-forward to the method of

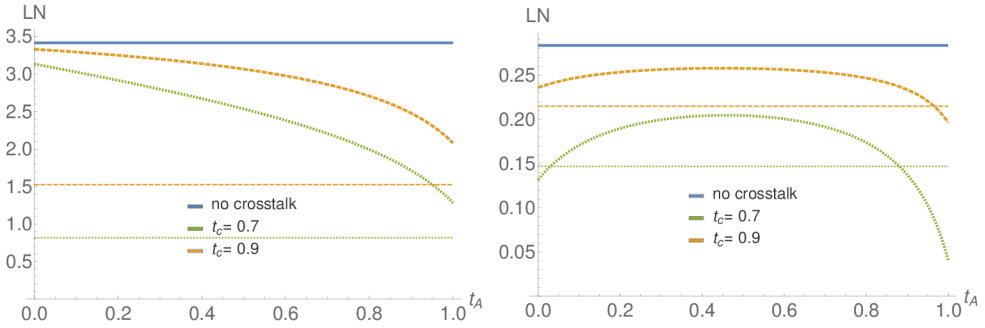

Fig. 6. Logarithmic negativity in the A_1, B_1 pair of modes after applying measurement of the pair A_2, B_2 and feed-forward control, versus detection setting t_A on the sender side. Left: low unbalanced channel loss ($T_1 = -0.4dB$, $T_2 = -0.5dB$), right: strong unbalanced channel loss ($T_1 = -10dB$, $T_2 = -10.5dB$). On both plots no excess noise is present ($\varepsilon = 0$). The thin dashed lines represent the logarithmic negativity in the A_1, B_1 pair without the optimized measurement and feed-forward control, but with the initial state variance being optimized as in (11).

optical interference, suggested in the previous section, as shown in Fig. 7 for low and high channel losses.

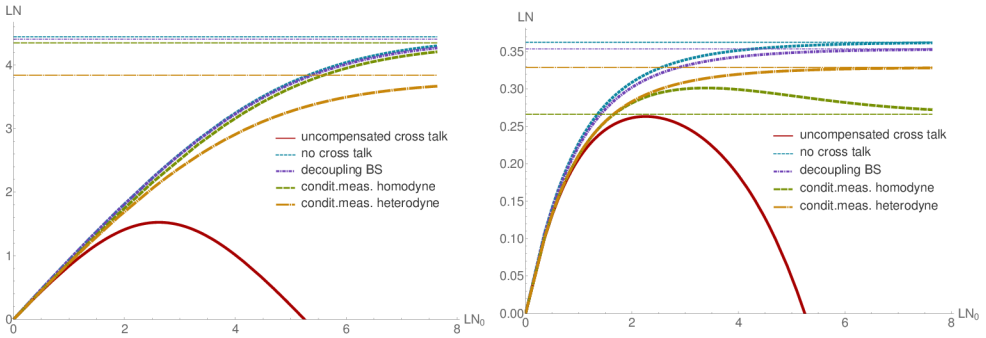

Fig. 7. Logarithmic negativity in the pair A_1, B_1 after applying optical interference method or measurement of the pair A_2, B_2 and feed-forward control, as indicated in the plots. Cross talk is $t_c = 0.9$, the optimal decoupling beam-splitter transmittance t_r is given by eq. (25), no excess noise ($\varepsilon = 0$). Left: low loss unbalanced channels ($T_1 = -0.4dB$, $T_2 = -0.5dB$), right: high loss unbalanced channels ($T_1 = -9dB$, $T_2 = -10dB$). The thin horizontal lines represent the asymptotes for $LN_0 \to \infty$ given by (26) for the decoupling method, (34) and (36) for the homodyne and heterodyne measurement method, and (6) for the no cross talk case.

It is evident from the plots, that the method of optimized optical interference is always more efficient in restoring the Gaussian entanglement and, besides, it preserves the multimode structure. Our further analysis shows, that this superiority holds always, unless the channels are strongly unbalanced (with either of the channels being strongly attenuating while another one being almost lossless, $T_i \to 1$ and $T_j \to 0$), which is, however, very unlikely in practical situations. While being less efficient, the measurement strategy can be sometimes nearly optimal and become very close to the optimized measurement strategy, however, the measurement inevitably destroys one pair modes. Both of the methods increase the amount of entanglement, that can be transferred,

and remove the necessity to optimize the initial entanglement. The lines corresponding to interference method (purple) and to the conditional measurement (green and yellow) continue to the right approaching the asymptotes given by (26), (34), (36), and the lines corresponding to the ideal case without cross talk (blue) approach the asymptote (6). We also compare the methods in Fig. 8 for the same initial entanglement in the large region of transmittance values and in the presence of unbalancing. In Fig.8 we plot the Gaussian entanglement for the both pairs

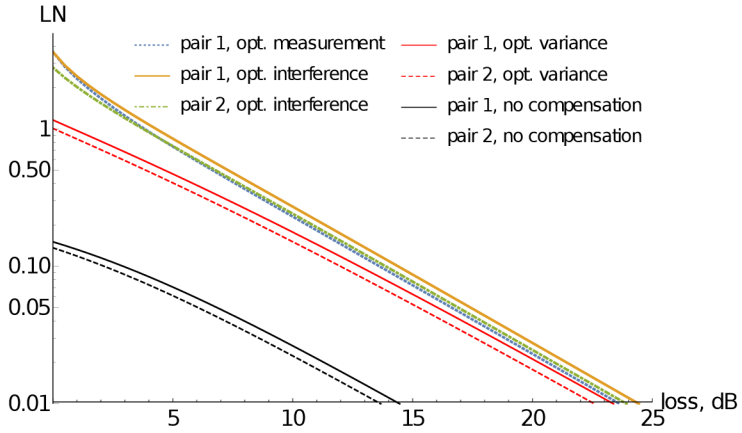

Fig. 8. Comparison of the methods for the cross talk compensation: optical interference using a decoupling beam-splitter, and entanglement concentration by optimized conditional measurement and feed-forward control. Plot shows the logarithmic negativity in a pair of modes after each respective method is applied. Initial entanglement is fixed $LN_0 = 4.0$, cross talk is $t_c = 0.8$, and transmittances ratio is $T_1/T_2 = 1.2$, parameters t_r and t_A are optimized. The ideal case without any cross talk is not shown, but would be indistinguishable from optimized interference for the given parameters.

of modes in case of the optimized optical interference and show that method allows to restore the entanglement in both the modes contrary to the method of conditional measurement. For a weaker unbalancing the entanglement of both pairs of modes after the optimized interference would overlap. Only one (blue) line in Fig.8 corresponds to the conditional measurement method, it demonstrates that although this method is quite effective for restoring entanglement in one pair, it also destroys the second pair of modes. We have not presented the case with no cross talk on the plot because for the given set of parameters it will be almost fully overlapping with the results for the optimized optical interference method. It illustrates the fact that even for relatively strong cross talk, the optimized interference approach allows to recover the entanglement almost completely. Both active methods give substantial gain compared to initial state before recovery. For any cross talk t_c, state variance V, and channel transmittance T_1, T_2 both the proposed methods outperform the simple optimization of the initial entanglement shared (or equivalently the variance V) as proposed in the Sec. 2.

Conditional measurement with feed-forward control gives guaranteed entanglement gain no matter how strong is the cross talk and does not rely on our knowledge of cross talk coupling t_c, while discarding one of the modes. However, this benefit is heavily paid for by a low probability of success of this asymptotic method. On the other hand, the optical interference scheme allows to preserve all the modes. It gives better results than the entanglement concentration with the conditional measurement scheme for most realistic values of t_c, especially in channels with higher loss. In the case of the state having only several modes, both of the methods perform comparably. For multimode states with higher number of modes the advantage of the optimal

interference method will be more pronounced as it preserves all the modes, while the conditional measurement method is based on discarding most of them.

5. Conclusion

Entanglement distribution is a key ingredient of modern quantum technology. We considered the effect of cross talk on entanglement distribution using Gaussian multimode twin-beam states and shown that initial entanglement inserted to a multimode link has to be optimized to reach its maximal transmission already if cross talk is weakly present. We then suggest the method of cross talk compensation based on optimized optical interference using adjustable phase control and linear coupling of modes, and show that the method can completely eliminate the negative effect of cross talk once the channel transmittance is balanced, i.e., is the same for all the modes. The method is still very efficient for small unbalancing between the channel transmittance values for different modes and is stable with respect to the linear coupling setting, but requires knowledge of the cross talk strength. This methodology can be extended to many multiplexed modes, however, in such a case the numerical analysis and optimization are needed for specific real channels, as the model of the cross talk will be more complicated and vary in practical situations. We therefore leave the analysis of the real cross talk in the source or channel for future experimental tests. As an alternative, we suggest the method of cross talk compensation for one of the pairs of modes by optimized Gaussian measurement on another pair and feed-forward control, which does not rely on knowledge of cross talk strength and can restore entanglement in the remaining pair, while reducing the multimode structure, and is also limited in the unbalanced channels. The method of optical interference remains more efficient unless the channels are very strongly unbalanced, which is however not likely in the practical situations, and preserves the amount of entangled modes transmitted through the channel. Our methods can be prospective for realization of multimode quantum communication in the presence of cross talk in the sources and channels. Note that the described cross talk compensation methods distribute entanglement between the modes, but do not increase it beyond the initial entanglement in the source before the cross talk, hence not contradicting the impossibility of entanglement distillation by local Gaussian unitary operations [53, 57]. Our results demonstrate basic principles in a simple case of only nearest-mode cross talk. The further investigation for larger number of modes in the presence of cross talk will require multi-parameter numerical optimizations and possibly application of modern methods of deep machine learning applicable to quantum optics [58] to find efficient strategy of cross talk compensation. Such numerical optimizations in application to complex multimode cross-talk effects will be the subject of future studies.

Funding

The research leading to these results has received funding from the H2020 European Programme under Grant Agreement 820466 CIVIQ. OK acknowledges support from Palacky University project IGA-PrF-2021-006. OK and VCU acknowledge support from the project 19-23739S of the Czech Science Foundation. R.F. acknowledges support by the project CZ 02.1.01/0.0/0.0/16_026/0008460 of MEYS CR and jointly, national funding from the MEYS and the funding from European Union's Horizon 2020 (2014-2020) research and innovation framework programme under grant agreement No 731473 (project 8C20002 ShoQC). Project ShoQC has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme.

Disclosures

The authors declare that there are no conflicts of interest related to this article.

References

1. W. T. Tittel and G. Weihs, "Photonic entanglement for fundamental tests and quantum communication," Quantum Inf. & Comput. **1**(2), 3 (2001).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145 (2002).
3. 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. Photon. **12**(4), 1012–1236 (2020).
4. P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nat. Phys. **10**(8), 582–587 (2014).
5. H. J. Kimble, "The quantum internet," Nature **453**(7198), 1023–1030 (2008).
6. R. Ukai, S. Yokoyama, J.-i. Yoshikawa, P. van Loock, and A. Furusawa, "Demonstration of a controlled-phase gate for continuous-variable one-way quantum computation," Phys. Rev. Lett. **107**, 250501 (2011).
7. X. Su, H. Shuhong, X. Deng, L. Ma, M. Wang, X. Jia, C. Xie, and K. Peng, "Gate sequence for continuous variable one-way quantum computation," Nat. communications **4**, 2828 (2013).
8. R. Filip, "Continuous-variable quantum nondemolishing interaction at a distance," Phys. Rev. A **69** (2004).
9. S. Yokoyama, R. Ukai, J.-i. Yoshikawa, P. Marek, R. Filip, and A. Furusawa, "Nonlocal quantum gate on quantum continuous variables with minimum resources," Phys. Rev. A **90**, 012311 (2014).
10. O. Morin, K. Huang, J. Liu, H. Le Jeannic, C. Fabre, and J. Laurat, "Remote creation of hybrid entanglement between particle-like and wave-like optical qubits," Nat. Photonics **8** (2013).
11. H. Jeong, A. Zavatta, M. Kang, S.-W. Lee, L. S. Costanzo, S. Grandi, T. C. Ralph, and M. Bellini, "Generation of hybrid entanglement of light," Nat. Photonics **8**(7), 564–569 (2014).
12. Z. Yan, L. Wu, X. Jia, Y. Liu, R. Deng, S. Li, H. Wang, C. Xie, and K. Peng, "Establishing and storing of deterministic quantum entanglement among three distant atomic ensembles," Nat. Commun. **8** (2017).
13. M. Huo, J. Qin, J. Cheng, Z. Yan, Z. Qin, X. Su, X. Jia, C. Xie, and K. Peng, "Deterministic quantum teleportation through fiber channels," Sci. Adv. **4**, eaas9401 (2018).
14. K. Huang, H. Le Jeannic, O. Morin, T. Darras, G. Guccione, A. Cavailles, and J. Laurat, "Engineering optical hybrid entanglement between discrete- and continuous-variable states," New J. Phys. **21**, 083033 (2019).
15. G. Vidal and R. F. Werner, "Computable measure of entanglement," Phys. Rev. A **65**(3), 032314 (2002).
16. A. Peres, "Separability criterion for density matrices," Phys. Rev. Lett. **77**, 1413–1415 (1996).
17. M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," Phys. Lett. A **223**(1), 1–8 (1996).
18. T. Eberle, V. Händchen, and R. Schnabel, "Stable control of 10 db two-mode squeezed vacuum states of light," Opt. Express **21**(9), 11546–11553 (2013).
19. B. Hage, A. Samblowski, and R. Schnabel, "Towards Einstein-Podolsky-Rosen quantum channel multiplexing," Phys. Rev. A **81**, 062301 (2010).
20. M. Heurs, J. G. Webb, A. E. Dunlop, C. C. Harb, T. C. Ralph, and E. H. Huntington, "Multiplexed communication over a high-speed quantum channel," Phys. Rev. A **81**, 032325 (2010).
21. T. Kouadou, L. L. Volpe, S. De, C. Fabre, V. Parigi, and N. Treps, "Single-pass generation of spatial and spectral multimode squeezed states of light," Frontiers in Optics + Laser Science APS/DLS (Optical Society of America, 2019), p. FTh3B.7.
22. S. Shi, L. Tian, Y. Wang, Y. Zheng, C. Xie, and K. Peng, "Demonstration of channel multiplexing quantum communication exploiting entangled sideband modes," Phys. Rev. Lett. **125**, 070502 (2020).
23. Z. Qu and I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," IEEE Photonics J. **9**(6), 1–8 (2017).
24. A. Christ, C. Lupo, and C. Silberhorn, "Exponentially enhanced quantum communication rate by multiplexing continuous-variable teleportation," New J. Phys. **14**(8), 083007 (2012).
25. G. de Valcarcel, G. Patera, N. Treps, and C. Fabre, "Multimode squeezing of frequency combs," Phys. Rev. A **74**, 61801– (2006).
26. O. Pinel, P. Jian, R. M. De Araujo, J. Feng, B. Chalopin, C. Fabre, and N. Treps, "Generation and characterization of multimode quantum frequency combs," Phys. Rev. Lett. **108**(8), 083601 (2012).
27. J. Roslund, R. M. De Araujo, S. Jiang, C. Fabre, and N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs," Nat. Photonics **8**(2), 109 (2014).
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**(3), 032046(R) (2020).
29. S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain," Nat. Photonics **7**(12), 982 (2013).
30. J.-i. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa, "Invited article: Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing," APL Photonics **1**(6), 060801 (2016).
31. 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).
32. X. Zhu, C.-H. Chang, C. González-Arciniegas, A. Pe'er, J. Higgins, and O. Pfister, "Hypercubic cluster states in the

phase modulated quantum optical frequency comb," arXiv preprint arXiv:1912.11215 .
33. T. Kudo and T. Ishigure, "Analysis of interchannel crosstalk in multimode parallel optical waveguides using the beam propagation method," Opt. Express **22**(8), 9675–9686 (2014).
34. L. Szostkiewicz, M. Napierala, A. Ziolowicz, A. Pytel, T. Tenderenda, and T. Nasilowski, "Cross talk analysis in multicore optical fibers by supermode theory," Opt. Lett. **41**(16), 3759–3762 (2016).
35. B. Nada and T. Berceli, "Crosstalk reduction in fiber links using double polarization," Opt. Quantum Electron. **52** (2020).
36. 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).
37. V. C. Usenko, L. Ruppert, and R. Filip, "Quantum communication with macroscopically bright nonclassical states," Opt. Express **23**(24), 31534–31543 (2015).
38. O. Kovalenko, K. Y. Spasibko, M. V. Chekhova, V. C. Usenko, and R. Filip, "Feasibility of quantum key distribution with macroscopically bright coherent light," Opt. Express **27**(25), 36154 (2019).
39. T. A. Eriksson, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, M. Takeoka, Y. Awaji, M. Sasaki, and N. Wada, "Crosstalk impact on continuous variable quantum key distribution in multicore fiber transmission," IEEE Photonics Technol. Lett. **31**(6), 467–470 (2019).
40. 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 (2012).
41. C. Lupo, L. Memarzadeh, and S. Mancini, "Removing correlations in signals transmitted over a quantum memory channel," Phys. Rev. A **85**, 012320 (2012).
42. R. Filip, "Squeezing restoration by a noisy probe from a classically correlated environment," Phys. Rev. A **81** (2010).
43. F. Verstraete, M. Popp, and J. I. Cirac, "Entanglement versus correlations in spin systems," Phys. Rev. Lett. **92**, 027901 (2004).
44. F. Sciarrino, E. Nagali, F. De Martini, M. Gavenda, and R. Filip, "Entanglement localization after coupling to an incoherent noisy system," Phys. Rev. A **79**, 060304 (2009).
45. M. Chen, N. Menicucci, and O. Pfister, "Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb," Phys. Rev. Lett. **112**, 120505 (2014).
46. P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**, 032309 (2012).
47. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Reports **6**, 19201 (2016).
48. G. Adesso, A. Serafini, and F. Illuminati, "Extremal entanglement and mixedness in continuous variable systems," Phys. Rev. A **70**, 022318 (2004).
49. V. Alwayn, *Optical Network Design and Implementation* (Cisco Press, 2014).
50. J. L. Streete, "Infrared measurements of atmospheric transmission at sea level," Appl. Opt. **7**(8), 1545–1549 (1968).
51. Y. Shiozawa, J.-i. Yoshikawa, S. Yokoyama, T. Kaji, K. Makino, T. Serikawa, R. Nakamura, S. Suzuki, S. Yamazaki, W. Asavanant, S. Takeda, P. Loock, and A. Furusawa, "Quantum nondemolition gate operations and measurements in real time on fluctuating signals," Phys. Rev. A **98**, 052311 (2017).
52. K. Miyata, H. Ogawa, P. Marek, R. Filip, H. Yonezawa, J.-i. Yoshikawa, and A. Furusawa, "Implementation of a quantum cubic gate by an adaptive non-gaussian measurement," Phys. Rev. A **93**, 022301 (2016).
53. J. Eisert, S. Scheel, and M. B. Plenio, "Distilling gaussian states with gaussian operations is impossible," Phys. Rev. Lett. **89**, 137903 (2002).
54. R. Filip, "Continuous-variable quantum erasing," Phys. Rev. A **67**, 042111 (2003).
55. U. Andersen, O. Glöckl, S. Lorenz, G. Leuchs, and R. Filip, "Experimental demonstration of continuous variable quantum erasing," Phys. Rev. Lett. **93**, 100403 (2004).
56. M. Sabuncu, R. Filip, G. Leuchs, and U. Andersen, "Environmental assisted quantum information correction for continuous variables," Phys. Rev. A **81** (2010).
57. J. Fiurášek, "Gaussian transformations and distillation of entangled gaussian states," Phys. Rev. Lett. **89**, 137904 (2002).
58. V. Dunjko and H. J. Briegel, "Machine learning and artificial intelligence in the quantum domain: a review of recent progress," Reports on Prog. Phys. **81**(7), 074001 (2018).

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]

Published: *Photonics research* Vol. 9, Issue 12, pp. 2351-2359 (2021)

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 and Shaanxi Key Laboratory of Information Photonic Technique, Xi'an Jiaotong University, Xi'an 710049, China

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, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2] *Laboratoire Kastler Brossel, Sorbonne Université, CNRS, ENS-Université PSL, Collège de France, 4 place Jussieu, 75252 Paris, France*
[3] *Department of Physics, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, Korea*
[4] *Key Laboratory for Physical Electronics and Devices of the Ministry of Education & Shaanxi Key Lab of Information Photonic Technique, Xi`an Jiaotong University, 710049 Xi`an, China*
[*] *kovalenko@optics.upol.cz*
[5] *caiyin@xjtu.edu.cn*

Abstract: 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 crosstalk and the gain can be minuscule. Advantageously, homodyne detectors allow solving this crosstalk 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 crosstalk between eight entangled pairs of modes. As the main result, we predict almost 15-fold higher secret key rate. This experimental test and analysis of frequency-multiplexed entanglement source opens the way for the field implementation of high-capacity quantum key distribution with continuous variables.

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, the optimal implementation of a quantum-secure network will be likely hybrid in the future, combining the advantages and suppressing the weaknesses of different protocols respectively to the requirements and conditions [2]. Currently, homodyne detection is fast, efficient and extremely low-noise, 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 crosstalk. Based on these advantages, a crosstalk elimination based on state or data manipulations has been addressed in [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 [28]). Differently 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 the transmitted modes.

Nowadays, CV QKD reaches a new level at which substantial increase of the secret key rate of mid-range protocols is a relevant target of the ongoing development and requires, in particular, development of crosstalk 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 neighbouring modes of the otherwise perfect entangled states [27]. In the current paper we suggest the multimode crosstalk 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 the security of the resulting CV QKD protocol. Without such a test on the multimode state with real crosstalk and errors it is impossible to estimate applicability of the crosstalk compensation for a large number of modes. A positive result demonstrating that the secret key rate can be enhanced by channel multiplexing with high efficiency, despite crosstalk 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 8 pairs of modes and mode-discriminating homodyne detection. For them, the crosstalk is a very natural phenomena 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 crosstalk and brings large improvement to the 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 secret key is still possible) by approximately 100 kilometres. 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 crosstalk in the source, however, it can be equally applicable to crosstalk 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 crosstalk). 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 entanglement source in multimode CV QKD test-bed 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 is 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 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

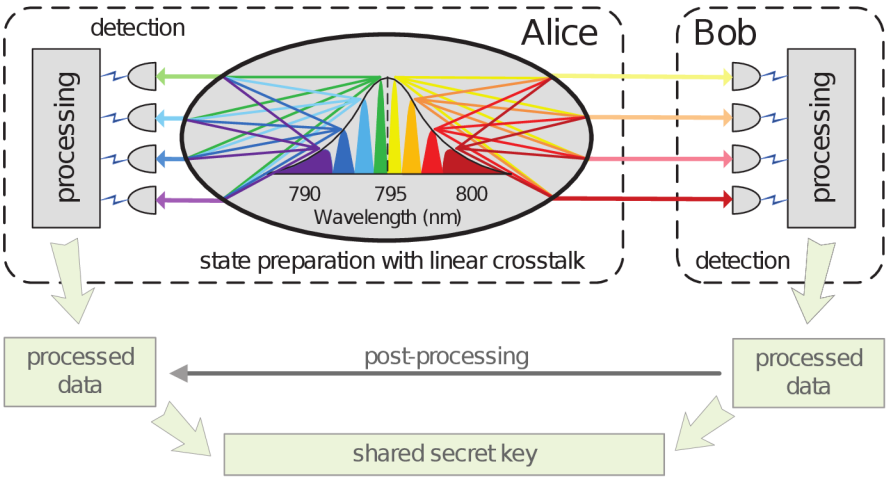

Fig. 1. Bright colors show a sketch of a CV QKD test-bed for study of the multimode entangled source at the side of sender, Alice, with crosstalk coupling between the frequency modes in both of the two beams, leaving the source. The entangled source is based on eight pairs of modes, where only four of them are shown for clarity. We consider a scenario where half of the modes (below the central frequency) is 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 crosstalk 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 modelled numerically so is illustrated in pale colors).

in a single beam, and the efficiency of the process is enhanced by the cavity constituting the SPOPO. For our purpose, we consider sixteen 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 x 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 sixteen 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 Fig. 5 of 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 crosstalk 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, while the Bob's modes travel directly towards 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). 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 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 purely lossy (attenuating) channel as the background noise is already very small in real optical fiber channels, such approach allows modelling 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 test-bed, where the multimode source was characterized, we assume that the crosstalk appears in the source, but our methodology can also be directly applied also to crosstalk in the channel and detectors.

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

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

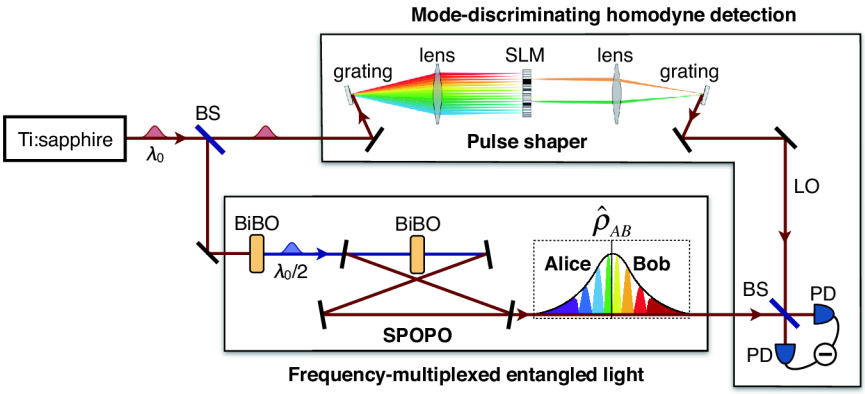

Fig. 2. Experimental setup for generation of frequency-multiplexed multimode entangled light and its measurement with mode-discriminating homodyne detection. The generated multimode light $\hat{\rho}_{AB}$ is in 16 frequency modes, where Alice (A) and Bob (B) access to the eight lower frequency modes 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.

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 -3dB. The positivity of the lower bound (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 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 respective security analysis methods, as described in the 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 (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 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

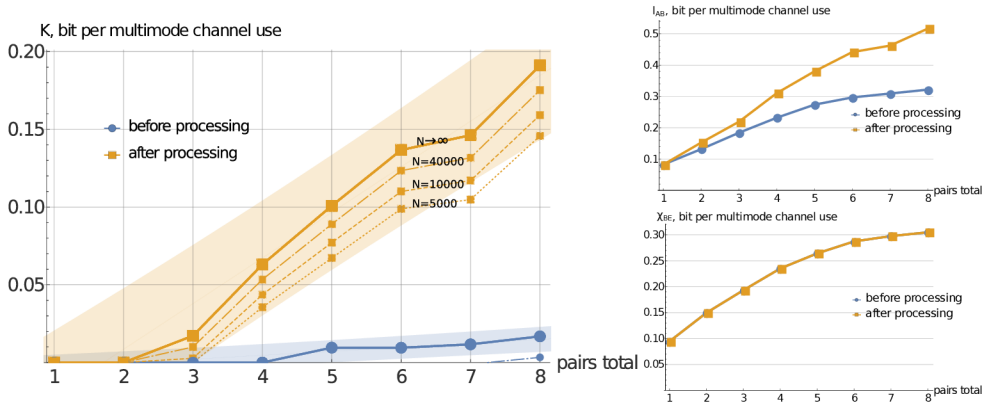

Fig. 3. Left panel: Estimated key rate (in terms of bits per multimode channel use) of CV QKD based on the frequency multiplexed entangled source in Fig.1 for different number of pairs measured by Alice and Bob as obtained from the original data before decoupling (circles, blue lines) and after decoupling of modes involved in the multimode crosstalk by optimized data processing performed by the trusted parties after the homodyne measurement (squares, yellow lines). The dotted, dot-dashed and dashed lines, represent the pessimistic estimates that take into account standard error for the respective number of measurements $N = 5 \cdot 10^3$, $N = 10^4$, $N = 4 \cdot 10^4$, 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.

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 crosstalk 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 analyse 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 8-pair covariance matrix after optimized data processing is illustrated in Fig. 4 in the Appendix A). By eliminating the crosstalk, 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 approx. 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 CV QKD protocol up to approx. 34 and 36 dB, see Appendix A for details. We also address the

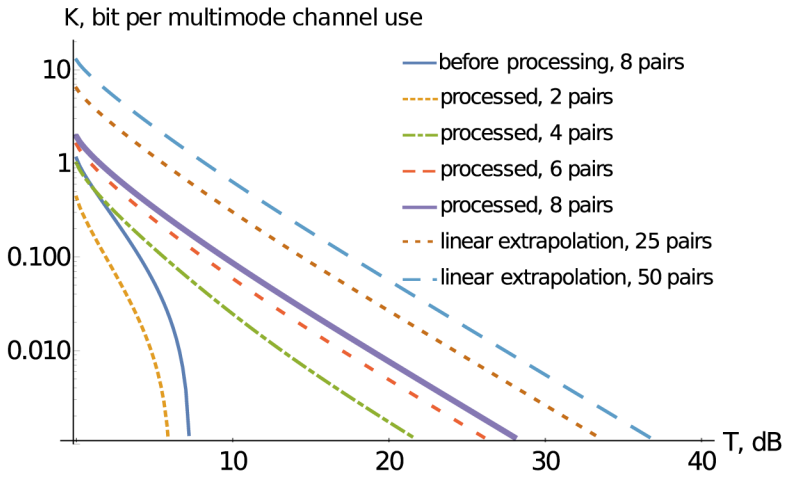

Fig. 4. Key rate of CV QKD versus channel transmittance T (in dB) as obtained from the original data on the full multimode entangled state (blue solid line), after optimized local data manipulations performed by the trusted parties for different number of used pairs of modes (non-solid lines for reduced 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.

efficiency of our method by comparing the achieved results to the bounds set by eight 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, the bound (eight 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, 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 8 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 crosstalk 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 crosstalk 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 crosstalk.

Summary and outlook

By optimally applying data manipulations we were able to compensate the crosstalk 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 three. 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 large number of modes [49]. Furthermore, the crosstalk 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 crosstalk in the multimode CV QKD source, the method can be also used to eliminate crosstalk 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 crosstalk compensation technique can be useful in other applications of continuous-variable quantum information, such as quantum imaging [52] or quantum illumination [53].

Appendix A

Security analysis

The key rate is calculated as $K = \max\left\{0, \beta I_{p_{AB}} - \chi_{BE}\right\}$, 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 data sets 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 data sets, 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 data sets 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 (1) is evaluated in bits 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, similarly 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 $S(E) = \sum_i \mathrm{G}\,\frac{\lambda_i - 1}{2}$, where λ_i are symplectic eigenvalues of γ_E and $\mathrm{G}(x) = (x+1)\log_2(x+1) - x\log_2 x$. 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 [32]).

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 covariance matrix for the i, j-pair is

$$\gamma_{ij} = \begin{pmatrix} V_i & C_{ij} \\ C_{ij} & V_j \end{pmatrix}. \tag{2}$$

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]

$$\sigma_{\gamma_{i,j}} = \frac{1}{\sqrt{N+1}} \begin{pmatrix} \sqrt{2}V_i & \sqrt{V_iV_j + C_{ij}^2} \\ \sqrt{V_iV_j + C_{ij}^2} & \sqrt{2}V_j \end{pmatrix}. \tag{3}$$

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 value of the off-diagonal elements (correlations) are decreased [56, 57]. The results are presented in the Fig. 2 as dashed lines. It is evident from the plots in the Fig. 2, that even multiplexing of all eight pairs can only slightly restore the non-zero 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 crosstalk 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 crosstalk and make the multimode resource more applicable for CV QKD.

Optimized data processing

Generally all the sixteen modes are getting coupled in the state preparation and such crosstalk should be possible to at least partially compensate for using a global 16x16 symplectic transformation that maximizes the mutual information. The quantum communication scenario makes such global transformation impossible, but the crosstalk can be significantly reduced even when we consider Alice and Bob performing only local operations independently of each other. Both Alice and Bob each control 8 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 crosstalk while preserving the security of the protocol. We are therefore looking for two 8x8 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

$$\gamma = \begin{pmatrix} V_1 & \cdots & C_{1,16} \\ \vdots & \ddots & \vdots \\ C_{16,1} & \cdots & V_{16} \end{pmatrix}, \tag{4}$$

with V_i and $C_{i,j}$ given in eq. (2) 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 is $(N/2-1)N/2 = 56$ 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

$$T_{ij} = \begin{pmatrix} \mathbb{I} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \sqrt{t_{ij}}\,\mathbb{I} & \sqrt{1-t_{ij}}\,\mathbb{I} & \cdots & 0 \\ 0 & \cdots & \sqrt{1-t_{ij}}\,\mathbb{I} & -\sqrt{t_{ij}}\,\mathbb{I} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \mathbb{I} \end{pmatrix}, \tag{5}$$

where t_{ij} is the transmittance coefficient, 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 $\gamma' = T_{1,2}\gamma T_{1,2}^T$, 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

$$U_A = T_{7,8}T_{6,8}...T_{1,3}T_{1,2} = \prod_{i=1,j=i+1}^{8} T_{i,j} \tag{6}$$

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

$$U_B = T_{15,16}T_{14,16}...T_{8,10}T_{8,9} = \prod_{i=9,j=i+1}^{16} T_{i,j} \tag{7}$$

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 $I_{x_{AB}}(\mathbf{t})$ and $I_{p_{AB}}(\mathbf{t})$ numerically, here

$\mathbf{t} = (t_{1,2}, t_{2,3}...t_{15,16})$ 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 isn't 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 limited memory Broyden–Fletcher–Goldfarb–Shannon (l-BGFS) optimization algorithm with bound constraints [59] from SciPy library. The l-BGFS performs $O(d)$ computation 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 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 [33]. It shows noticeable redistribution of correlations between the modes.

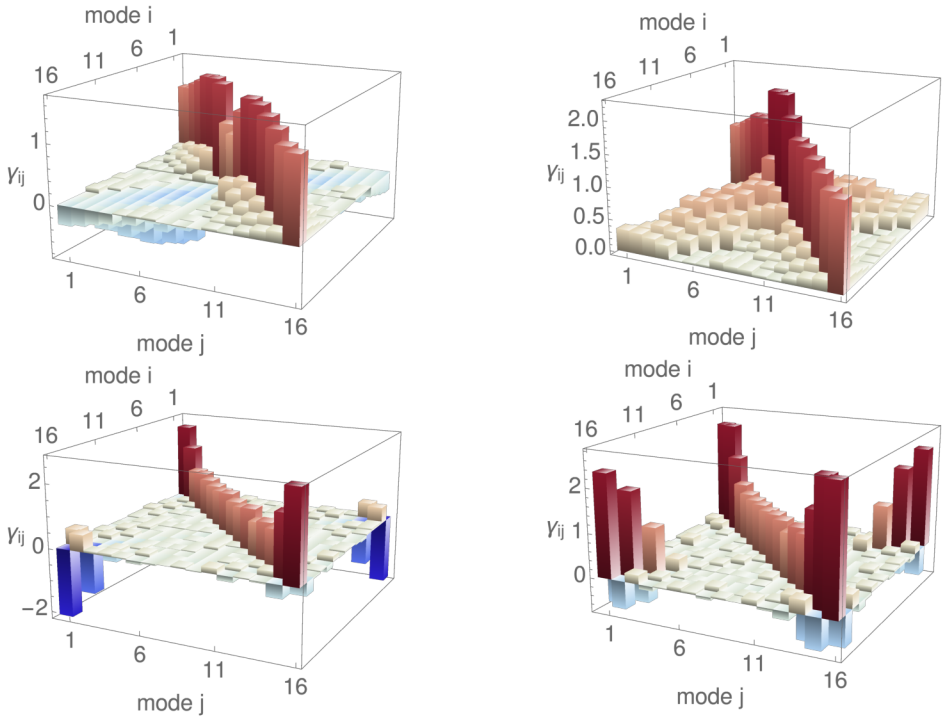

Fig. 5. Visualization of covariance matrices in $\hat{x}$ quadrature (left) and $\hat{p}$ quadrature (right) before (top) and after (bottom) the optimized linear data processing.

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. Besides, the most general set 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 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 sender or 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 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.

Results extrapolation

We predict the efficiency of our method for larger number 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 crosstalk) 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

O.K. acknowledges project IGA-PrF-2021-006 of Palacky University; Y.-S.R. acknowledges support from the European Commission through Marie Skłodowska-Curie actions (Grant No. 708201) and from a National Research Foundation of Korea grant funded by the Korea government Ministry of Science and ICT (Grant No. NRF-2019R1C1C1005196); Y.C acknowledges projects 11904279 and 12174302 of National Natural Science Foundation of China; O.K. and V.C.U. acknowledge project 19-23739S of the Czech Science Foundation; R.F. acknowledges project CZ.02.1.01/0.0/0.0/16_026/0008460 of the Czech Ministry of Education and national funding from the MEYS and the funding from European Union's Horizon 2020 (2014-2020) research and innovation framework programme under grant agreement No 731473 (project 8C20002 ShoQC). Project ShoQC has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. The authors also acknowledge support from COST Action CA 15220 QTSpace. The research leading to these results has received funding from the H2020 European Programme under Grant Agreement 820466 CIVIQ and 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. Photon. **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. Reports **6** (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," EPL (Europhysics 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** (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 (2017).
22. H. Ishio, J. Minowa, and K. Nosu, "Review and status of wavelength-division-multiplexing technology and its application," J. Light. Technol. **2**, 448–463 (1984).
23. K. Grobe and M. Eiselt, *Wavelength Division Multiplexing: A Practical Engineering Guide* (John Wiley & Sons, 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 *2018 41st International Conference on Telecommunications and Signal Processing (TSP),* (IEEE, 2018).
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(R) (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**, 61801– (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 (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 (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** (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. Royal Soc. A: Math. Phys. Eng. Sci. **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 (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** (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. review letters **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. review letters **94**, 020504 (2005).
55. M. G. Kendall, A. Stuart, and J. K. Ord, *Kendall's Advanced Theory of Statistics* (Oxford University Press, Inc., USA, 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. on 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, New York, NY, 2003).

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]

Published: *Optics Express* Vol. 27, Issue 25, pp. 36154-36163 (2019)

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

Following is an exact copy of the published article.

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

Optics EXPRESS

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

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

Optics EXPRESS

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.

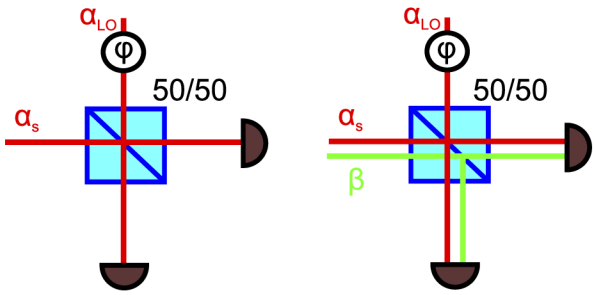

Fig. 1. The standard scheme for homodyne detection (left) and the scheme with uncompensated modes in the multimode signal beam (right).

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 $\varepsilon_{tot}^2 = 1/|\alpha_{LO}|^2$. 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.

Optics EXPRESS

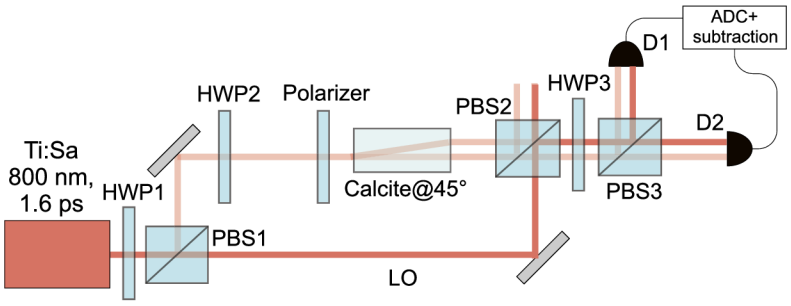

Fig. 2. The experimental setup used for the test of homodyne measurement of bright multimode coherent light.

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.

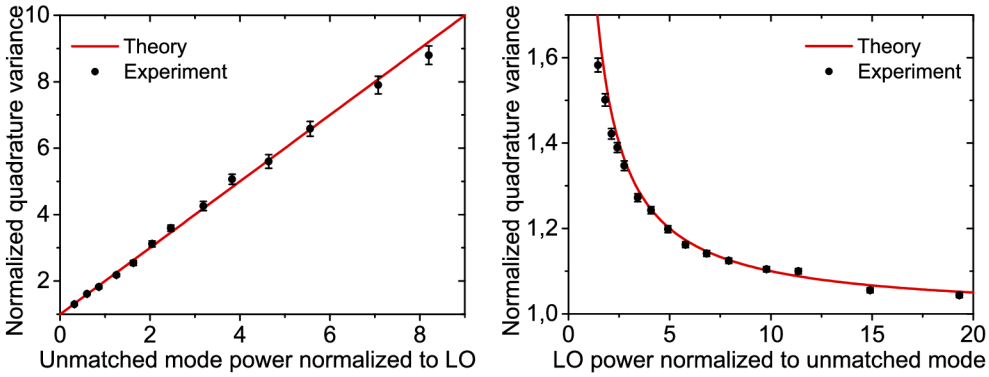

Fig. 3. Dependence of the normalized variance in SNU, experimentally measured (points) and theoretically predicted, according to Eq. (3) (lines), on unmatched mode power (left panel) and on LO power (right panel).

Optics EXPRESS

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 $\epsilon = 1$.

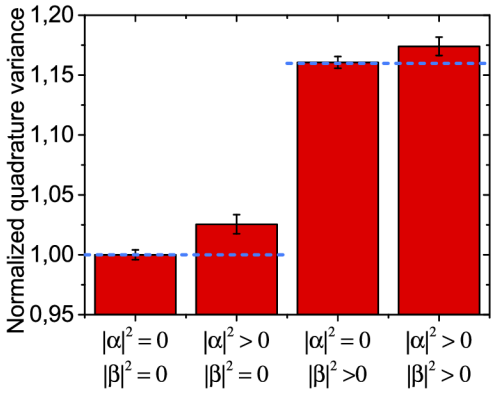

Fig. 4. Normalized variance of the quadrature measurements in SNU in the absence and presence of matched $|\alpha\rangle$ and unmatched $|\beta\rangle$ modes, $|\beta|^2 = 0.16|\alpha_{LO}|^2$. Theoretical prediction according to Eq. (3) is given in blue dashed lines.

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

Optics EXPRESS

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

Optics EXPRESS

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],

Optics EXPRESS

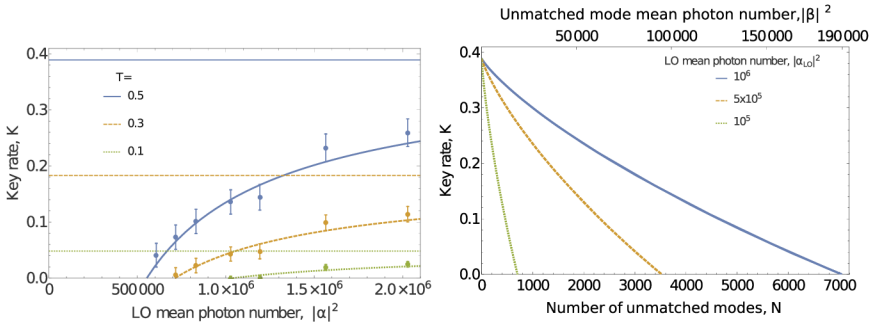

Fig. 5. Left: the key rate for multimode coherent-state CV QKD in the presence of mode mismatch versus the LO brightness at different values of the channel transmittance T, obtained from the experimentally measured noise (points with error bars) and from the calculated quadrature variance Eq. (1), $N/M = 1$ (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);

Optics EXPRESS

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).

Optics EXPRESS

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).

7 | Conclusions and outlook

In this thesis we theoretically study possibility to implement mode multiplexing in Gaussian quantum communication, in particular entanglement distribution and quantum key distribution. Our theoretical results have been experimentally verified in collaboration with LKB team at Sorbonne University in Paris (Prof. N. Treps) and the group at MPL Erlangen (Prof. M. Chekhova). Using the multimode quantum states, besides obvious advantage of multiplexing the protocol and increase in its capacity, can bring some issues, we address in detail one of them, the inter-mode cross talk, i.e. coupling of multiplexed modes among themselves. We also address the case when the mode-discriminating measurement is not available, and the multiple modes are not used for channel multiplexing, but to increase the signal brightness.

In Chapter 3 we theoretically study the cross talk problem in a simple 2-TMSV state model looking for the effect linear cross talk has on entanglement distribution. The entanglement shared is shown to be damaged by the cross talk. The cross talk puts limit on maximal entanglement that could be shared through the channel of given parameters. Presence of the cross talk also makes the entanglement more sensitive to other deteriorating factors, the channel loss and the excess noise. These negative effects of the cross talk can be compensated with an optimally chosen network of passive optical elements. We propose a compensation scheme with the phase adjustment and optimized interference on a beam-splitter, and compare it to an alternative scheme that uses optimal generalised homodyne measurement with feed-forward control. Both compensation schemes allow to almost fully eliminate negative cross talk influence. The proposed interference method, if implemented in an optimal way, shows better results and, unlike the measurement with feed forward control, preserves all the modes intact. To further advance this research, a model with larger number of modes should be considered, that will take into account random cross talk coupling occurring between modes in the source, channel and during detection, this model extension will allow to numerically evaluate performance of the suggested methods for large-scale multiplexing. We leave this step to experimental verification of such multiplexed protocols. Knowing how the proposed methods are scaling up is significant information for further development of multiplexed CV QKD.

In Chapter 4 we apply the optimal mode interference method, simplified version of which is theoretically described in Chapter 3, to an experimental multimode source. The synchronously pumped optical parametric oscillator produces a frequency multiplexed entangled state that is measured with mode-discriminating homodyne measurement. In the process of the state generation and measurement significant noise is introduced to

the signal, some of this noise can be attributed to linear cross talk among the frequency modes as in the theoretical model described in Chapter 3. We model an entanglement-based QKD protocol using data obtained from this experimental source, assuming that the party that posses the source shares half of the frequency modes bellow the maximal frequency with another remote party through a pure loss channel, and the parties then proceed to generate the secret key. Our analysis show that this QKD protocol can be implemented with the state generated in the SPOPO experiment only with the channel of comparatively low attenuation. We apply optimal numerical postprocessing (equivalent to the sequence of optimized beam-splitters, that is a multimode generalisation of the optimal interference method from Chapter 3) with the aim to compensate the cross talk and increase the mutual information and the secret key rate. The postprocessing allowed to increase the secret key rate and robustness of the protocol to channel attenuation from 8 dB to 28 dB, showing that the given frequency multiplexed source after being improved with postprocessing can be used for entanglement-based QKD. The next step is to implement experimentally and to analyse the frequency-multiplexed QKD protocol with modes distribution among users and to numerically assess its security. This will require certain technical development of the multiplexed sources and mode selective homodyne detectors.

Another way the use of multimode states can help QKD implementations is discussed in Chapter 5. While mode multiplexing allows to enhance the QKD protocol performance if the modes can be successfully distinguished in the measurement, in case the mode-discriminating measurement is not available and all the modes are measured on a single homodyne detector, the multimode states can still be useful, as extra modes increase the signal brightness making it easier to handle in the experiment. The problem in the implementation may arise if the modes are not perfectly matched with the local oscillator on the balanced beam-splitter of the homodyne detector, the unmatched modes bring noise to the signal. This noise can be suppressed by increasing of the local oscillator intensity, as it was shown in proof-of-principle experiment described in Chapter 5. The extra noise destroys the security and decreases the secret key rate of the coherent state protocol we model with the help of the experimental data. We show that optimal state modulation and noise suppression by increasing local oscillator intensity improves the protocol performance. As a next step, full implementation of bright squeezed-state QKD protocol using parametric homodyne detectors recently developed at MPL Erlangen should be considered.

To conclude, mode multiplexing for quantum communication presents multiple challenges in practical implementation, this thesis tackles some of them, concentrating mainly on the inter-mode cross talk. In the future this general line of work can be further expanded in several directions, experimentally with the verification of the CV QKD protocol we modelled with frequency multiplexed source implementing physically mode separation and the channel between the protocol participants. When mode separation is efficiently implemented, the multimode structure of the state can be further used for advantage of multi-party QKD, where secure key distribution between the parties can be either controlled externally or by the users. Theoretically also the more complicated models of cross

talk (including more distant modes and possibly nonlinear interactions) can be considered if experimental practice will require it. The presented work is an essential step in development and implementation of efficient continuous-variable quantum communication with mode multiplexing towards large-capacity multi-user local secure networks.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[2] E. Schrodinger. Die gegenwartige situation in der quantenmechanik. *Die Naturwissenschaften*, 23(48):807–812, nov 1935.

[3] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14):938–941, apr 1972.

[4] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of bell's inequalities. *Physical Review Letters*, 49(2):91–94, jul 1982.

[5] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng. Realization of the einstein-podolsky-rosen paradox for continuous variables. *Physical Review Letters*, 68(25):3663–3666, jun 1992.

[6] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996.

[7] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, volume 175, page 9, Bangalore, India, 1984. IEEE.

[8] Yuemeng Chi, L Tian, B Qi, L Qian, and HK Lo. *High speed homodyne detector for gaussian-modulated coherent-state quantum key distribution*. University of Toronto, 2009.

[9] Yichen Zhang, Zhengyu Li, Ziyang Chen, Christian Weedbrook, Yijia Zhao, Xiangyu Wang, Chunchao Xu, Zhang Xiaoxiong, Zhenya Wang, Mei Li, Xueying Zhang, Ziyong Zheng, Binjie Chu, Xinyu Gao, Nan Meng, Weiwen Cai, Zheng Wang, Gan Wang, Song Yu, and Hong Guo. Continuous-variable qkd over 50 km commercial fiber. *Quantum Science and Technology*, 4:035006, 05 2019.

[10] Yichen Zhang, Ziyang Chen, Stefano Pirandola, Xiangyu Wang, Chao Zhou, Binjie Chu, Yijia Zhao, Bingjie Xu, Song Yu, and Hong Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Physical Review Letters*, 125(1):010502, jun 2020.

[11] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9, 05 2015.

[12] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.*, 118:060503, Feb 2017.

[13] J. Aasi, Judith Abadie, B. Abbott, R. Abbott, T. Abbott, Matthew Abernathy, C. Adams, Teneisha Adams, Paolo Addesso, C. Affeldt, Odylio Aguiar, P. Ajith, Bruce Allen, E. Ceron, D. Amariutei, S. Anderson, Warren Anderson, K. Arai, and John Zweizig. Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light. *Nature Photonics*, 7:613, 07 2013.

[14] Seth Lloyd and Samuel L. Braunstein. Quantum computation over continuous variables. *Phys. Rev. Lett.*, 82:1784–1787, Feb 1999.

[15] Olivier Pfister. Continuous-variable quantum computing in the quantum optical frequency comb. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 53(1):012001, nov 2019.

[16] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[17] Adeline Orieux and Eleni Diamanti. Recent advances on integrated quantum communications. *Journal of Optics*, 18(8):083002, jul 2016.

[18] J. Y. Zhang, G.and Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13(12):839–842, Dec 2019.

[19] Eleni Diamanti and Anthony Leverrier. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy*, 17, 06 2015.

[20] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63(5):052311, apr 2001.

[21] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, Jan 2001.

[22] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002.

[23] Christian Weedbrook, Andrew M Lance, Warwick P Bowen, Thomas Symul, Timothy C Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical Review Letters*, 93(17):170504, 2004.

[24] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, May 2018.

[25] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012.

[26] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Reply to 'discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nature Photonics*, 9(12):773–775, Dec 2015.

[27] Vladyslav C. Usenko and Radim Filip. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A*, 81:022318, Feb 2010.

[28] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A*, 86:022318, Aug 2012.

[29] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A*, 83:042312, Apr 2011.

[30] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[31] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[32] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560:27–32, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[33] Jason Pereira and Stefano Pirandola. Hacking alice's box in continuous-variable quantum key distribution. *Phys. Rev. A*, 98:062319, Dec 2018.

[34] Ivan Derkach, Vladyslav C. Usenko, and Radim Filip. Continuous-variable quantum key distribution with a leakage from state preparation. *Physical Review A*, 96(6):062309, dec 2017.

[35] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343, 2010.

[36] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109:100502, Sep 2012.

[37] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J Cerf. Security of continuous-variable quantum key distribution against general attacks. *Physical Review Letters*, 110(3):030502, 2013.

[38] Stefano Pirandola. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.*, 3:043014, Oct 2021.

[39] Duan Huang, Peng Huang, Dakai Lin, Chao Wang, and Guihua Zeng. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Optics Letters*, 40(16):3695, aug 2015.

[40] Xiaoxiong Zhang, Yichen Zhang, Zhengyu Li, Song Yu, and Hong Guo. 1.2-ghz balanced homodyne detector for continuous-variable quantum information technology. *IEEE Photonics Journal*, 10(5):1–10, 2018.

[41] C.A. Brackett. Dense wavelength division multiplexing networks: principles and applications. *IEEE Journal on Selected Areas in Communications*, 8(6):948–964, 1990.

[42] Peter Winzer. Making spatial multiplexing a reality. *Nature Photonics*, 8, 04 2014.

[43] René-Jean Essiambre and Robert W. Tkach. Capacity trends and limits of optical communication networks. *Proceedings of the IEEE*, 100(5):1035–1055, 2012.

[44] Guilherme B. Xavier and Gustavo Lima. Quantum information processing with space-division multiplexing optical fibres. *Communications Physics*, 3(1):9, Jan 2020.

[45] Tobias A. Eriksson, Benjamin J. Puttnam, Georg Rademacher, Ruben S. Luís, Mikio Fujiwara, Masahiro Takeoka, Yoshinari Awaji, Masahide Sasaki, and Naoya Wada. Crosstalk impact on continuous variable quantum key distribution in multicore fiber transmission. *IEEE Photonics Technology Letters*, 31(6):467–470, 2019.

[46] S Sarmiento, S Etcheverry, J Aldama, I H López, L T Vidarte, G B Xavier, D A Nolan, J S Stone, M J Li, D Loeber, and V Pruneri. Continuous-variable quantum key distribution over a 15 km multi-core fiber. *New Journal of Physics*, 24(6):063011, jun 2022.

[47] François Roumestan, Amirhossein Ghazisaeidi, Haik Mardoyan, Jérémie Renaudier, Eleni Diamanti, and Philippe Grangier. 6 mb/s secret key rate transmission over 13.5 km smf using pcs-256qam super-channel continuous variable quantum key distribution. In *Optical Fiber Communication Conference (OFC) 2022*, page Tu3I.4. Optica Publishing Group, 2022.

[48] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution over multicore fiber. *Opt. Express*, 24(8):8081–8087, Apr 2016.

[49] Weiwen Kong, Yongmei Sun, Yaoxian Gao, and Yuefeng Ji. Coexistence of quantum key distribution and optical communication with amplifiers over multicore fiber. *Nanophotonics*, 12(11):1979–1994, 2023.

[50] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, 04 2017.

[51] Fei Li, Hai Zhong, Yijun Wang, Ye Kang, Duan Huang, and Ying Guo. Performance analysis of continuous-variable quantum key distribution with multi-core fiber. *Applied Sciences*, 8:1951, 10 2018.

[52] Nicolas C. Menicucci, Steven T. Flammia, and Olivier Pfister. One-way quantum computing in the optical frequency comb. *Phys. Rev. Lett.*, 101:130501, Sep 2008.

[53] Jonathan Roslund, Renné Medeiros De Araujo, Shifeng Jiang, Claude Fabre, and Nicolas Treps. Wavelength-multiplexed quantum networks with ultrafast frequency combs. *Nature Photonics*, 8(2):109, 2014.

[54] Y Cai, J Roslund, G Ferrini, F Arzani, X Xu, C Fabre, and Nicolas Treps. Multimode entanglement in reconfigurable graph states using optical frequency combs. *Nature Communications*, 8:15645, June 2017.

[55] William N. Plick, Francesco Arzani, Nicolas Treps, Eleni Diamanti, and Damian Markham. Violating bell inequalities with entangled optical frequency combs and multipixel homodyne detection. *Phys. Rev. A*, 98:062101, Dec 2018.

[56] A. Gatti, R. Zambrini, M. San Miguel, and L. A. Lugiato. Multiphoton multimode polarization entanglement in parametric down-conversion. *Phys. Rev. A*, 68:053807, Nov 2003.

[57] Timur Iskhakov, Maria V Chekhova, and Gerd Leuchs. Generation and direct detection of broadband mesoscopic polarization-squeezed vacuum. *Physical Review Letters*, 102(18):183602, 2009.

[58] Christoph Simon and Dik Bouwmeester. Theory of an entanglement laser. *Phys. Rev. Lett.*, 91:053601, Aug 2003.

[59] Timur Sh Iskhakov, Ivan N Agafonov, Maria V Chekhova, and Gerd Leuchs. Polarization-entangled light pulses of 10 5 photons. *Physical Review Letters*, 109(15):150502, 2012.

[60] R. J. Sewell, N. Behbood, G. Colangelo, F. Martin Ciurana, G. Tóth, and M. W. Mitchell. Generation of long-range entanglement in a macroscopic spin singlet. In *2015 European Conference on Lasers and Electro-Optics - European Quantum Electronics Conference*. Optica Publishing Group, 2015.

[61] Vladyslav C Usenko, Laszlo Ruppert, and Radim Filip. Entanglement-based continuous-variable quantum key distribution with multimode states and detectors. *Physical Review A*, 90(6):062326, 2014.

[62] Vladyslav C Usenko, Laszlo Ruppert, and Radim Filip. Quantum communication with macroscopically bright nonclassical states. *Optics Express*, 23(24):31534–31543, 2015.

[63] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[64] Roy J. Glauber. Coherent and incoherent states of the radiation field. *Phys. Rev.*, 131:2766–2788, Sep 1963.

[65] Leonard Mandel and Emil Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[66] Michael M Wolf, Geza Giedke, and J Ignacio Cirac. Extremality of gaussian quantum states. *Physical Review Letters*, 96(8):080502, 2006.

[67] Ulrik L Andersen, Tobias Gehring, Christoph Marquardt, and Gerd Leuchs. 30 years of squeezed light generation. *Physica Scripta*, 91(5):053001, apr 2016.

[68] Roman Schnabel. Squeezed states of light and their applications in laser interferometers. *Physics Reports*, 684:1–51, 2017. Squeezed states of light and their applications in laser interferometers.

[69] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley. Observation of squeezed states generated by four-wave mixing in an optical cavity. *Phys. Rev. Lett.*, 55:2409–2412, Nov 1985.

[70] C.W. Gardiner and C.M. Savage. A multimode quantum theory of a degenerate parametric amplifier in a cavity. *Optics Communications*, 50(3):173–178, 1984.

[71] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.

[72] Ling-An Wu, H. J. Kimble, J. L. Hall, and Huifa Wu. Generation of squeezed states by parametric down conversion. *Phys. Rev. Lett.*, 57:2520–2523, Nov 1986.

[73] Henning Vahlbruch, Moritz Mehmet, Karsten Danzmann, and Roman Schnabel. Detection of 15 db squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency. *Phys. Rev. Lett.*, 117:110801, Sep 2016.

[74] C. F. Lo and R. Sollie. Generalized multimode squeezed states. *Phys. Rev. A*, 47:733–735, Jan 1993.

[75] Samuel L Braunstein and Peter Van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513, 2005.

[76] A.S. Holevo and O. Hirota. Quantum gaussian channels. In *2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060)*, pages 277–, 2000.

[77] Alessio Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. 07 2017.

[78] Arvind, Biswadeb Dutta, N. Mukunda, and R. Simon. The real symplectic groups in quantum mechanics and optics. *Pramana*, 45:471–497, 1995.

[79] R Simon, Shashi Chaturvedi, and V. Srinivasan. Congruences and canonical forms for a positive matrix: Application to the schweinler-wigner extremum principle. *Journal of Mathematical Physics*, 40, 12 1998.

[80] Julien Laurat, Gaëlle Keller, José Augusto Oliveira-Huguenin, Claude Fabre, Thomas Coudreau, Alessio Serafini, Gerardo Adesso, and Fabrizio Illuminati. Entanglement of two-mode gaussian states: characterization and experimental production and manipulation. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(12):S577, nov 2005.

[81] Horace P. Yuen and Vincent W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8(3):177–179, Mar 1983.

[82] A Luis and J Perina. Generalized measurements in eight-port homodyne detection. *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B*, 8(4):873, aug 1996.

[83] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7):535–552, October 2003.

[84] Yijun Wang, Yiyu Mao, Wenti Huang, Duan Huang, and Ying Guo. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express*, 27(18):25314–25329, Sep 2019.

[85] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A*, 88:022339, Aug 2013.

[86] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A*, 87:062313, Jun 2013.

[87] I Suleiman, J A H Nielsen, X Guo, N Jain, J Neergaard-Nielsen, T Gehring, and U L Andersen. 40 km fiber transmission of squeezed light measured with a real local oscillator. *Quantum Science and Technology*, 7(4):045003, jul 2022.

[88] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2726–2729, Mar 2000.

[89] Lu-Ming Duan, Geza Giedke, J. Cirac, and P Zoller. Inseparability criterion for continuous variable systems. *Physical review letters*, 84:2722–5, 04 2000.

[90] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996.

[91] Katharina Schwaiger and Barbara Kraus. Relations between bipartite entanglement measures. *Quantum Information and Computation*, 18, 01 2017.

[92] Gerardo Adesso and Fabrizio Illuminati. Bipartite and multipartite entanglement of gaussian states. *arXiv preprint arXiv:quant-ph/0510052*, 11 2005.

[93] Ludovico Lami, Alessio Serafini, and Gerardo Adesso. Gaussian entanglement revisited. *New Journal of Physics*, 20(2):023030, feb 2018.

[94] Gerardo Adesso, Alessio Serafini, and Fabrizio Illuminati. Extremal entanglement and mixedness in continuous variable systems. *Phys. Rev. A*, 70:022318, Aug 2004.

[95] M. B. Plenio. Logarithmic negativity: A full entanglement monotone that is not convex. *Phys. Rev. Lett.*, 95:090503, Aug 2005.

[96] Masato Koashi. On the irreversibility of measurements of correlations. *Journal of Physics: Conference Series*, 143(1):012007, jan 2009.

[97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, oct 1997.

[98] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[99] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 9 2005. Available at http://arxiv.org/abs/quant-ph/0512258.

[100] Michael Ben-Or, Michał Horodecki, Debbie W Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Theory of Cryptography*, pages 386–406, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[101] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006, aug 2009.

[102] Gilles Assche. *Quantum Cryptography and Secret-Key Distillation*. 01 2006.

[103] László Ruppert, Vladyslav C. Usenko, and Radim Filip. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Physical Review A*, 90(6):062310, 2014.

[104] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *Physical Review Letters*, 114(7):070501, 2015.

[105] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 120:220505, Jun 2018.

[106] Bing-Ze Yan, Qiong Li, Hao-Kun Mao, Hong-Wei Xu, and Ahmed A. Abd El-Latif. Large-scale and high-speed fpga-based privacy amplification for quantum key distribution. *Journal of Lightwave Technology*, 41(1):169–175, 2023.

[107] Xiaolong Su, Wenzhe Wang, Yu Wang, Xiaojun Jia, Changde Xie, and Kunchi Peng. Continuous variable quantum key distribution based on optical entangled states without signal modulation. *EPL (Europhysics Letters)*, 87(2):20005, jul 2009.

[108] Lars S Madsen, Vladyslav C Usenko, Mikael Lassen, Radim Filip, and Ulrik L Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nature Communications*, 3:1083, 2012.

[109] Ning Wang, Shanna Du, Wenyuan Liu, Xuyang Wang, Yongmin Li, and Kunchi Peng. Long-distance continuous-variable quantum key distribution with entangled states. *Phys. Rev. Appl.*, 10:064028, Dec 2018.

[110] Alexander Holevo and Reinhard Werner. Evaluating capacities of bosonic gaussian channels. *Physical Review A*, 03, 2001.

[111] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[112] Xiangyu Wang, Yichen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.049167*, 03 2017.

[113] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. 05 2002.

[114] Spyros Tserkis and Timothy C. Ralph. Quantifying entanglement in two-mode gaussian states. *Phys. Rev. A*, 96:062338, Dec 2017.

[115] Miguel Navascués, Frédéric Grosshans, and Antonio Acin. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97(19):190502, 2006.

[116] Raul Garcia-Patron and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):190503, 2006.

[117] Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard Werner, and Roman Schnabel. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nature Communications*, 6:8795, 10 2015.

[118] Frédéric Grosshans and Nicolas J. Cerf. Continuous-variable quantum cryptography is secure against non-gaussian attacks. *Phys. Rev. Lett.*, 92:047905, Jan 2004.

[119] Anthony Leverrier and Philippe Grangier. Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, 81, 06 2010.

[120] Fabian Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A*, 90:042325, Oct 2014.

[121] Nedasadat Hosseinidehaj, Nathan Walk, and Timothy C. Ralph. Optimal realistic attacks in continuous-variable quantum key distribution. *Phys. Rev. A*, 99:052336, May 2019.

[122] Renato Renner and J Ignacio Cirac. De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102(11):110504, 2009.

[123] Anthony Leverrier. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Physical Review Letters*, 118(20):200501, 2017.

[124] B Kraus, Nicolas Gisin, and R Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical review letters*, 95:080501, 09 2005.

[125] Chun Cai, Yongmei Sun, Yongrui Zhang, Peng Zhang, Jianing Niu, and Yuefeng Ji. Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber. *Opt. Express*, 27(4):5125–5135, Feb 2019.

[126] Olivier Pinel, Pu Jian, Renné Medeiros De Araujo, Jinxia Feng, Benoît Chalopin, Claude Fabre, and Nicolas Treps. Generation and characterization of multimode quantum frequency combs. *Physical Review Letters*, 108(8):083601, 2012.

[127] 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, May 2014.

[128] Yin Cai. *Quantum coherent control with an optical frequency comb.* Theses, Ecole normale supérieure - ENS PARIS ; East China normal university (Shanghai), October 2015.

[129] Yin Cai, Yu Xiang, Yang Liu, Qiongyi He, and Nicolas Treps. Versatile multipartite Einstein-Podolsky-Rosen steering via a quantum frequency comb. *Physical Review Research*, 2(3):032046(R), aug 2020.

[130] Ivan Derkach, Vladyslav C. Usenko, and Radim Filip. Preventing side-channel effects in continuous-variable quantum key distribution. *Physical Review A*, 93(3):032309, mar 2016.

[131] Nitin Jain, Ivan Derkach, Hou-Man Chin, Radim Filip, Ulrik L Andersen, Vladyslav C Usenko, and Tobias Gehring. Modulation leakage vulnerability in continuous-variable quantum key distribution. *Quantum Science and Technology*, 6(4):045001, aug 2021.

[132] Takuya Kudo and Takaaki Ishigure. Analysis of interchannel crosstalk in multimode parallel optical waveguides using the beam propagation method. *Optics Express*, 22(8):9675–9686, 2014.

[133] Lukasz Szostkiewicz, Marek Napierala, Anna Ziolowicz, Anna Pytel, Tadeusz Tenderenda, and Tomasz Nasilowski. Cross talk analysis in multicore optical fibers by supermode theory. *Optics Letters*, 41(16):3759–3762, 2016.

[134] Badraoui Nada and Tibor Berceli. Crosstalk reduction in fiber links using double polarization. *Optical and Quantum Electronics*, 52, 03 2020.

[135] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[136] Richard H. Byrd, Peihuang Lu, Jorge Nocedal, and Ciyou Zhu. A limited-memory algorithm for bound constrained optimization. *SIAM Journal on Scientific Computing*, 16:1190–1208, 1994.

[137] Philip R Bevington and D Keith Robinson. *Data reduction and error analysis for the physical sciences; 3rd ed.* McGraw-Hill, New York, NY, 2003.

PALACKY UNIVERSITY OLOMOUC
FACULTY OF SCIENCE

Department of Optics

Summary of thesis

Multiplexed quantum optical communication using multimode entangled states

Olena Kovalenko

Study program: Physics, P1701
Study program: Optics and Optoelectronics, 1701V029

Supervisor: prof. Mgr. Radim Filip, Ph.D.
Consultant: Dr. Vladyslav C. Usenko Ph.D.

Olomouc 2023

Title:	Multiplexed quantum optical communication using multimode entangled states
Author:	Olena Kovalenko
Supervisor:	Prof. Mgr. Radim Filip, Ph.D.
Co-supervisor:	Dr. Vladyslav C. Usenko Ph.D.
Study progamme:	Optics and Optoelectronics
Institution:	Department of Optics, Faculty of Science, Palacký University Olomouc
Reviewers:	_____
	_____
	_____
	_____

I hereby declare that my thesis titled **"Multiplexed quantum optical communication using multimode entangled states"** have been composed solely by myself under the guidance of my supervisor prof. Mgr. Radim Filip, Ph.D. and my PhD consultant Dr. Vladyslav C. Usenko Ph.D. This thesis has not been previously submitted for a degree or diploma at any other higher education institution. I agree with the further usage of this thesis in accordance with the requirements of Palacky University and the Department of Optics.

My thesis is available at the study department of the Faculty of Science, Palacký University, 17. listopadu 12, Olomouc, and also online at stag.upol.cz.

Abstract

This thesis deals with the task of improvement of existing quantum communication protocols using multimode entangled states. Firstly, we consider the mode-multiplexing in entanglement distribution and quantum key distribution. Mode-multiplexing allows to improve performance and increase capacities of quantum communication protocols, in this case each mode carries separate signal and should be handled and measured separately. Unfortunately while improving protocols capacities, multi-mode structure of quantum signal can also introduces new imperfections, such as the intramode cross talk. We study effects of the cross talk and the ways to compensate it. We then test one of the suggested methods to compensate for the cross talk in an experimental source of frequency-multiplexed entangled light. We model the quantum key distribution protocol using this frequency multiplexed source and demonstrate how the cross talk compensation method improves the secure key.

The other side of multimode state use, we study is the application of multimode bright states of light in quantum communication, in this case the modes are not discriminated in the measurement, the protocol does not use them for multiplexing, but instead multiple modes make the signal brighter and easier to work with in experimental implementation.

Key words

Quantum communication, quantum key distribution, entanglement, continuous variables, Gaussian states, entangled states of light.

Contents

1 Introduction

This report gives a brief summary of the main results of my thesis "Multiplexed quantum optical communication using multimode entangled states". While quantum entanglement as a phenomenon was discovered almost a century ago, the technology employing it for quantum communication is still ongoing its development stage. One of the ways to improve communication protocols is to allow transfer of several entangled states simultaneously by multiplexing the channels. Quantum communication and, more narrowly, mode-multiplexing in quantum communication is a vast field of research, this work concentrates on several use-cases. We theoretically study application of multimode Gaussian states of light for scalability improving efficiency of quantum key distribution (QKD) and of Gaussian entanglement distribution, that has its application in QKD, in quantum teleportation and in the future, in distributed quantum computing. Mode multiplexing allows to increase channel capacities, which is essential for practical implementations of the the protocols.

The thesis aims at studying and removing the problems and limitations that can arise while implementing multiplexed CV entanglement distribution and QKD protocols using multimode entangled states, at developing methods to overcome these limitations and, to extent possible with the available experiments, at testing these methods on the experimental data. This work was conducted during my Ph.D. studies at Palacky University in Olomouc and

this thesis is based on 3 articles published in peer-reviewed and impacted journals (Photonics research and Optics Express) during the course of my study.

Firstly, in Chapter 1 we introduce theoretical concepts the most crucial this thesis. Chapter 2 concerns the theoretical model of the entanglement distribution in the presence of cross talk. We suggest a way to compensate the cross talk and restore entanglement with the help of optimized interference. Then we proceed comparing the suggested compensation method to another one that traces out some modes while enhances the entanglement of the other modes. In Chapter 3 we describe a result of experimental-theoretical collaboration, where we implement the proposed compensation method numerically to eliminate the cross talk in the experimentally measured frequency multiplexed entangled state. We then model the CV QKD protocol using the multiplexed state, showing how the optimal postprocessing successfully eliminated the cross talk and, hence increased the secure distance of the QKD protocol. Chapter 4 concerns another experimental-theoretical collaboration. We model CV QKD protocol with macroscopically bright coherent state, the bright state contains multiple modes that are measured with a mode-non-discriminating measurement. Using the data from the proof-of principle experiment we show how the noise coming from the imperfect mode-matching can be suppressed and the secure key restored. Finally in Chapter 4 we give the summary of the main results, conclusions and outlook for future work.

2 Methods

The continuous-variable (CV) states of light are characterized by the conjugate quadratures of electromagnetic field, $\hat{x} = \hat{a}^\dagger - \hat{a}$ or $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, in analogy to oscillator's position and momentum operator.

Gaussian states are fully characterised by its first statistical moments (displacements) and matrix of second statistical moments [1]. Important nonclassical Gaussian bipartite states, widely employed in quantum communication (and in this work), are two-mode squeezed vacuum states (TMSV) [2]. TMSV has zero mean displacement and covariance matrix

$$\gamma_{AB} = \begin{pmatrix} V\ \mathbb{I} & \sqrt{V^2-1}\ \mathbb{Z} \\ \sqrt{V^2-1}\ \mathbb{Z} & V\ \mathbb{I} \end{pmatrix}, \tag{2.1}$$

here $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity matrix, $\mathbb{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is a Pauli Z matrix. Covariance matrix of N-mode Gaussian states, is a $2N \times 2N$ matrix with elements $\gamma_{ij} = \langle r_i r_j \rangle$, where $r_i = \{x_i, p_j\}$, $i \in [1, 2N]$.

In this thesis, we consider only bipartite entanglement and the task of multiplexing of bipartite entanglement. It is necessary, although not sufficient, resource for many of quantum communication applications, in particular for QKD.

As an operational measure of bipartite Gaussian entanglement

that quantifies negativity of partial transpose we use logarithmic negativity (LN) [3].

$$LN_i = \max\{0, \log_2 ||\rho^{\Gamma_p}||_1\}, \tag{2.2}$$

where $||\rho||_1 = \mathrm{Tr}\sqrt{\rho\rho^\dagger}$ is a trace norm. ρ^{Γ_p} signifies partial transpose of the state ρ. The logarithmic negativity of Gaussian states can be expressed in terms of symplectic eigenvalues

$$LN_i = \max\{0, -\log_2 \nu_-\}, \tag{2.3}$$

where ν_- is the smallest symplectic eigenvalue of the covariance matrix of the partially transposed state.

We are interested in the communication protocols where two parties A and B aim to distribute a multimode entangled state. The

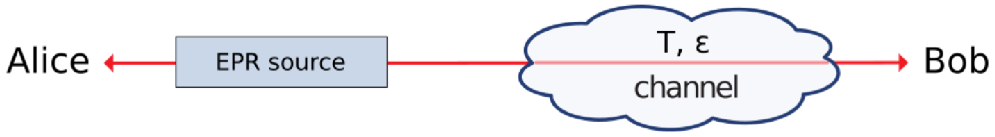

Figure 2.1: Basic one-way entanglement distribution protocol

simplest Gaussian entanglement distribution protocol is described by the scheme given in Fig. 2.1. One party (Alice) possesses a source of TMSV states, she shares it with the remote party (Bob) through a quantum channel that introduces loss and adds noise to the shared state. The parties have additional free access to classical communication channel and can perform other operations locally in each lab (including Gaussian measurements), i.e. only local operations and classical communication (LOCC) can be performed on the shared state. The noiseless channel with constant transmittance T can be modeled as a simple beam-splitter interaction that couples one of the modes of the signal to a vacuum state. The channel also adds excess noise ε to the second quadrature moments. Entanglement distribution implementation is essential part of many quantum technologies, in quantum teleportation [4], in quantum

random number generation [5], for quantum-enhanced sensing [6], it can be employed in quantum key distribution for entanglement-based protocols.

Gaussian CV quantum key distribution (QKD) employs continuous-variable states (squeezed and coherent) and coherent homodyne or heterodyne detection [7]. It can be implemented with well developed and easily accessible optical technologies [8] The task of QKD is to generate information-theoretic secure one-time pad for two distant trusted authenticated parties in presence of malicious eavesdropper with unlimited abilities bounded only by laws of physics. Traditionally the parties are referred to as Alice (sender) and Bob (receiver), and Eve (the eavesdropper). Alice and Bob share quantum states through a quantum channel that is considered to be fully controlled by the eavesdropper, and classical communication is happening openly through an authenticated classical channel. The goal of eavesdropper is to get a copy of the key while not bringing in enough noise into state for trusted parties to notice and terminate the protocol.

To evaluate the security of QKD protocol we have to evaluate lower bound of the secure key rate. Assuming that sides can use protocol infinite number of times (asymptotic limit), Devetak-Winter bound [9] gives the asymptotic secret key rate.

$$K = \max\{0, \beta I_{AB} - \chi_{BE}\} \tag{2.4}$$

here I_{AB} is the classical (Shannon) mutual information shared between Alice and Bob; χ_{BE} is Holevo bound [10] (upper bound on information between eavesdropper and the reference side of the protocol) for Gaussian state with covariance matrix γ_E; $\beta \in [0, 1]$ is postprocessing efficiency, it depends on error correction algorithm used in classical postprocessing, in practice it can be close to 0.96 [11] for Gaussian (or nearly Gaussian) data sets. Holevo bound on information available to Eve is calculated with the assumption that she is capable of collective measurement of the states leaked to her through the noisy attenuating quantum

channel [12]. It is calculated as difference of quantum information (von Neumann entropy) of the state prior and after measurement by Bob: $\chi_{BE} = S(\gamma_E) - S(\gamma_{E|B})$, here $S(\gamma)$ von Neumann entropy of a state with covariance matrix γ, it is calculated as $S(E) = \sum_i \mathrm{G}\,\frac{\lambda_i - 1}{2}$, where λ_i are symplectic eigenvalues of γ_E and $\mathrm{G}(x) = (x+1)\log_2(x+1) - x\log_2 x$.

To assess security of QKD protocol against collective attacks [13–15] we have to assume that Eve holds purification of the state. It is shown for the Gaussian protocols considered in this thesis, that security against collective attacks also implies security against general attacks in the asymptotic limit [16]. Assuming that the tripartite state shared between Alice, Bob and Eve is pure (i.e. eavesdropper holds purification of the state), the bound on Eve's information becomes $\chi_{BE} = \chi_{AB} = S(\gamma_{AB}) - S(\gamma_{A|B})$.

3 Cross talk compensation for multimode entanglement distribution

Preparing and distributing multiplexed entangled states with significant number of modes almost inevitably leads to cross talk between the modes [17–20]. We use a significantly simplified model of linear cross talk in distribution of two TMSV states to demonstrate possibility to compensate its negative effects with local manipulations of data on one of the sides of communication protocol. This data processing uses advantageous properties of continuous variable states and measurements that has no known analogy with single photon DV QKD.

We model a four-mode CV entanglement distribution scheme that consists of two TMSV states Fig. 3.1. We assume that cross talk, characterized by the linear coupling t_c, occurs between two of the signal modes B_1B_2 prior to them being transmitted through an attenuating quantum channel. Two of the modes B_1B_2 are shared over lossy and noisy channels with transmittance T_i for an i-th mode and with channel excess noise ε added to all the modes.

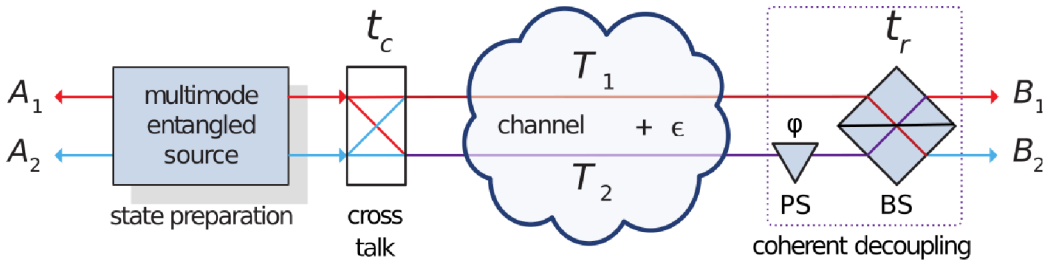

Figure 3.1: Entanglement distribution scheme with two pair of TMSV states, where cross talk is modeled as a beam-splitter of transmittance t_c. The cross talk is compensated with optical interference, when the remote side optimally applies phase shift (PS) by π to one of the modes and couples the signal modes on a variable coupler t_r.

The 8x8 covariance matrix of the shared state with cross talk is

$$\gamma_{A_1A_2B_1B_2} = \begin{pmatrix} V\,\mathbb{I} & \sqrt{t_cT_1}\sqrt{V^2-1}\,\mathbb{Z} & 0 & -\sqrt{r_cT_2}\sqrt{V^2-1}\,\mathbb{Z} \\ \sqrt{t_cT_1}\sqrt{V^2-1}\,\mathbb{Z} & [T_1(V+\varepsilon-1)+1]\,\mathbb{I} & \sqrt{r_cT_2}\sqrt{V^2-1}\,\mathbb{Z} & 0 \\ 0 & \sqrt{r_cT_1}\sqrt{V^2-1}\,\mathbb{Z} & V\,\mathbb{I} & \sqrt{t_cT_2}\sqrt{V^2-1}\,\mathbb{Z} \\ -\sqrt{r_cT_1}\sqrt{V^2-1}\,\mathbb{Z} & 0 & \sqrt{t_cT_2}\sqrt{V^2-1}\,\mathbb{Z} & [T_2(V+\varepsilon-1)+1]\,\mathbb{I} \end{pmatrix} \tag{3.1}$$

here $r_c \equiv 1 - t_c$, $\mathbb{I} = diag[1,1]$ is the unity matrix, $\mathbb{Z} = diag[1,-1]$.

Knowing $\gamma_{A_1A_2B_1B_2}$ we can evaluate logarithmic negativity for each pair of modes separately using Eq. (2.3). In the entanglement distribution scheme with cross talk in Fig. (3.1) the initial logarithmic negativity of one TMSV state, before any cross talk and the channel loss occurs, is

$$LN_0(V) = -\frac{1}{2}\log_2\left(2V^2 - 1 - 2V\sqrt{V^2-1}\right), \tag{3.2}$$

After taking into account the cross talk, the channel attenuation and the excess noise, the logarithmic negativity of the first mode A_1B_1 of the shared state with the covariance matrix $\gamma_{A_1A_2B_1B_2}$ in

Eq.(3.1) becomes

$$LN = -\frac{1}{2}\log_2\frac{1}{2}\Big(1+2T_i[\varepsilon+(V-1)(t_cV+t_c+1)]+ T_i^2(\varepsilon+V-1)^2+V^2-[1+V+T_i(\varepsilon+V-1)]\times \sqrt{T_i^2(\varepsilon+V-1)^2+(V-1)^2-2T_i(V-1)[\varepsilon-2t_c(V+1)+V-1]}\Big). \tag{3.3}$$

Without the cross talk the shared entanglement increases monotonously with the state variance and, in principle with the squeezing being unlimited, it can grow up to the repeaterless bound [21] of the entanglement distribution. In the limit of infinite state variance ($V \to \infty$) and no cross talk in the attenuating channel with excess noise the repeaterless bound depends not only on on T but also ε and becomes

$$\lim_{V\to\infty} LN = -\log_2\frac{1-T_i(1-\varepsilon)}{1+T_i}. \tag{3.4}$$

In the presence of cross talk the shared logarithmic negativity is not growing function of initial state variance anymore. With increase of the initial entanglement (or, equivalently, the state variance), the shared entanglement reaches its maximum and vanishes if the initial variance exceeds

$$V_{max} = \frac{1+t_c-\varepsilon}{1-t_c}. \tag{3.5}$$

As an example of application for the multiplexed entanglement distribution scheme in Fig. 3.1, we consider a scenario where each mode of the 4-mode entangled state shared by the remote parties is measured with balanced homodyne detectors, and then the parties proceed to establish the secret key among themselves, implementing multiplexed version of the entanglement-based CV QKD protocol [22]. The mutual information distributed between Alice and Bob by two pairs of modes is additive and the secure key rate Eq. (2.4)

becomes

$$K = \max\left\{0, \beta(I_{A_1B_1} + I_{A_2B_2}) - \chi_{B_1B_2E}\right\}. \tag{3.6}$$

Taking into account the assumption that eavesdropper holds purification of the total state, here

$$\chi_{B_1B_2E} = S(\gamma_{A_1A_2B_1B_2}) - S(\gamma_{A_1A_2B_1B_2|B_1B_2}).$$

By reducing or destroying the state's entanglement, cross talk also negatively influences the secure key rate. The analogy between the cross talk effects on the secure key and entanglement can be seen comparing Fig. 3.2 left and right panels. In both cases cross talk reduces both shared entanglement and the secure key rate and introduces limitations on the initial state variance.

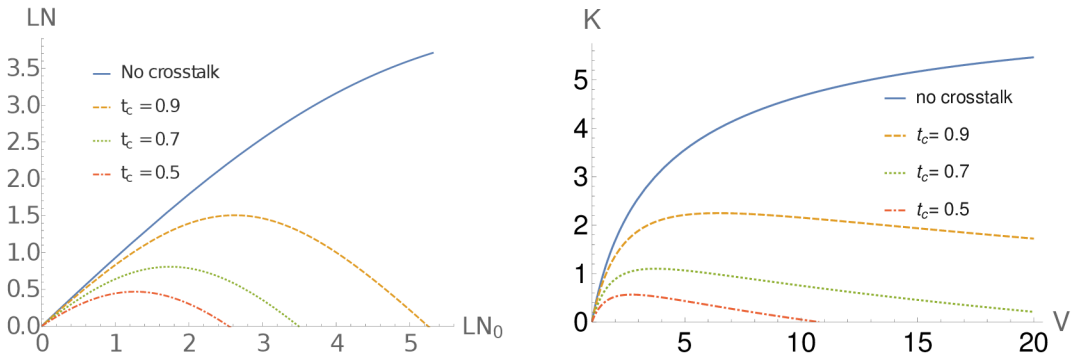

Figure 3.2: Secret key rate for multiplexed state γ_{A_1,A_2,B_1,B_2} with cross talk t_c after attenuation by channel with transmittance $T = 0.9$ versus the initial state variance V of the state (left) and versus the channel noise (right). Left: no excess noise $\varepsilon = 0$. Right: fixed signal state variance $V = 5$. Postprocessing efficiency $\beta = 0.96$.

The initial state variance could be optimized with respect to cross talk t_c and channel parameters T and ε. Depending if the goal is to maximize the logarithmic negativity or the secure key rate, the optimal initial state variance in general would differ. But even with the optimization, the damage done by the cross talk remains significant.

Linear cross talk we consider in our model should be possible to compensate by the linear interactions, combination of phase shifts and beam-splitters, similar to the method to combat correlations in quantum memory channels [23]. In a more complicated case with higher number of modes the most general compensating scheme would consist of a sequence of Mach-Zender interferometers, but for a simpler case of two TMSV states we only need a sequence of a phase shift by π on one mode with the modes B_1, B_2 then interacting on a beam-splitter with transmittance t_r, as shown in Fig. 3.1, here t_r is the parameter to be optimized.

Applying this decoupling interaction changes the covariance matrix of a pair A_1, B_1 to

$$\gamma_{A_1B_1} = \begin{pmatrix} V\ \mathbb{I} & \left(\sqrt{T_2 r_c r_r}+\sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\ \mathbb{Z} \\ \left(\sqrt{T_2 r_c r_r}+\sqrt{T_1 t_c t_r}\right)\sqrt{V^2-1}\ \mathbb{Z} & [1+T_1 t_r(V-1)+T_2 r_r(V-1)]\ \mathbb{I} \end{pmatrix}, \tag{3.7}$$

where $r_r \equiv 1 - t_r$. The pair of modes A_2, B_2 has similar covariance matrix up to the replacement of T_1 with T_2.

For a noiseless channel with balanced transmittance (same transmittance for both modes $T_1 = T_2 \equiv T$) it is straightforward to see that putting $t_r = t_c$ fully eliminates the cross talk from the covariance matrix in Eq. (3.7)

In general case the channel transmittance is unbalanced, i.e. it is different for different pairs of modes $T_1 \neq T_2$ (without loss of generality we assume $T_1 > T_2$), then the optimal t_r has to be found numerically. Its value is bound from below and above by two important edge cases of very weak and infinitely strong initial entanglement for the mode pair A_1, B_1

$$t_r^1 = \frac{T_1 t_c}{T_1 t_c + T_2(1-t_c)}, \quad V \sim 1 \tag{3.8}$$

and

$$t_r^\infty = \frac{T_2 t_c}{T_2 t_c + T_1(1-t_c)}, \quad V \to \infty. \tag{3.9}$$

Applying optimal coupling t_r allows to significantly restore en-

tanglement and to remove the limitations on the maximal initial variance V_{max} in Eq.(3.5). For optimally chosen t_r the logarithmic negativity is an increasing function of V. For infinitely large initial state variance and t_r given by (3.9) the logarithmic negativity approaches the limit:

$$\lim_{V\to\infty} LN_{rev} = -\log_2\left[\frac{t_c T_2 + T_1(1-t_c-T_2)}{t_c T_2 + T_1(1-t_c+T_2)}\right]. \tag{3.10}$$

The proposed decoupling method allows to almost fully restore the entanglement and eliminate the cross talk in both pairs of modes, but it depends on numerical optimization with respect to the generally unknown parameter t_r.

Further we consider an alternative way to compensate for entanglement loss (see Fig. 3.3), that relies on the conditional measurement of one pair of modes with feeding forward the measurement result to displace another pair of modes A_1, B_1. This method is similar to entanglement localization proposed by [24, 25]. This approach allows to increase entanglement in one pair of modes at the expense of completely losing the other pair, but it does not need any prior estimation of the cross talk strength.

On both sides Alice and Bob perform generalised homodyne measurement dividing the pair A_2, B_2 on beam-splitters of variable transmittances t_A and t_B respectively and then measuring both quadratures. t_A and t_B are the parameters to be optimized to maximize the logarithmic negativity. The optimal measurement of Bob's side does not depend on the state or channel parameters, it is always a homodyne measurement of either of the quadratures, the optimal t_B is either $t_B = 1$ for measurement of $\hat{x}$ or $t_B = 0$ for measurement of $\hat{p}$. Without loss of generality we further put $t_B = 1$. Optimal measurement on Alice's side does depend on the state variance V and the cross talk t_c, channel transmittance T_1 and T_2 and excess noise ε and in general case optimal t_A can only be found numerically. Independently of what kind of the generalized measurement is applied to the pair of modes A_2B_2 (and what t_A

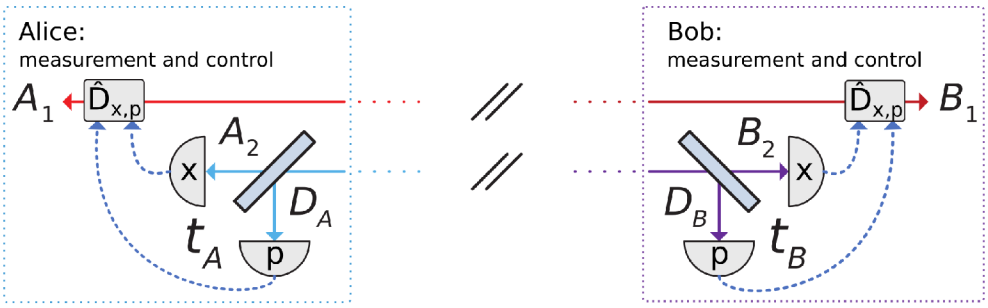

Figure 3.3: Measurement and feed-forward control scheme to compensate the cross talk in the pair of modes A_1, B_1. The two parties perform generalized Gaussian measurements by splitting modes A_2, B_2 on variable beam-splitters t_A, t_B and measuring x-quadratures on the modes A_2, B_2 and p-quadratures on the auxiliary detection modes D_A, D_B. The measurement outcomes are then used to feed-forward modes A_1, B_1. The rest of the scheme (source, cross talk and channel) is as in Fig. 3.1. The scheme allows increasing entanglement in modes A_1, B_1 at the cost of tracing out modes A_2, B_2.

and t_B are chosen), the measurement with feed forward always improves the entanglement in the pair A_1B_1.

In the limit of a very long channel with extremely high loss $T_{1,2} \to 0$ the optimal measurement is the balanced heterodyne detection with $t_A = 1/2$. The logarithmic negativity of the pair A_1, B_1 LN_{het} is a growing function of the state variance and in the limit of $V \to \infty$ and no excess noise ($\varepsilon = 0$) it asymptotically approaches

$$\lim_{V\to\infty} LN_{het} = -\frac{1}{2}\log_2\left[\frac{(1-t_cT_1)[1-t_c(T_1-T_2)-T_2]}{(1+t_cT_1)^2-(1-t_c)T_2(1-t_cT_1)}\right]. \tag{3.11}$$

All the proposed compensation methods are compared in Fig. 3.5 and3.4, demonstrating that all the compensation methods allow to significantly restore the Gaussian entanglement and the optimal interference method significantly restores the key rate. Comparison, how the entanglement in both pairs of modes is restored by

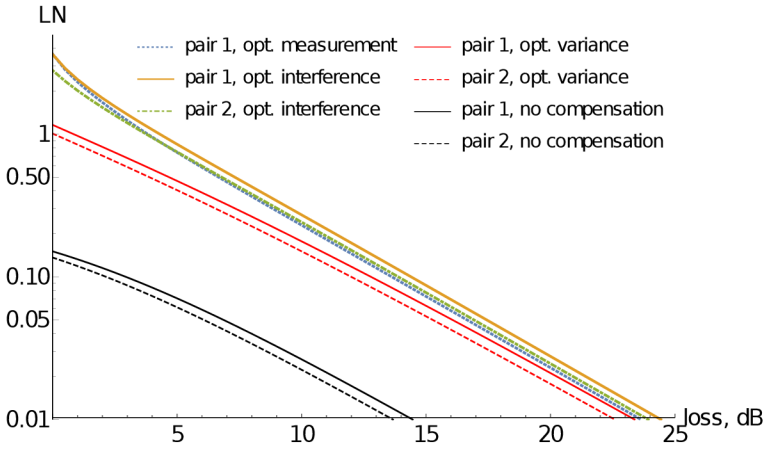

Figure 3.4: Comparing different ways of cross talk compensation: optical interference using a decoupling beam-splitter, and entanglement concentration by optimized conditional measurement and feed-forward control. Plot shows the logarithmic negativity in a pair of modes after each respective method is applied. Initial entanglement is fixed $LN_0 = 4.$, cross talk is $t_c = 0.8$, and transmittance ratio is $T_1/T_2 = 1.2$, parameters t_r and t_A are optimized. The ideal case without any cross talk is not shown, but would be indistinguishable from the optimized interference method for given parameters.

the different ways to compensate for cross talk, depending on the channel attenuation is given in Fig. 3.5. The passive method that implies the initial state variance optimization is the easiest to implement, it gives comparable results to the active methods, but only for high attenuation, it also does depend on the knowledge of the cross talk coupling t_c. The active compensation schemes always perform better, in particular the optimal interference, in case of its ideal implementation, beats all the other methods. The optimal interference also preserves all the modes intact, while relying on the correct choice of the parameter t_r, which can be challenging. While the measurement with the feed forward control halves the number of modes successfully distributed, but can be implemented without any knowledge of the strength of the cross talk t_c.

Depending on the applications this disadvantage can be crucial.

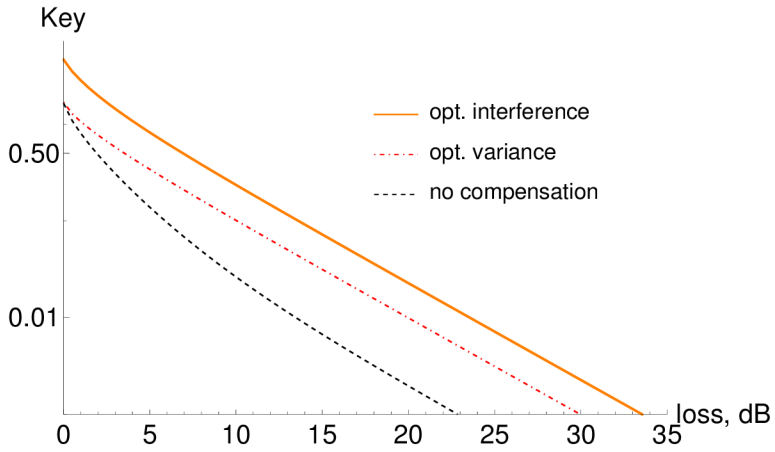

Figure 3.5: Different ways of cross talk compensation influencing the secret key rate for total state. Initial entanglement is fixed $LN_0 = 4.0$, cross talk is $t_c = 0.8$, and transmittance ratio is $T_1/T_2 = 1.2$, t_r is optimized. The compensation method using optimal measurement with feed forward is not applicable for QKD.

In QKD, where the mutual information in the pairs of modes is additive, the entanglement concentration method that traces out one of the mode pairs does not help to increase the key rate, but only deteriorates it further (except for the case of unrealistically strong cross talk). In Fig. 3.4 we demonstrate how the proposed optimal interference compensation method allows to restore the secret key rate in the multiplexed entanglement-based QKD scenario.

Summary. In the entanglement distribution scheme presence of the cross talk deteriorates entanglement and the secret key rate. Depending on channel parameters and cross talk strength the initial state variance could be optimized to maximize entanglement shared. The negative effects of cross talk can be at least partially compensated by either of two methods we suggest and compare here. Depending on the purpose of entanglement distribution, e.g. for entanglement-based QKD protocols, the physical implementation of the cross talk compensating schemes could be substituted with numerical data processing. In the following Chapter 4 we demonstrate applicability of numerical implementation of the opti-

mal interference method to compensate the cross talk in the experimental source with significantly more modes.

4 Compensating cross talk in frequency multiplexed entangled QKD source

In this Chapter we present the main results of the published paper, where we study a way to increase the performance of the entanglement based CV QKD protocol by mode-multiplexing of optical transmission channel in the frequency domain. We test the method on the experimental data, obtained using the SPOPO as a source of entangled states and the mode-discriminating homodyne detection. Using the experimental data we then model a multimode version of the entanglement-base CV QKD with homodyne detection. The cross talk between signal modes appears to be very strong, it deteriorates the secret key rate and negates benefits of multiplexing. We apply the multimode cross talk compensation method based on data manipulation, equivalent to linear state manipulations, similar to the optimized interference method suggested in previous Chapter. We evaluate security of resulting CV QKD protocol, confirming

the efficiency of cross talk compensation.

We model an EB CV QKD protocol using data from the experiment [26] with SPOPO as a source of frequency multiplexed entanglement and mode-discriminating homodyne detection that distinguishes 16-frequency bands. To generate the entangled light, a synchronously pumped optical parametric oscillator (SPOPO) including a 2-mm-thick BiB_3O_6 (BiBO) crystal, which operates below the threshold, was employed. The main laser is a Ti-sapphire pulse laser, with pulse 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 LO for mode-discriminating homodyne detection. The pump laser for the SPOPO (centered at $\lambda_0/2$) is prepared by second-harmonic generation of the main laser in a 0.2-mm-thick BiBO crystal.

In the actual experiment all 16 frequency modes are generated in a single beam, when we suggest the way to use it in the QKD protocol, we consider a scenario, as shown in Fig. 4.1, where half of the frequency modes are measured by Alice and the other half are distributed to Bob through pure loss channel. 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.

Optimized symplectic transformation we applied is equivalent to set of passive local operations on each side. The most general case would be a set of Mach-Zehnder interferometers acting on each possible combination of modes [27]. However, due to absence of the correlations between $\hat{x}$ and $\hat{p}$ quadratures no phase shifts can increase correlation (and, consequently, the mutual information) and

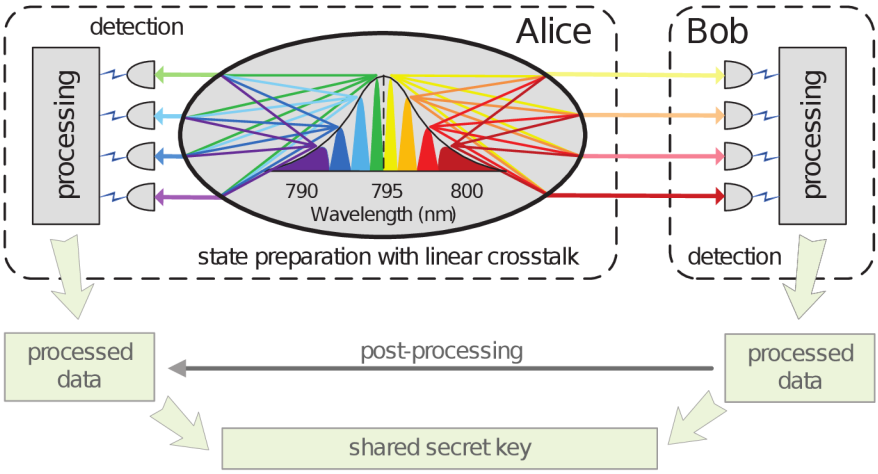

Figure 4.1: Bright colors show a sketch of a CV QKD test-bed for study of the multimode entangled source at the side of sender, Alice, with cross talk coupling between the frequency modes in both of the two beams, leaving the source. The entangled source is based on eight pairs of modes, here only four of them are shown for simplicity. The part of the CV-QKD protocol tested experimentally is given in bright colors, while the part, that is modelled theoretically, is given in dim colors.

a sequence of Mach-Zehnder interferometers simplifies to a sequence of beam-splitters between all possible pairwise mode permutations on each side. Optimal symplectic unitary operation is equivalent to a basis change and it cannot influence information that leaked to eavesdropper. Basis change does not influence Holevo bound on Eve's information. To maximize the key rate Eq.(2.4) it is therefore enough to maximize the mutual information. In the CV QKD protocol with homodyne detection only one quadrature can be chosen for the quantum key generation, we therefore consider $\hat{p}$ quadrature for the key.

We compare the secure key rate robustness to channel loss with the original experimental data and the data after optimal processing in Fig. 4.2. The optimized data manipulation has noticeably improved robustness to loss (and, respectively, increased the secure distance) of frequency-multiplexed CV QKD protocol, the tolera-

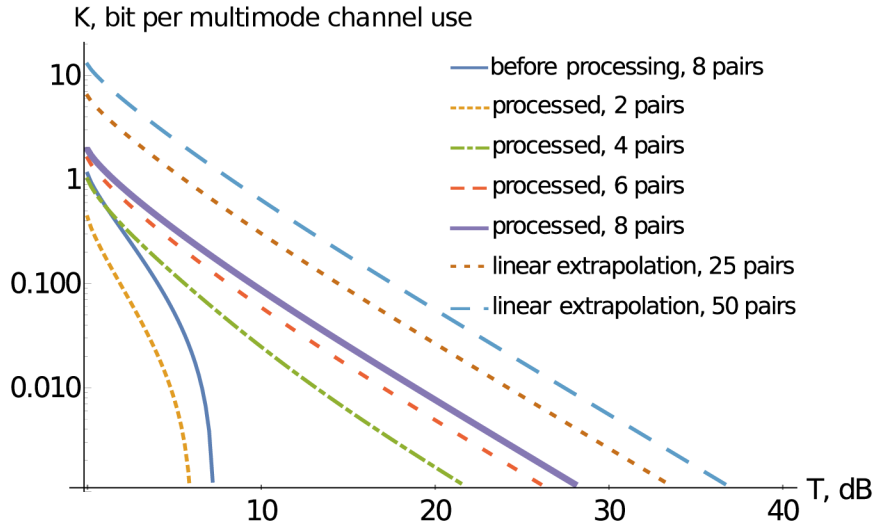

Figure 4.2: Key rate of CV QKD versus channel transmittance T (in dB) as obtained from the original data on the full multimode entangled state (blue solid line), after optimized local data manipulations performed by the trusted parties for different number of used pairs of modes (non-solid lines for 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 $\beta = 96\%$.

ble loss increased from 7.5 dB before processing (blue) to 28 dB (orange). To show how multimode nature of the source increases the key rate we also calculated the key rates for reduced states with only some modes used for the key generation and extrapolated it to the cases with significantly larger numbers of modes (dashed lines). Comparing the results for different number of modes and extrapolations suggests that increasing the number of frequency bands measured with mode-discriminating homodyne detection can further increase performance of the QKD protocol.

Summary. This work suggests SPOPO in prospect can be a useful source for implementation of frequency-multiplexed entanglement-based CV QKD protocols. During generation and measurement this source suffers from cross talk between different frequency modes that can be compensated by optimally applying data manip-

ulations in the postprocessing stage of the protocol. The optimal data processing allowed to increase the mutual information between the sets of modes on both sides, while the leaked information is not affected. We observed increase of protocol robustness to channel attenuation from about 7.5 dB to 28 dB.

5 | QKD with macroscopically bright coherent states of light

Besides channel multiplexing, when each mode carriers signal individually and has to be measured individually, multimode states can be used even in quantum communication scenarios without mode-discriminating measurement.Bright states containing multiple modes can be treated in an experiment as single-mode states of higher intensity. The possibility to implement entanglement-based QKD protocol with BSV was proposed earlier [28]. Here we present the main results of the published paper that considers a prepare-and-measure CV QKD protocol with bright coherent states, based on the results of the experimental test of their generation and detection.

Bright states are called so in the sense that they consist of multiple modes, making them easier to handle in practical QKD implementations. The downside of having multiple signal modes is that not all of them overlap successfully with the local oscillator during the homodyne measurement, hence creating additional noise. We

test the possibility to reduce the resulting noise and estimates the applicability of the bright states for CV QKD.

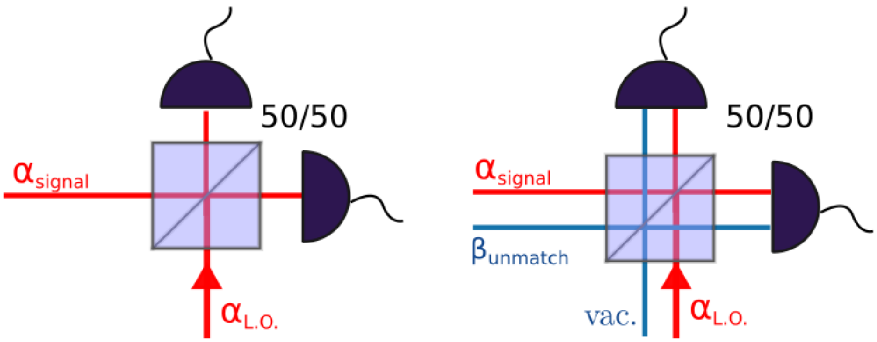

Figure 5.1: The standard scheme for homodyne detection (left) and the scheme with uncompensated modes in the multimode signal beam (right).

In regular homodyne detection in Fig. 5.1 (left) single-mode signal beam is mixed with single-mode local oscillator on the balanced beam-splitter, while in homodyne detection of bright states it is necessary to mix all modes of the signal state with the multimode local oscillator. In case the mode matching is imperfect, some signal modes do not match with the local oscillator modes, these unmatched modes mix with vacuum on the beam-splitter, adding extra noise to measurement results [28]. In Fig. (5.1 (right) we show the case with only two signal modes, one of which does not overlap with the local oscillator. The measured quadrature variance gains extra noise from the unmatched mode, let's name the matched mode $|\alpha\rangle$ and the unmatched one $|\zeta\rangle$, the measured quadrature variance becomes

$$Var\left(x\right)_{meas} = 1 + \frac{|\zeta|^2}{|\alpha_{LO}|^2}, \tag{5.1}$$

where $Var(x)$ is the quadrature variance of the matched signal modes (being $Var(x) = 1$ for pure coherent states), $|\zeta|^2$ is the mean number of photons in an unmatched signal mode, $|\alpha_{LO}|^2$ is the mean photon number of the LO.

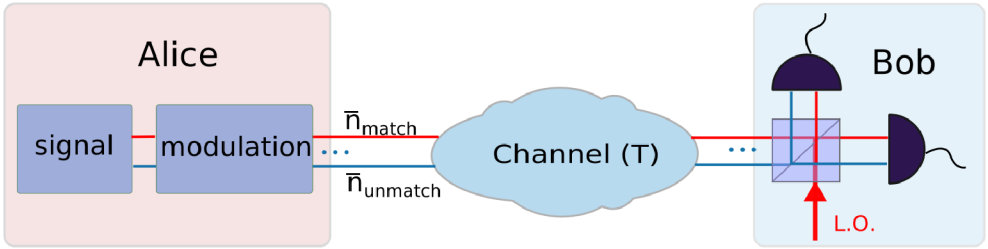

Figure 5.2: Operational scheme of prepare-and-measure CV QKD protocol using bright coherent states. Alice prepares bright coherent states and applies Gaussian modulation to them. She sends them (and local oscillator) through the attenuating quantum channel to Bob, who measures the signal with homodyne detection. The detection is assumed to be imperfect.

In the experiment performed by the group at MPL Erlangen (Prof. M. Chekhova) the homodyne detection with two modes one mutched and one unmatched was performed on coherent states. Based on the experimental data we consider a coherent state prepare-and-measure protocol described in Fig.5.2.

Initially Alice posses a bright coherent state with covariance matrix $\gamma^B_{coh} = \mathbb{I}$. After Alice applies modulation according to random variables she draws from two Gaussian distributions with zero mean, the covariance matrix of the state becomes that of a thermal state $\gamma^B_{coh} = \begin{pmatrix} V_m + 1 & 0 \\ 0 & V_m + 1 \end{pmatrix}$. The signal then travels through a quantum channel to a remote party Bob, who measures one of the signal quadratures with homodyne detection. The variance of the modulation has to be optimized depending on the channel parameters, attenuation T and excess noise V_N. The covariance matrix of the state shared through a channel for the the equivalent entanglement-based protocol used for security proof [29] is

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & \left[T(V+V_N)+1-T+\varepsilon^2_{tot}\overline{n}\right]\mathbb{I} \end{pmatrix}, \tag{5.2}$$

The secret key rate is calculated from the covariance matrix γ_{AB}

using Eq. (2.4). The presence of unmatched modes brings extra noise to the results of Bob's homodyne measurement. The security proof assumes that the eavesdropper purifies the state, forcing to attribute any noise to the eavesdropper's interference and lowering the secure key rate.

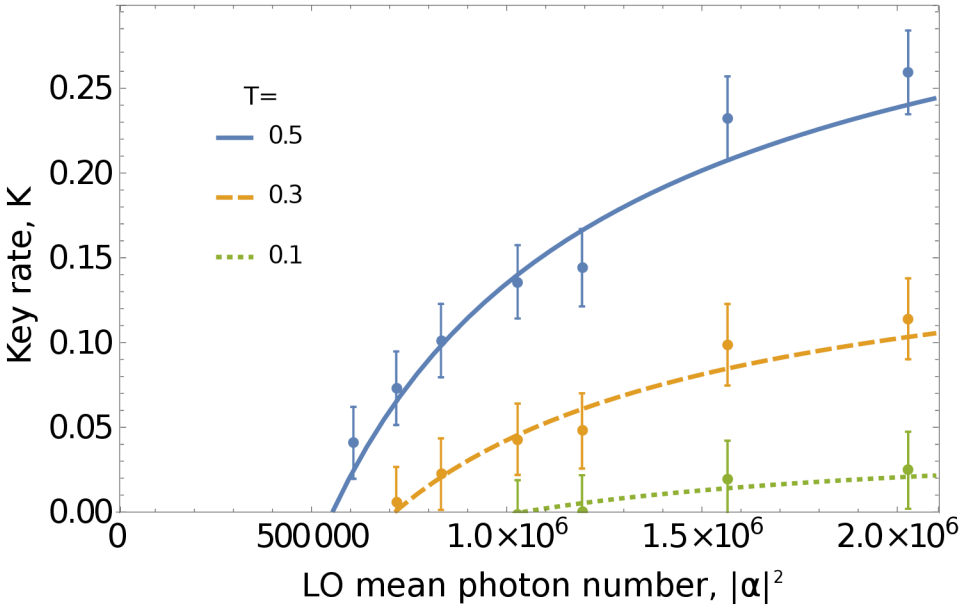

Figure 5.3: The key rate for multimode coherent-state CV QKD in the presence of mode mismatch versus the LO brightness at different values of the channel transmittance T, obtained from the experimentally measured noise (points with error bars) and from the calculated quadrature variance (5.1), (lines). The modulation variance is optimized, $\beta = 0.96$ and $\epsilon^2 = 1$ as confirmed in the experiment.

The asymptotic secure key rate versus increase in LO brightness for different channel transmittance is given in Fig. 5.3. The key rate grows with the larger LO photon number, the maximal key rated is obtained with the maximum LO brightness of 10^6 photons reached in the experiment. In practice it is impossible to indefinitely rise LO brightness due to detectors limitations, in Fig. 5.4 the theoretical prediction of the key rate vs mean photon number in unmatched modes is given for different fixed LO mean photon numbers for a

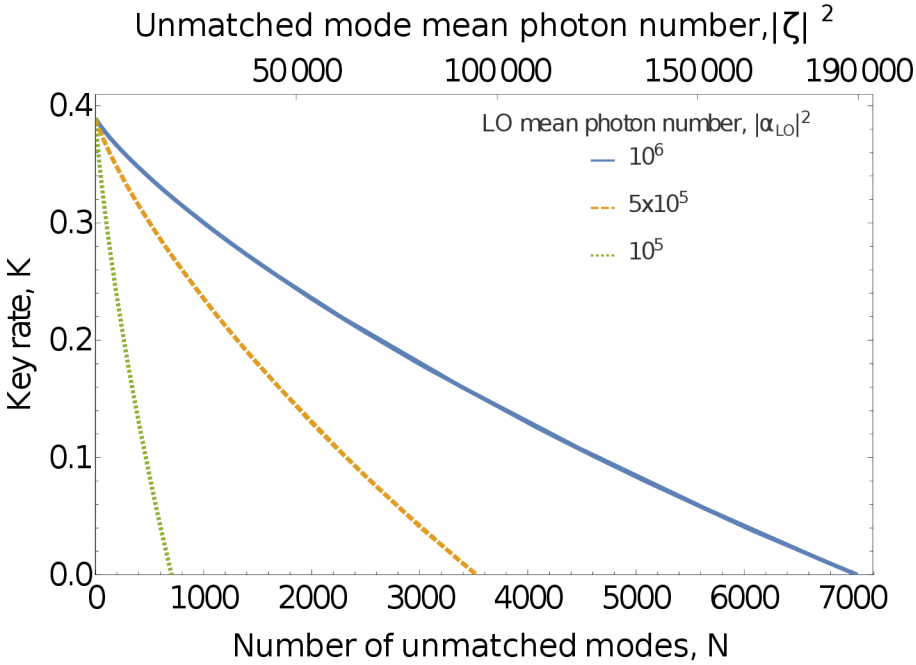

Figure 5.4: The key rate for multimode coherent-state CV QKD in the presence of mode mismatch versus the unmatched mode brightness, $|\zeta|^2$, when only the matched mode is modulated, or, equivalently, versus the number of unmatched modes, N, when all the modes are modulated, and the LO brightness is varied, $T = 0.5$. The modulation variance is optimized, $\beta = 0.96$ and $\epsilon^2 = 1$ as confirmed in the experiment.

mid-range 3 dB channel is plotted, showing how the key rate is destroyed by the noise the unmatched modes create.

Summary. Presence of bright unmatched modes can undermine the security of coherent-state CV QKD with multimode states by leading to the excess noise in homodyne measurement results, which has to be assumed untrusted. We used experimental data that demonstrated how this noise can be suppressed by increase of the power of the local oscillator, to model a CV QKD protocol with multimode coherent states, showing the possibility to perform CV QKD with bright states using optimal modulation and proper mode matching.

6 Conclusions

In this work we theoretically study possibility to implement mode multiplexing in Gaussian quantum communication, in particular entanglement distribution and quantum key distribution. Our theoretical results have been experimentally verified in collaboration with LKB team at Sorbonne University in Paris (Prof. N. Treps) and the group at MPL Erlangen (Prof. M. Chekhova). Using the multimode quantum states, besides obvious advantage of multiplexing the protocol and increase in its capacity, can bring some issues, we address in detail one of them, the inter-mode cross talk, i.e. coupling of multiplexed modes among themselves. We also address the case when multiple modes are not used for channel multiplexing, but to increase the signal brightness.

Firstly, we theoretically study the cross talk problem in a simple 2-TMSV state model looking for the effect linear cross talk has on entanglement distribution. The entanglement shared is shown to be damaged by the cross talk. The negative effect of cross talk can be compensated with an optimally chosen network of passive optical elements. We propose a compensation scheme with the phase adjustment and optimized interference on a beam-splitter, and compare it to an alternative scheme that uses optimal generalised homodyne measurement with feed-forward control. The proposed interference method, if implemented in an optimal way, shows better results and, unlike the measurement with feed forward control, preserves all the modes intact.

We then proceed to apply a more generalised version of the proposed optimal mode interference method to an experimental multimode source of entanglement and model a CV QKD protocol using this source, the synchronously pumped optical parametric oscillator. In the process of the state generation and measurement significant noise is introduced to the signal, some of this noise can be attributed to linear cross talk among the frequency modes. We apply optimal numerical postprocessing (that is a multimode generalisation of the optimal interference method) with the aim to compensate the cross talk and increase the mutual information and the secret key rate. As a result we increase robustness of the protocol to channel attenuation from 8 dB to 28 dB.

Lastly, we study a case where the mode-discriminating measurement is not applicable and multimode structure of the signal is used to increase its brightness, making it easier to handle in the experiment. The problem in the implementation may arise if the modes are not perfectly matched with the local oscillator on the balanced beam-splitter of the homodyne detector. The unmatched modes bring noise to the signal, decreasing the secret key rate of the coherent state protocol we model with the help of data from the proof-of-principle experiment. We show that optimal state modulation and noise suppression by increasing local oscillator intensity improves the protocol performance.

To conclude, mode multiplexing for quantum communication presents multiple challenges in practical implementation, this thesis tackles some of them, concentrating mainly on the inter-mode cross talk. In the future this general line of work can be further expanded in several directions, experimentally with the verification of the CV QKD protocol we modelled. Theoretically also the more complicated models of cross talk can be considered if experimental practice will require it. The presented work is an essential step in development and implementation of efficient continuous-variable quantum communication with mode multiplexing

Bibliography

[1] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[2] Samuel L Braunstein and Peter Van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513, 2005.

[3] Guifré Vidal and Reinhard F Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, 2002.

[4] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9, 05 2015.

[5] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.*, 118:060503, Feb 2017.

[6] J. Aasi, Judith Abadie, B. Abbott, R. Abbott, T. Abbott, Matthew Abernathy, C. Adams, Teneisha Adams, Paolo Addesso, C. Affeldt, Odylio Aguiar, P. Ajith, Bruce Allen, E. Ceron, D. Amariutei, S. Anderson, Warren Anderson, K. Arai, and John Zweizig. Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light. *Nature Photonics*, 7:613, 07 2013.

[7] Horace P. Yuen and Vincent W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8(3):177–179, Mar 1983.

[8] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[9] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[10] Alexander Holevo and Reinhard Werner. Evaluating capacities of bosonic gaussian channels. *Physical Review A*, 03, 2001.

[11] Xiangyu Wang, Yichen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.049167*, 03 2017.

[12] Frédéric Grosshans. Collective attacks and unconditional security in continuous variable quantum key distribution. *Physical review letters*, 94(2):020504, 2005.

[13] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002.

[14] Miguel Navascués, Frédéric Grosshans, and Antonio Acin. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97(19):190502, 2006.

[15] Raul Garcia-Patron and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):190503, 2006.

[16] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J Cerf. Security of continuous-variable quantum key distribution against general attacks. *Physical Review Letters*, 110(3):030502, 2013.

[17] Takuya Kudo and Takaaki Ishigure. Analysis of interchannel crosstalk in multimode parallel optical waveguides using the beam propagation method. *Optics Express*, 22(8):9675–9686, 2014.

[18] Lukasz Szostkiewicz, Marek Napierala, Anna Ziolowicz, Anna Pytel, Tadeusz Tenderenda, and Tomasz Nasilowski. Cross talk analysis in multicore optical fibers by supermode theory. *Optics Letters*, 41(16):3759–3762, 2016.

[19] Jonathan Roslund, Renné Medeiros De Araujo, Shifeng Jiang, Claude Fabre, and Nicolas Treps. Wavelength-multiplexed quantum networks with ultrafast frequency combs. *Nature Photonics*, 8(2):109, 2014.

[20] Badraoui Nada and Tibor Berceli. Crosstalk reduction in fiber links using double polarization. *Optical and Quantum Electronics*, 52, 03 2020.

[21] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, 04 2017.

[22] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63(5):052311, apr 2001.

[23] Cosmo Lupo, Laleh Memarzadeh, and Stefano Mancini. Removing correlations in signals transmitted over a quantum memory channel. *Phys. Rev. A*, 85:012320, Jan 2012.

[24] F. Verstraete, M. Popp, and J. I. Cirac. Entanglement versus correlations in spin systems. *Phys. Rev. Lett.*, 92:027901, Jan 2004.

[25] Fabio Sciarrino, Eleonora Nagali, Francesco De Martini, Miroslav Gavenda, and Radim Filip. Entanglement localization after coupling to an incoherent noisy system. *Phys. Rev. A*, 79:060304, Jun 2009.

[26] Y Cai, J Roslund, G Ferrini, F Arzani, X Xu, C Fabre, and Nicolas Treps. Multimode entanglement in reconfigurable graph states using optical frequency combs. *Nature Communications*, 8:15645, June 2017.

[27] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[28] Vladyslav C Usenko, Laszlo Ruppert, and Radim Filip. Quantum communication with macroscopically bright nonclassical states. *Optics Express*, 23(24):31534–31543, 2015.

[29] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7):535–552, October 2003.

Published articles

1. Olena Kovalenko, Vladyslav C. Usenko, and Radim Filip, **"Cross talk compensation in multimode continuous-variable entanglement distribution"**, *Optics Express* Vol. 29, Issue 15, pp. 24083-24101 (2021)

2. Olena Kovalenko, Young-Sik Ra, Yin Cai, Vladyslav C. Usenko, Claude Fabre, Nicolas Treps, and Radim Filip, **"Frequency multiplexed entanglement for continuous-variable quantum key distribution"** , *Photonics research* Vol. 9, Issue 12, pp. 2351-2359 (2021)

3. Olena Kovalenko, Kirill Yu. Spasibko, Maria V. Chekhova, Vladyslav C. Usenko and Radim Filip, **"Feasibility of quantum key distribution with macroscopically bright coherent light"**, *Optics Express* Vol. 27, Issue 25, pp. 36154-36163 (2019)