PALACKY UNIVERSITY OLOMOUC
FACULTY OF SCIENCE

Department of Optics

Robustness of Continuous-Variable Quantum Key Distribution

Ivan Derkach

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 2020

Abstract

The aim of this thesis is to present the results of the research conducted during the course of my Ph.D. studies at Palacky University in Olomouc, Czech Republic. The research tackles the issue of improvement and optimization of existing Gaussian Continuous-Variable Quantum Key Distribution protocols. We approach the issue from two different angles: by altering the assumptions about the boundaries of the trusted sides, and by studying the behavior of protocols in free space channels, in order to devise novel improvement methods compatible with already existing ones.

Taking into account trusted device imperfections, and analyzing their influence on the security, as well as, tolerance (to losses and noise) of the Gaussian protocols prompts to enhance accessibility and applicability of respective protocols. More specifically, we investigate generalized side channels [1], access to which could allow an adversary to break the security by utilizing implementation weakness rather than the protocol itself. We addresses two types of side channels, both of which constitute a security concern as they impose limitations on the rate of the key generation, and effectively reduce the secure distance. We continue the analysis [2], and further investigate the threat of side channels on the trusted preparation side. Furthermore, the we also account for another type of feasible threat on preparation - a case of non-signal modes being emitted by the trusted sender, and accessible to an eavesdropper, and carrying partial (or full) information about the encoded key bits. In both works we determine security boundaries, and develop methods based on linear optics and Gaussian operations for compensation, or even complete elimination of negative impact of respective sources of information leakage or noise infusion.

We also approach the issue of incorporating the protocol in realistic free space untrusted channels with the aim of maximizing the efficiency of use of the resources required for growing the secret key between remote trusted parties. We study the applicability of beam expansion as the way to stabilize the transmittance fluctuations which have been shown to impose significant restraints on the performance of the CV QKD protocols established over turbulent atmospheric channel [3]. Suggested method is experimentally verified in collaboration with scientific group from Max Planck Institute for the Science of Light. We show the requirement for the optimization of the beam width, and prove the positive effect of such stabilization technique in mid-range terrestrial free space links.

Lastly, we analyze the role of squeezing in free-space CV QKD protocols [4]. We determine an approach for efficient use of squeezing and encoding alphabet size to improve or even restore the security of the protocols. We confirm the validity of suggested approach using numerical simulations of realistic turbulent fading channels under various atmospheric conditions, based on novel models for transmittance probability distributions [5–7].

Throughout the research we attempt to strengthen the link between theoretical protocol design and real-life implementations. By investigating possible loopholes we pursuit establishment of more rigid set of assumptions that underlie the security of CV QKD pro-

tocols. Developed methods for elimination of the loopholes are crucial for advancement towards more robust, faster and reliable QKD-based communication systems.

Key words

Quantum key distribution, continuous variables, Gaussian states, squeezed light, coherent states, side channels, free space communication.

Acknowledgement

I would like to express my immense gratitude to my supervisor Prof. Radim Filip for his belief in me, encouragement and for being a continuous source of knowledge and inspiration.

I am forever indebted to my co-supervisor and mentor Dr. Vladyslav C. Usenko for providing me with an opportunity to join the ranks of students and the research team, thus allowing me to start a new and breathtaking chapter of my life. It is no overstatement to say that without his patience, feedback and guidance this work would have never existed.

A heartfelt thanks to my colleagues at the Department of Optics - Martina Nováková and Ivo Straka for being incredible and supporting friends. I couldn't ask for better people to share the office with.

A special word of gratitude to Adam, my baby son, who has been an inexhaustible source of happiness, joy, distraction, strength, and motivation for the last two years.

Above all I would like to thank my wife for her tireless support, and unconditional love. Thank you for unhesitatingly following and adamantly believing in me. I am blessed to have you, holding my hand in triumphs and sorrows. Thank you for the infinite garden.

Lastly, to everyone else whom I hold dear, who never asked, but always knew.

Declaration

I hereby declare that this thesis titled **"Robustness of Continuous-Variable Quantum Key Distribution"** have been composed solely by myself under the guidance of my supervisor prof. Mgr. Radim Filip, Ph.D. and my co-supervisor 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.

.....
Ivan Derkach

In Olomouc, ... 2020

List of Abbreviations

CV	Continuous Variable
DV	Discrete Variable
QKD	Quantum Key Distribution
DR	Direct Reconciliation
RR	Reverse Reconciliation
BS	Beam Splitter
R	Secure key rate
SNU	Shot Noise Units
SNR	Signal to Noise Ratio
dB	Decibel (unit of measurement)
η	Transmittance
ε	Excess noise
I	Mutual Information
χ	Holevo bound
LO	Local Oscillator
EPR	Entangled state (*abbreviation refers to Einstein-Podolski-Rosen paradox*)
σ_R^2	Rytov parameter
C_n^2	Structure constant of refractive index of air
β	post-processing algorithm efficiency
γ	covariance matrix
PDT	Probability distribution of the transmittance
PZT	Piezoelectric transducer
PD	Photodetector
OPO	Optical Parametric Oscillator
TMSV	Two-Mode Squeezed Vacuum

Contents

1 Introduction

Information theory theories allows to interpret the insights provided by Quantum Mechanics, a fundamental theory inherently derived from a set of purely abstract mathematical ideas and concepts, in a way that deepens our understanding of, and, most importantly, is applicable in the real world. It was inevitable that a practical application would arise at the intersection of these scientific fields. The very first conceived proposal introduced the idea of conjugate coding [8] and used it as a basis for the design of bank notes that would employ quantum mechanics to ensure the impossibility of forging. However, it was not until later that the idea found its use in a quantum secret key distribution protocol, now known as BB84 [9], that promised an unprecedented level of security. More specifically, it allowed a secure delivery of classical symmetrical encryption keys of one-time pad algorithm, the only algorithm proven to be mathematically unbreakable. The protocol gave birth to a novel method of secure communication and spurred the creation of great number of new more resilient, faster, reliable and affordable protocols and systems. It quickly evolved into a whole new distinct area of research - *Quantum Key Distribution* (QKD), that currently encompasses numerous scientific groups and individual researchers, physicists and engineers around the globe, both in academic and commercial institutions. The field of QKD further expanded and is now a part of major group of algorithms and protocols that belong to Post-Quantum Cryptography field of research.

The work conducted during the course of my Ph.D. studies at Palacky University (Olomouc, Czech Republic) concerns a family of Continuous-Variable (CV) QKD protocols that make use of carrier states described by a finite covariance matrix, and are operated with accessible and efficient existing quantum optics technologies. The research is dedicated to studying the security conditions and boundaries, and is aimed at improvement of the protocols by means of addressing the influence of realistic effects, and developing methods for enhancing the tolerance again the negative effects, and consequently improving the speed and range of applicability of the protocols.

Outline of the thesis

The thesis is structured as follows. The Chapter 2 introduces the basics of continuous-variable (CV) quantum key distribution protocol (QKD). First, we outline general steps

taken during each round, and further delve into the details of the structure of the protocol. We define main distinctions between CV QKD protocols, in terms of techniques used by sending and receiving parties, as well as, based on the nature of the untrusted channel, and attacks conceived by the adversary. We compare the performance of CV QKD protocols with regards to the secure key rate, and excess noise tolerance. Lastly, at the end of the chapter we introduce two purification schemes, used during the research, for incorporation of complex issues (such as source attacks or side channels) into the security analysis.

Chapter 3 constitutes an extensive review of contemporary state of research. It describes the obstacles present at each step of the protocol implementation, starting with the generation and modulation of the Gaussian states, and ending with classical processing conducted by trusted parties after the satisfactory amount of data has been amassed. Majority of effects, which are present in already implemented systems, can be viewed as either additional losses or noise (both of which can also be assumed to be trusted or untrusted), hence we provide a short summary of theoretical treatment of respective losses or noise. Furthermore, we address possible existing solutions to implementation problems that pose security concerns.

Chapters 4-6 demonstrate a short summary of the results obtained throughout the research, including the models used for the analysis. More specifically, Chapter. 4 is concerned with the side-channel effects and their role on the security of CV QKD protocols. We distinguish between various side channels according to their general effect (information leakage or increased noise), and point of intrusions, which determines the effect on specific part of protocol operation. We also suggest methods for partial or full compensation of side-channel effects.

Chapter 5 describes the repercussions of information leakage into the auxiliary optical modes emitted from the preparation side. We examine the effect on major CV QKD protocols, and determine the influence of such leakage on various aspects of performance of the respective protocols. We suggest optimization of affected protocols aimed at reducing the respective negative effects.

Chapter 6 summarizes the results of experimental-theoretical collaboration aimed at stabilization of transmittance fluctuations in free-space atmospheric channels by means of beam expansion. We show the regimes where the suggested method yields positive results for both the non-classical properties of light, and the security of the CV QKD protocols.

Chapter 7 presents the outcome of investigation of the role of the squeezed states and their presumable advantages in free-space turbulent communication links. We develop an optimization approach and assert it's applicability in short urban links, using numerical simulations based on advanced models and available in open-access experimentally obtained characteristics of transmittance probability distribution.

In Chapter 9 we outline main achievements of the performed research, consider both theoretical and practical implications, as well as suggestions for future work. Finally, we conclude with copies of published and submitted articles in Chapter 8, and with Bibliography.

2 | Quantum Key Distribution

The ultimate security for communication has been sought throughout human history. The threat of interception, and consequent revelation of secrets and vital information has been ceaselessly pushing the development of ciphers and codes. Perpetual arms race between codemakers and codebreakers have led to evolution of codes and ciphers, and powerful methods to attack them, bringing forth advancements and breakthroughs in a wide spectrum of disciplines, from linguistics and mathematics to information, and quantum theory.

Undoubtedly, the supreme goal of a codemaker has always been the creation of an "uncrackable" encryption technique. Such technique has in fact been created and carries the name *one-time pad* [10]. It descents from the Vigenère cipher, which belongs to the same family as the famous Enigma machine - polyalphabetic ciphers. While having a reputation of an unbreakable, or "impossible of translation" for a long time, Vigenère cipher was fundamentally flawed due to its cyclic nature, and has been eventually broken. However the cipher has been later improved upon and used as a foundation for Vernam-Vigenèr cipher, where the key size has been increased to match the one of the message. The length of the key itself is still not sufficient to confidently withstand an arbitrary attack, as it has been shown that reuse of (short random key, as initially suggested by Vernam), or predictable nature (sequence of vocabulary words) of the key is an underlying weakness. Finally, the head of cryptographic research for the US Army, Major Joseph O. Mauborgne, suggested the use of non-repeatable truly random key. The original realization of the cipher was done in a form of two copies of a thick pad with hundreds of pages of random and unique keys, one for the sender and the other for the receiver. The sheets with used key sequences were discarded never to be used again, hence the name of the cipher - the one-time pad.

One-time pad has been proven by Claude Shannon to be "information-theoretically secure" [11], and it satisfies the strongest possible requirements for a cipher, as long as:

- key length is equivalent to message length;
- the key is truly random;
- the key is unique and is used only once.

The matching length and randomness of the key seeds the randomness of the cipher-text, and devoids the latter from any pattern or structure. The non-repeatability further

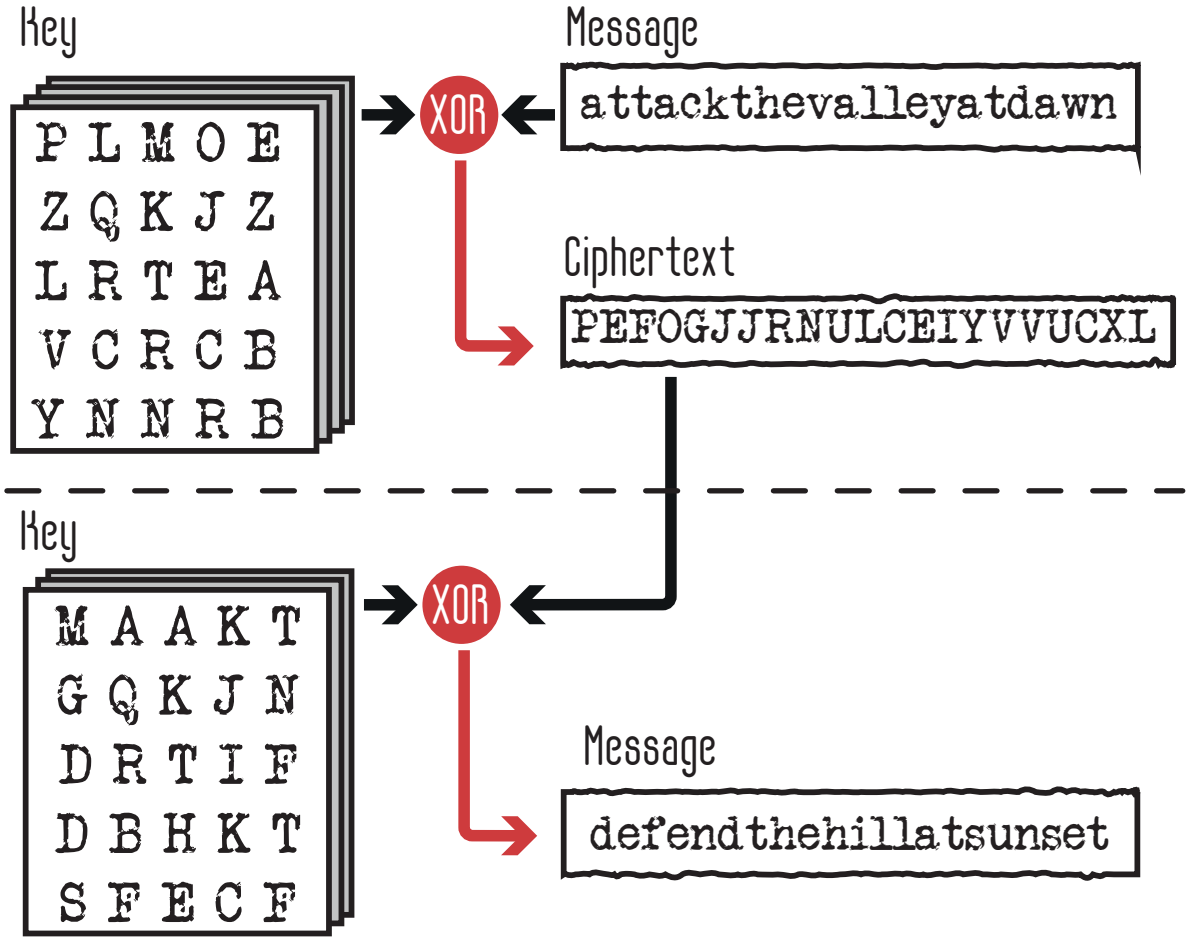


Figure 2.1: Illustration of one-time pad encoding process. Random key and the message of equal lengths are combined via XOR operation and result in a ciphertext. Applying the same key to the ciphertext would result in the original message recovery, however another key sequence may lead to completely different, yet sensible message [12].

ensures the protection the encoded plaintext, and renders any further cryptoanalysis ineffective. One can argue that it is still possible to guess the correct key by brute force as the number of possible keys is still finite, however the correct message is indistinguishable from any kind of sensible message generated using the same ciphertext, as illustrated in Fig.(2.1).

Despite being "the Holy Grail of cryptography" [12] the actual practical implementations have to solve the issue of generation of perfectly random keys, which is currently achieved using hardware systems that make use of fundamental randomness of quantum physics [13, 14]. Lastly, it is imperative for the generated keys to be reliably distributed among trusted parties. The solution has been found, and, in fact, it stemmed a new branch of quantum information science, namely the QKD.

In 1984 C. H. Bennett and G. Brassard have published a pioneering paper *Quantum Cryptography: Public Key Distribution and Coin Tossing* [9], where they first introduced a protocol (BB84) that exploits the non-cloning principle [15] in order to establish secure transmission of the one-time pad keys. While conventional classical cryptographic

protocols are forced to accept ever-present possibility of a third party to reliably copy transmitted information, BB84 relies on unavoidable alteration of the transmitted (by means of a quantum system) key as the way to expose the attempted eavesdropping. The brilliant idea went unnoticed until later, when A. K. Ekert have independently [16] developed another protocol (E91), where an entangled state is shared by trusted parties, and the security is guaranteed from the point of view of fundamental completeness of quantum mechanics. While BB84 takes a prepare-and-measure (P&M) approach, as the protocol commences with straightforward preparation of linearly polarized (in a random horizontal-vertical, or 45-degree rotated basis) single photons, E91 is an entanglement-based protocol, as it involves distribution of parts of the entangled state and nonlocal preparation of the the state on the receiver station by conducting polarization measurements on the sender side. Security of BB84 is confirmed via inspection of an error rate (QBER) during post-processing step of the protocol, while E91 requires verification of the Bell-inequalities violation. Nevertheless, both protocols have been shown to be equivalent [17], as they effectively achieve the same goal and match in performance.

The spotlight brought by E91 stimulated a rapid development of QKD, starting with creation of modified versions of BB84: B92 and SARG04 protocols [18, 19], invention of plug-and-play approach [20, 21], and first experimental demonstrations [22–25] including 22.7 km long quantum channel in an underwater optical fiber [26].

Initial security proofs assumed the use of ideal source that outputs single-photon Fock states. However, in practice the signal states in conventional QKD protocols are obtained from faint coherent laser pulses, and a non-vanishing probability of emitting a second photon turned out to be a crucial security threat, provided a photon-number splitting attack [27, 28] is employed. This led to development of protocols with decoy states [29–31].

Initially the security of the protocols has been considered against explicit eavesdropping strategies, however rigorous security proofs were eventually derivated, first for collective [32] and coherent [33] attacks, and ultimately extended to composable security framework [34–37], including realistic considerations of finite block sizes [38].

BB84 protocol and it's modified versions constitute an extensive family of *discrete-variable* (DV) QKD protocols. In the DV protocols a carrier photon state belongs to a discrete set, where each state is assigned a binary value, hence allowing for a convenient translation from and to a binary key sequence. However, such protocols require dedicated equipment, namely for photon-counting measurement that is broadband, demands cooling and is sensitive to stray light. Integration of such equipment into telecommunication infrastructure is an expensive and arduous endeavor. Instead one can look into an alternative family of protocols based on multiphoton Gaussian states that can be generated at higher rates (comparing to single-photon states), and measured by coherent homodyne/heterodyne detection techniques, compatible with existing optical communication systems, at room temperatures and high efficiencies. Even though mapping of key bits onto single-photon states is straightforward and intuitively clear, aforementioned technical compatibility stimulated to explore the implementation of QKD with multiphoton states. The very first protocols supporting this idea adopted the strategy of discrete modulation according to a binary key, but employed amplitude and phase quadrature

modulation of the coherent states, and consequent homodyne detection [39]. Later, more efficient and robust protocols have been suggested based on single-mode squeezed vacuum states [40], and entangled two-mode squeezed states, where a bit value is governed by the state at the input of nondegenerate parametric amplifier [41], or by the choice of measured observable at the sender side [42]. Such protocols, although still applying discrete modulation of continuous amplitude and phase, belong to a family of *continuous-variable* (CV) protocols. They've been successfully experimentally realized [43], including over 100 km long channel [44], and are still the topic of an ongoing research and development [45–48] and recently proven to be composably secure in the finite-size regime under collective attacks [49].

Another branch of CV QKD protocols fully embraces Gaussian states and, instead of mere substitution for single-photon states, enforces distribution of continuous secret keys. Such family of protocols draws the key from continuous Gaussian distribution and translates it directly to continuous quadrature observable. The key is retrieved on the remote side by means of homodyne (or heterodyne) measurement, and only after is digitized and corrected for errors. The very first all-continuous protocol relied on displaced single-mode squeezed vacuum states to carry the key, and it have been introduced by N.J. Cerf, M. Lévy, and G. Van Assche in 2001 [50]. The requirement for sub-shot-noise of the carrier state have been later alleviated by F. Grosshans and Ph. Grangier, as the coherent-state protocol (GG02) have been shown [51] to be secure, as well.

The channels used for QKD were limited to 3 dB loss, because under higher losses the receiver would always be in a disadvantage (information-wise), as the majority of the state is being received by an eavesdropper. While post-selection [52] or entanglement-purification [53, 54] were suggested to overcome the limit, the constraint on losses can be dismissed entirely if trusted parties agree that the trusted party that prepares and sends the state will adjust the data according to the measurement outcomes of receiving party. In fact, such (reverse) reconciliation method is optimal, assuming the channel used is noiseless [55].

One of the early challenges of CV QKD which constrained the output rate of the protocols was not the speed and efficiency of optical equipment, but rather the speed of classical algorithms involved in error correction and privacy amplification [56]. The inevitable deviation of error correction algorithms performance from the Shannon limit [57] in real-world applications was first investigated in noiseless channels [58], with post-selection suggested for improvement of loss and detector noise tolerance of the protocol. Data processing and acquisition speeds imposed limitations on achievable secure distance, as experimental setups were bounded by $\sim$80% post-processing efficiency, thus limiting the channel length to 20 km in standard single-mode telecom fiber [59,60]. The coherent-state protocol with reverse reconciliation (see Ch. 2.1.4) was soon adopted for complete implementation of QKD system, where the fiber channel was extended to 25 km, maintaining the secure key rate of 2 $kbit/s$ [61]. The same CV QKD protocol has been used to test polarization-frequency-multiplexing scheme aimed at reduction of excess noise caused by local oscillator (LO) leakage, achieving 0.3 $bit/pulse$ secure key rate [62]. A portable CV QKD prototype has been tested as part of a SECOQC quantum network in Vienna [43].

The system delivered an average key rate of 8 $kbit/s$ over a 3 dB loss channel for the duration over 3 days. Long-term robustness and reliability have been further tested and confirmed during 6 months on the 17.7 km long fiber link near Paris [63].

Significant secure distance increment to 80 km has been achieved by implementing efficient high-speed error correction codes [64]. Obtained key rate of the coherent-state protocol was secure against collective attacks (see Sec. 2.1.3), and the block sizes were compatible with finite-size effects (see Sec. 3.4.7). The range of the coherent-state protocol has been extended even further to 100 km by adopting sensitive homodyne detectors and accurate compensation for phase drift between signal and LO [44]. Lastly, a recent experiment achieved a secure distance of 202.81 km by employing reconciliation with 98% efficiency and high precision phase compensation [65].

Tremendous achievements in experimental implementations of point-to-point QKD protocols are just the first step towards QKD secured networks. The feasibility of the latter has first been studied by the DARPA Quantum network project which started operating in 2003 [66]. Between 2004 and 2008 another QKD network, that incorporated multiple types of QKD links and technologies, has been engineered and set up in Vienna - SECOQC network [67]. Swiss Quantum Network has been operating between 2009 and 2011 connecting 3 nodes located in France and Switzerland [68]. Under Durban–QuantumCity project a 4-node DV QKD network based on plug-and-play BB84 protocol has been set up in 2010 [69]. In the same year Tokyo QKD Network as the result of collaboration between multiple companies and institutions has been created [70]. The network utilized six kinds of QKD systems which allowed to perform (one-time pad encrypted) live TV conferencing between any two out of four access points of the network.

As sources and detectors evolved to be more reliable and faster, so did the QKD networks. The steady progress gradually allowed to increase key distribution speed, and coverage, connecting trusted parties separated by hundreds of kilometers or potentially even globally. In 2013 US-based firm Battelle have installed quantum network between Columbus and Dublin (Ohio) [71], with a future plan to extend the network further to Washington (DC) which would result in total distance to exceed 700 km. Another prominent example of ongoing QKD network research and development is a long-distance network connecting Cambridge, London and Bristol, as part of UK Quantum Technology Hub [72]. Metropolitan QKD networks have been already deployed in several cities in China, that will be connected to a 2000 km long Shanghai-Hefei-Jinan-Beijing link [73]. The network will rely on 32 trusted nodes to measure and resend quantum keys.

It is important to note that there is no single QKD protocol or even family of protocols that would be universally suitable for a whole range of application requirements. With respect to the secure distance, the DV protocols are commonly accepted as more suited for long-range links [74], while CV protocols are an efficient, high-rate [75] solution for shorter distances [64]. However, the protocols are not contesting, but rather complement each other, covering opposing ends of the secure range. Thus aforementioned networks rarely rely on a single type of QKD protocols - for example SECOQC, and Shanghai-Hefei-Jinan-Beijing networks incorporate both DV and CV QKD links. A fiber-based sub-network of the latter, that was deployed and tested in Shanghai, operates solely on

CV QKD protocols [46]. Development of satellite-based QKD [74,76,77] opens possibilities for global connection of multiple, already existing, QKD networks, each making use of best available technologies and protocols suitable and convenient for given locations and conditions.

Crucially QKD protocols have to balance the secure key rate and a level of security. The latter is a complex subject that incorporates the strength of assumed attack on the system, the trust in used equipment, and other aspects of implementation and security assumptions. For derivation of security proofs numerous obstacles, including infinite dimensions, unbounded variables, discretization, etc., had to be overcome. At first the security was successfully generalized from explicit attacks to optimal individual [78], and collective attacks [79, 80], though only in asymptotic regime of infinitely many signals. The fact that Gaussian states minimize the entanglement, as well as distillable secret key rate [81][1], and existence of analogous security proofs for DV QKD [33], supported the assumption that the security would also hold for the case of the most general attacks. The assumption had yet to be proven, but CV QKD maintained vigorous development rate, both experimental and theoretical [43,82–84]. In 2009 extended version of de Finetti theorem has been used to show that security of CV QKD protocols[2] against the collective attacks implies the security against the most general case of coherent attacks [87]. However, at the time, existing security bounds were not suited for practical implementations as they were required to be adapted to finite-size effects. The basis of finite-size analysis has been established by A. Leverrier, F. Grosshans and P. Grangier in 2010 [88], and allowed to correct the asymptotic key rate for finite precision of parameter estimation.

Based on the de Finetti theorem [89] and entropic uncertainty principle, the advent of composable CV QKD security proofs started when the lower bound on the composably secure key has been derived [90] for the DR protocol employing TMSV states and homodyne detection. Later, under similar assumptions, the security for the RR scenario has been proven too [91]. An approach based on rotational phase-space symmetries was used to validate the security of the coherent-state protocol first against collective [88], then against coherent attacks [92] (for both DR and RR). The same approach was involved in creation of the framework for composable security proof that can integrate properly modeled device imperfections, and it was used to confirm security versus collective and, using post-selection [35, 93], coherent attacks [94]. The common assumption of optimality of Gaussian attacks has been recently confirmed using Gaussian de Finetti reduction [95].

Despite tremendous progress in security analysis [96], there are still open question regarding both entropic uncertainty relation, and de Finetti theorem (*i.e.* symmetrization requirement) techniques, as a consequence existing security proofs are applicable only to limited range of CV QKD protocols. Furthermore, they impose strict requirements on equipment efficiency, demand monitoring, and do not account for possible deviations from Gaussian modulation.

Although the search for general composable security proof applicable in realistic sce-

[1] This notion is also known as extremality of Gaussian states, and is explained later in the text

[2] The proof is applied to majority of CV QKD protocols, except Differential Phase Shift and the Coherent One-Way protocols [85, 86].

narios is still ongoing, it is vital to develop operational security as well. Implementation weakness and deviations from theoretical models used for security proofs have to be accounted for, and either operational countermeasures or improvement of theoretical models must be devised. The studies of side channels in chapter 4, leakage of modulated non-signal modes in chapter 5 and compensation of turbulence effects presented in chapters 6,7 are aimed at enhancing operational security of CV QKD protocols.

2.1 CV QKD protocols

The main goal of any QKD protocol is to distribute sequence of bits between two faithful, authenticated parties, conventionally referred to as Alice and Bob, where usually the former plays the role of the sender and the latter of the receiver. The objective of QKD protocols is to distribute and ensure security of the key, which can be later used to encrypt data. The disturbances in distribution of the key are attributed to the third party, Eve. Her sole intent is to acquire the copy of the transmitted key. Generally Eve's role is far from passive eavesdropping, and in more pessimistic scenarios she is not confined to the channel alone, as she can intervene onto the trusted side to extract additional information, or temper with equipment via side channels. Despite the assumptions on boundaries of Eve's invasiveness, she is not limited by current technologies, merely by the laws of physics.

2.1.1 Outline

We consider quantum systems consisting of n bosonic modes of the electromagnetic radiation. Each mode is described on an infinite-dimensional Hilbert space, and the overall system is the described on a tensor-product Hilbert space $\mathcal{H}^{\otimes n} = \otimes_{j=1}^{n} \mathcal{H}_i$ [97–99]. The description of each mode is given in terms of a pair of bosonic field ladder operators $\{\hat{a}, \hat{a}^\dagger\}_{j=1}^{n}$, also referred to as the annihilation and the creation operators, respectively. CV QKD analysis primarily deals with moments of dimensionless canonical observables of these modes, with the observables being quadrature field operators defined[3] as:

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

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

The overall system can be described by a vectorial operator $\hat{\mathbf{q}} := (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_n, \hat{p}_n)^T$, where commutation relation between each pair of operators is given by the symplectic

[3]The definition of quadrature operators $\hat{x}$ and $\hat{p}$, and their explicit dependency on the ladder operators can vary and depend simply on notational and/or computational convenience. In current work we employ shot-noise units, while other often used are: natural units [100], where $\hat{x} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a})$; and SI-units [101], where $\hat{x} = \sqrt{\frac{\hbar}{2\omega}}(\hat{a}^\dagger + \hat{a}), \hat{p} = i\sqrt{\frac{\hbar}{2\omega}}(\hat{a}^\dagger - \hat{a})$.

form Ω_{kl} [97]:

$$[q_k, q_l] = 2i\Omega_{kl}, \quad \Omega_{kl} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.3}$$

The quadrature field operators $\hat{x}, \hat{p}$ can be directly measured using homodyne detection. Prior to the detection, the light signal is coupled on a balanced beamsplitter to a local oscillator (LO) beam that serves as a phase reference. Photodetection of light from two output ports and subsequent subtraction of photocurrents yields the value proportional to an amplitude or a phase quadrature (depending on the phase of the LO [97]) of the signal.

Operational structure of the protocol

Any CV QKD protocol is executed in four main stages:

State preparation $\rightarrow$ *Channel* $\rightarrow$ *Measurement* $\rightarrow$ *Classical post-processing.*

The *state preparation* is usually split into state generation and modulation, which are performed on Alice's side, while *measurement* (in one-way prepare-and-measure QKD protocols) is carried out on Bob's side. Conventionally, aside from equipment on respective sides, Alice and Bob have access to two channels: quantum (*a priori* untrusted) channel, and classical (*a posteriori* reliable) channel. The former is under full control of Eve[4], while the latter is public, but cannot be tampered with. The authentication implies the existence of prior secret information between Alice and Bob, and in this sense QKD can also be seen as a secret key growing. We also consider side channels, that are defined as auxiliary channels with either input or output controlled by a trusted party but, respectively, output or input is controlled by an eavesdropper. Such definition allows to distinguish side channels (and their influence) from the main untrusted channel, where an eavesdropper controls both input and output of the channel. In other words, Eve is free to prepare any physical ancilla and store it after its interaction with the signal in the untrusted channel, while she can either send an additional ancilla in a side channel, or store the state coming out of a side channel. The side channels are the generalization of the various effects that can occur in quantum domain providing an eavesdropper with additional information on the key by means of either disruption of the trusted equipment operation or benefiting from leakage of the signal.

Let us now describe the operational steps of the one-way prepare-and-measure CV QKD protocol:

0 *Handshake.* Alice and Bob establish and authenticate classical channel. They agree on the type of carrier states to be used, and modulation and measurement to be performed. Moreover, trusted parties settle on the reconciliation direction, and families of codes, and hash functions required for error correction and privacy amplification.

[4]By full control we understand Eve's ability to substitute the channel with a perfect noiseless channel, with losses and noise imposed on the signal being the result of the interaction with Eve's ancillas. However trusted parties cannot discern sources of losses and noise by channel tomography. In other words, Eve can hold the purification the overall signal state.

1. *State generation.* Alice generates two N sets of random variables governed by two independent Gaussian distributions with zero mean:

$$x = \{x_1, x_2, \dots x_N\},\ x \sim \mathcal{N}(0, V_m^x);$$
$$p = \{p_1, p_2, \dots p_N\},\ p \sim \mathcal{N}(0, V_m^p);$$

and another N set consisting of equally likely binary values (*i.e.*, corresponding to a balanced Bernoulli process):

$$h = \{h_1, h_2, \dots h_N\},\ h \sim \mathcal{B}(1, 0.5).$$

Alice then prepares squeezed vacuum states $|0, \xi_n\rangle$, where $\xi_n = re^{i2\theta_n}$ with $r \in [0, \infty)$ being the squeezing value[5], while $\theta_n = h_n\pi/2$ determines the squeezing orientation (*i.e.*, $\hat{x}$-, or $\hat{p}$-squeezed state will be used).

2. *Modulation.* Alice displaces the squeezed vacuum state according to a generated random variable as

$$\hat{D}([1-h]^g x)_n \hat{D}(ih^g p)_n |0, \xi_n\rangle = |(1-h)^g x + ih^g p, \xi\rangle.$$

The value of g (negotiated during handshake step of the protocol) can be set to either 1, corresponding to modulation in single quadrature, or 0, corresponding to modulation in both quadratures[6].

3. *Transmission.* Carrier states are transmitted from Alice to Bob via an untrusted channel, where the signal is subjected to losses and noise.

4. *Measurement.* Bob, depending on initial arrangements, will measure either one or both quadratures of the incoming state. In the former case he generates N set according to balanced Bernoulli process:

$$u = \{u_1, u_2, \dots u_N\},\ u \sim \mathcal{B}(1, 0.5).$$

During each round of the protocol he will adjust the phase shift $\theta_{LO}(u)$ of the local oscillator and measure respective quadrature.

5. *Sifting.* After N rounds Alice and Bob coarsely discretize the digital data on their sides according to agreed alphabet, and compare h and u values, keeping the data for the rounds when values match, and discard the rest. At the end of this step

[5]Note that in principle initial states need not be pure coherent or squeezed states as some protocols admit the use of initially noisy or thermal states [102–104], for example if carrier states are at longer wavelengths [105]

[6]Conventional protocols that employ the coherent-states ($r = 0$), usually require displacement of the state in both quadratures ($g = 0$), however during *e.g.* unidimensional protocol [106, 107] single quadrature modulation is sufficient.

Alice and Bob share a sequence of correlated classical variables $L \leq N$[7].

6. *Parameter estimation.* Alice and Bob agree on a random subset of data $m \subset L$ to disclose the corresponding values via classical channel in order to estimate the security. The protocol may abort at this step if estimated channel attenuation and excess noise[8] exceed a predetermined threshold.

7. *Error correction.* Alice and Bob try to eliminate the errors in the data sets remaining on their sides using classical error correction algorithms, resulting in raw key $l_{raw} \leq L - m$. Due to non-negligible failure probability of the error correction [109], Alice and Bob compare the hash values of the new sequence l_{raw}. In case of disagreement the protocol is aborted.

8. *Privacy amplification.* To eliminate any correlations Eve may have with the raw key l_{raw}, Alice and Bob conduct privacy amplification [110–112]. They choose hash function (from predetermined family) [113] that accepts l_{raw} at the input and outputs a sequence with higher entropy $l_{final} \leq l_{raw}$. The final key now satisfies all the prerequisites to perform a one-time pad encryption [10, 11].

There are many variations of the protocol, however the overall structure remains intact, though the protocol may include additional steps to improve its performance, or implementation convenience. The steps may include state engineering and optimization of protocol parameters (r, V_m) based on channel estimation, prevention of side channel effects, substitution of LO with reference pulses that enable Bob to generate local oscillator at his side [114] or postselection [115]. The latter, under assumption of asymptotic regime, is an efficient tool, however may not be compatible with majority of security proofs.

Further we go into details regarding certain steps of the protocol that deserve additional attention, such as conditional remote state preparation [116], and discuss the security of the protocol along with eavesdropping strategies.

2.1.2 State preparation

During each round of the protocol Alice first generates Gaussian signal state using either laser or single-mode squeezer, or by measuring one of the modes emitted by two-mode squeezer. Remarkably, first and second moments are sufficient for the description of the Gaussian states [98], with the second moment being expressed as the positive-semidefinite symmetric covariance matrix defined as:

$$\gamma_{i,j} = \frac{1}{2}\langle\{\Delta x(p)_i, \Delta x(p)_j\}\rangle, \tag{2.4}$$

[7]The length of the sequence depends on the reconciliation direction and measurement type, *e.g.* for protocols with heterodyne detection $L = N$.

[8]Depending on the nature of the channel, more parameters may be required to be estimated, *e.g.* transmittance probability distribution $\tau(\eta)$ [108]

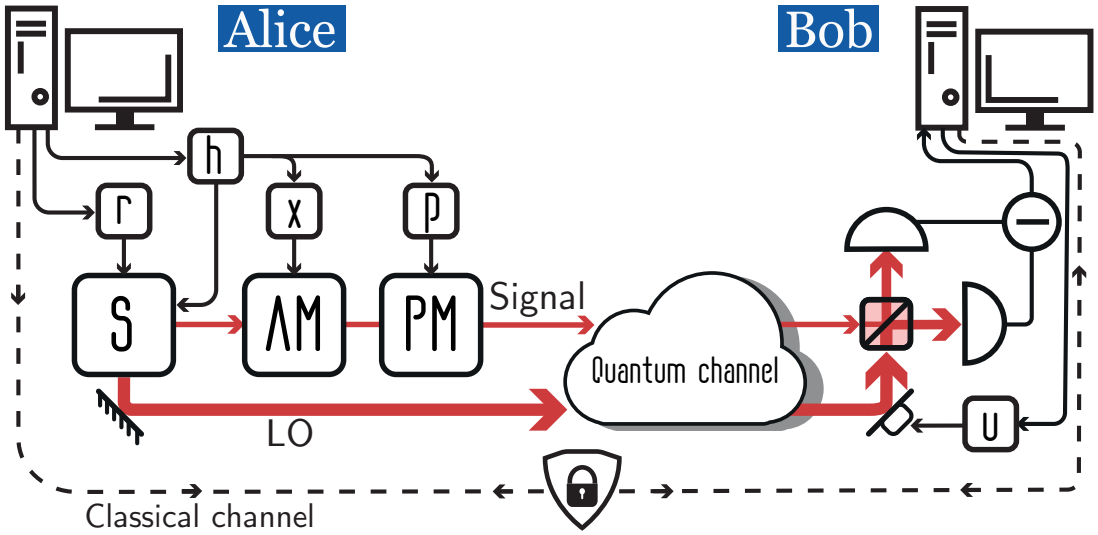


Figure 2.2: Operational scheme of a CV QKD protocol. Alice generates a quantum state (note that r can be adaptively changed based on channel parameters, in order to increase the rate of the protocol, see for example Ch.7). using source S and prepares it according to randomly generated (h, x, p) parameters using amplitude (AM) and phase (PM) modulators. Alice sends the signal along with local oscillator (LO) beam through quantum channel to Bob. The latter conducts the homodyne (or alternatively, the heterodyne) detection and advances to sifting, error correction and privacy amplification with Alice via classical authenticated channel.

where $\{.\}$ is the anti-commutator, and $\Delta x_i = x_i - \langle x_i \rangle$. Prior to modulation, carrier states are distributed around the origin of phase space and their overall source variance is:

$$\gamma_B^{squeezed} = \begin{pmatrix} 1/V_s & 0 \\ 0 & V_s \end{pmatrix}, \quad \gamma_B^{coherent} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.5}$$

for the squeezed[9]- and coherent-state, respectively. Note that Eqs.2.5 are valid only for perfect sources that output pure states, which is generally not the case [117] (see also Ch.3.1.4). The key bits are encoded[10] into the states, *i.e.* the latter are shifted on phase space according to the drawn variables from one (in case of squeezed states) or two (for coherent-states protocol) independent Gaussian distributions. The protocol does not assume strictly Gaussian modulation, as the final security analysis exploits Gaussian extremality [81] (see Sec. 2.1.4). Generally variance of each distribution may differ, but for simplicity we assume they are both equal to V_m. After the modulation the variance of signal state is:

[9] Without loss of generality we assume $\hat{x}$-quadrature squeezed states

[10] Unlike classical cryptographic systems, QKD does not require any encoding algorithms, since the string of data and the actual transferred message are the same. Trusted parties rely on authenticated classical noiseless channel during the stage of post-processing to obtain identical and secure keys. In further work by encoding we understand mapping of classical Gaussian random variable onto carrier quantum state.

$$\gamma_B^{squeezed} = \begin{pmatrix} 1/V_s + V_m & 0 \\ 0 & V_s \end{pmatrix}, \quad \gamma_B^{coherent} = \begin{pmatrix} 1 + V_m & 0 \\ 0 & 1 + V_m \end{pmatrix}. \tag{2.6}$$

Overall Alice's station outputs a thermal state with zero mean and the covariance matrix $\gamma_B = V\mathbb{1}$, where $\mathbb{1}$ is 2×2 unity matrix. Generally the squeezed state can be modulated in both quadratures, and variances of both quadrature need not be equal.

Aforementioned state preparation, also known as *prepare-and-measure* (P&M) is a conventional approach taken by majority of CV QKD protocols implementations, however theoretical analysis relies on the use of equivalent *entanglement-based* scheme (EPR). In the latter Alice and Bob share a bipartite state, which is however perturbed by Eve. The overall state shared by all involved parties is a pure state that aside from modes of Alice and Bob contains a number of additional modes attributed to Eve. The covariance matrix describing such a state is sufficient for the evaluation of (upper bound on) accessible information and consequently the impact of more general collective attacks (see Ch.2.1.3). Such description of a state offers a more intricate analysis of noise and losses present at trusted stations (see Ch.3.1.4 and 3.3.5).

In order to present state preparation in EPR scheme, it is first useful to recall the effect of partial measurement on a multipartite state in terms of it's first and second moments. Given a two-mode (with modes denoted as A and B) Gaussian state with mean values $d_A^{in} = (\langle x_A \rangle, \langle p_A \rangle)$ and $d_B^{in} = (\langle x_B \rangle, \langle p_B \rangle)$ and a covariance matrix

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{pmatrix}, \tag{2.7}$$

the homodyne detection of one of the modes, *e.g.* A in x quadrature, will alter the mean values of states in the remaining mode as [118, 119]

$$d_B^{\text{out}} = \sigma_{AB} \left(\boldsymbol{X}\gamma_A\boldsymbol{X}\right)^{MP} \left(D_A^{\text{out}} - d_A^{\text{in}}\right) + d_B^{\text{in}}. \tag{2.8}$$

The value of $D_A^{\text{out}} = (\langle x_A \rangle, 0)$ is obtained directly from the measurement results. The covariance matrix describing the state in the remaining mode is given by [54, 98]:

$$\gamma_B^{[x_A]} = \gamma_B - \sigma_{AB}^T \cdot \left(\boldsymbol{X}\gamma_A\boldsymbol{X}\right)^{MP} \cdot \sigma_{AB} \tag{2.9}$$

where in Eqs. 2.8 and 2.9 MP stands for Moore–Penrose pseudoinverse, T for transpose, and $\boldsymbol{X}$ (and superscript $[x_A]$) corresponds to the choice of the measured quadrature. To account for measurement of p quadrature $\boldsymbol{X}$ must respectively be substituted with $\boldsymbol{P}$, where both are given as:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \boldsymbol{P} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.10}$$

Equations 2.8 and 2.9 can be applied to the case of a multipartite state, be expanding the subsystem B. For (N+1)-mode overall state with $\gamma_{A,B_1,\cdots B_N}$, γ_B would be a $2N \times 2N$

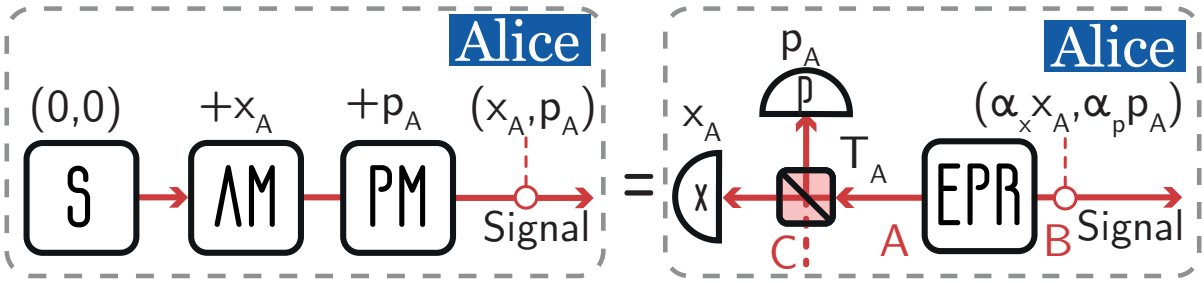


Figure 2.3: State preparation in CV QKD protocol. The prepare-and-measure method (left) involves direct displacement of the state on phase space, while the equivalent entanglement-based method (right) uses measurement of one of the modes of an EPR state to conditionally prepare the state in the remaining mode. Both methods are equivalent and (up to factors α_x and α_p) and directly correspond to each other. To alternate between the squeezed-, and the coherent- state protocol one can change the transmittance of the T_A to 1 or 1/2, respectively.

matrix, and σ_{AB} by a $2N \times 2$ matrix that describes the correlations of a measured state with the states in remaining modes $B_1, \cdots, B_N$.

Balanced heterodyne detection projects Bob's mode onto a coherent state, so that respective mean values are [119]

$$d_B^{[x_A,p_A]} = \sqrt{2}\sigma_{AB}\left(\gamma_A + \mathbb{1}\right)^{-1}\left(D_A^{\text{out}} - d_A^{\text{in}}\right) + d_B^{\text{in}}, \tag{2.11}$$

where $D_A^{\text{out}} = \left(\langle x_A\rangle, \langle p_A\rangle\right)$ are obtained directly from the measurement results. The covariance matrix of subsystem B turns to [119]:

$$\gamma_B^{[x_A,p_A]} = \gamma_A - \sigma_{AB}(\gamma_B^{\text{in}} + \mathbb{1})^{-1}\sigma_{AB}^T. \tag{2.12}$$

Now in the entanglement-based representation of CV QKD protocol, trusted parties share a state with a zero mean values $d_A = d_B = (0,0)$ and following covariance matrix [118]:

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{1} & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1} \end{pmatrix}, \tag{2.13}$$

where σ_z is the Pauli matrix

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.14}$$

Next, Alice keeps one mode (A) on her side and heterodynes it. Balanced heterodyne measurement will alter d_B and γ_B according to Eq.2.11 and 2.12, respectively.

Equivalently, the results of heterodyne measurement can be obtained by coupling, on (generally unbalanced) beamsplitter T_A, mode A to an ancillary system (mode C as shown on the right of Fig.2.3), with an initial covariance matrix of an overall tripartite state being $\gamma_{CAB} = \mathbb{1}_C \otimes \gamma_{AB}$. This changes γ_{CAB} as follows:

$$\gamma'_{CAB} = (S_{CA} \otimes \mathbb{1}_B)^T \gamma_{CAB} (S_{CA} \otimes \mathbb{1}_B) = \begin{pmatrix} \frac{V+1}{2}\mathbb{1} & \frac{V-1}{2}\mathbb{1} & \sqrt{\frac{V^2-1}{2}}\sigma_z \\ \frac{V-1}{2}\mathbb{1} & \frac{V+1}{2}\mathbb{1} & \sqrt{\frac{V^2-1}{2}}\sigma_z \\ \sqrt{\frac{V^2-1}{2}}\sigma_z & \sqrt{\frac{V^2-1}{2}}\sigma_z & V\mathbb{1} \end{pmatrix}, \tag{2.15}$$

where matrix S_{CA} describes a coherent combination of respective modes:

$$S_{CA} = \begin{pmatrix} \sqrt{T_A}\mathbb{1} & \sqrt{T_A}\mathbb{1} \\ -\sqrt{T_A}\mathbb{1} & \sqrt{T_A}\mathbb{1} \end{pmatrix}. \tag{2.16}$$

The results of concurrent homodyne detection of modes A and C of the tripartite state with γ'_{CAB} (2.15) is evaluated using Eqs.2.8, 2.9. One can first obtain covariance matrix describing bipartite state conditioned by measurement of *e.g.* mode C in p quadrature - $\gamma_{AB}^{[p_C]}$, and then from it the covariance matrix of single mode state $\gamma_B^{[x_A,p_C]}$ conditioned by measurement of both modes C and A in conjugated quadratures, respectively. This projects Bob's mode into a state with covariance matrix:

$$\gamma_B^{[x_A,p_C]} = \begin{pmatrix} \frac{\delta_A V+1}{V+\delta_A} & 0 \\ 0 & \frac{V+\delta_A}{\delta_A V+1} \end{pmatrix}, \tag{2.17}$$

where $\delta_A = (1-T_A)/T_A$. The mean values are obtained similarly

$$d_B^{[x_C,p_A]} = \left(\alpha_x x_A, \alpha_p p_A\right) = \left(\frac{\sqrt{T_A(V^2-1)}}{T_A V + (1-T_A)} x_A, \frac{\sqrt{(1-T_A)(V^2-1)}}{(1-T_A)V + T_A} p_A \right). \tag{2.18}$$

Setting $T_A = 1$ corresponds to the homodyne detection of mode A, which yields:

$$d_B^{[x_A]} = \sqrt{1-1/V^2}\left(\langle x_A \rangle, 0\right), \tag{2.19}$$

$$\gamma_B^{[x_A]} = \begin{pmatrix} 1/V & 0 \\ 0 & V \end{pmatrix}. \tag{2.20}$$

Gaussian state with mean 2.19 and covariance matrix 2.20 is a displaced x-squeezed state. Provided $V_s + V_m = V$ and $1/V_s = V$ and accounting for $\alpha_x = \sqrt{1-1/V^2}$ (the factor also becomes negligible for high V values) perfect correspondence between prepare-and-measure and entanglement-based schemes of squeezed-state protocols can be established.

Setting $T_A = 1/2$ corresponds to the balanced heterodyne measurement, and conse-

quent preparation of a coherent state $\gamma_B^{[x_A,p_A]} = \mathbb{1}$, displaced by

$$d_B^{[x_A,p_A]} = \sqrt{2\frac{V-1}{V+1}}\,(x_A,\, p_A)\,.$$

This preparation via measurement, with respect to factor $\sqrt{2(V-1)/(V+1)}$ is equivalent to P&M scheme of a coherent-state protocol.

2.1.3 Adversary

One of the basic assumptions about the quantum channel is that it completely lies in the domain of influence of Eve. She can do with channel anything quantum mechanics allows and Alice and Bob could not detect. Ultimately, her goal is to obtain the copy of the key avoiding the termination of the protocol. Alice and Bob always upper bound on Eve's influence and accessible information, hence Eve has to devise a strategy that would allow key acquisition regardless. Currently known optimal attack strategies are undoubtedly challenging to implement even with state-of-the-art technologies, however for the highest security to be future-proof one cannot rely on technological limitations. This forces trusted parties to resort to certain assumptions about Eve's resources and power:

- Eve has full access to the quantum channel and can perform any operation permitted by the laws of physics.
- Eve can freely copy and monitor the information flow in classical channel, but without violating the authentication.
- Eve's computational power is unbounded.
- Eve cannot control trusted stations (both from outside and inside).

The latter implies that devices are operating as intended and thus are trusted, however such assumption can be fully or partially omitted in device-independent or measurement-device independent protocols [120, 121]. Alleviation of the first two assumptions would make the whole process of secure key distribution unfeasible, and as such they are minimum necessary for the QKD protocols.

Untrusted channel

The choice of the channel used by trusted parties depends on the convenience of implementation and scale of targeted application. While fiber channels can be suitable for majority of applications, the cost of infrastructure and inflexibility can be a significant obstacle for some networks. One can expect that wide-scale network in near future will combine fiber channels, and atmospheric channels in a form of short links between trusted parties in urban areas, or long-range links on global scale via intermediate trusted nodes on satellites.

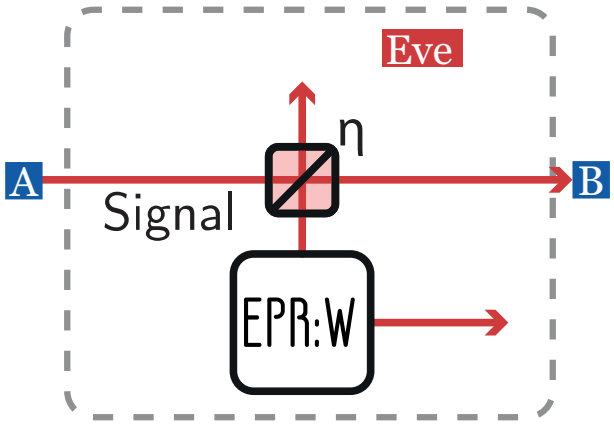


Figure 2.4: Model of a Gaussian noisy channel. Eve can combine the signal with one of the modes radiated by an EPR source, and store the latter (along with the second mode radiated by the source) for a measurement based on the eavesdropped classical communication. The respective states are characterized by the variance $W = 1+\epsilon/(1-\eta)$, where η is channel transmittance, and ϵ is the excess noise, estimated by trusted parties.

Fiber channel. In current work we assume that Eve can substitute the real link between Alice and Bob and simulate a noisy channel between them. Generally, the channel does not have to be Gaussian, however the extremality of Gaussian states (see Sec.2.1.4) allows us to use Gaussian channel models to discuss basic protocol performances. More specifically as an interaction of the signal with a thermal state of variance $W = 1+\epsilon/(1-\eta)$ on a BS η, as in Fig. (2.4), resulting in covariance matrix of the trusted state (*i.e.* the state shared between the trusted parties) to become:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{1} & \sqrt{\eta(V^2-1)}\sigma_z \\ \sqrt{\eta(V^2-1)}\sigma_z & \left[1+\eta(V-1)+\epsilon\right]\mathbb{1} \end{pmatrix}, \tag{2.21}$$

where η is the channel transmittance, and ϵ is the excess noise referred to the output of the channel[11]. Channel estimation is required to determine all elements the covariance matrix, which consequently allow to assess the security of the protocol.

The model is successfully applied to the description of fiber-optics channels, however one must be wary of effects (phase noise [122], crosstalk in a multimode signal [123] or with multiplexed simultaneous classical communication [124], *etc.*) encountered in real experimental fiber-based systems. Such effects, if overlooked, may increase attenuation and noise, and consequently lead to security misestimation.

Aside from the overall ability to establish secure key distribution between trusted parties and the profile of the key rate function depending on transmittance, an important figure of merit in such channels is the distance up to which the protocol maintains a relatively high key rate (before the substantial drop, typical for the key rate dependence), which almost coincides with the secure distance *i.e.* maximal length of the fiber channel that still permits key distribution. Typical telecom fiber admits $0.2\,dB$ of loss per

[11] Excess noise can also be considered at the input of the channel. In such a case it is scaled by the transmittance.

kilometer [125], which can be translated into transmittance:

$$\eta_{fiber} = 10^{-0.02d}, \tag{2.22}$$

where d is the length (in km) of the fiber link between trusted parties. This results in losses at 100 km to be $\eta = 0.1$ which will lower the variance of the state at the input from *e.g.* $V_{\text{input}} = 20$ to $V_{\text{output}} = 2.9$ provided no excess noise is present.

Free-space channel. Eve can employ more sophisticated strategy that would demand trusted parties to estimate more parameters. An example of such channel is channel that exhibits transmittance fluctuations which are non-negligible over the course of generation of a single data block. The fluctuations are described by a distribution $\tau(\eta)$, and the channel can be deconstructed as a set of *subchannels* $\{\eta_j\}$ [126]. A subchannel here is understood as a channel where transmittance fluctuations are negligible, and which occurs with probability $\tau(\eta_j)$, provided $\sum_{j=1}^{\infty} \tau(\eta_j) = 1$. The Gaussian Wigner function of a state after a fading channel is a sum of Winger functions after all individual subchannels [108]. Therefore the trusted state γ'_{AB} is now classically non-Gaussian being a mixture of states with zero mean and covariance matrix γ^j_{AB} after each subchannel. Thus, the covariance matrix of the shared state γ'_{AB} can be obtained by averaging over fluctuating transmittance values. This significantly simplifies the analysis of the channel, as it does not require the explicit determination of $\tau(\eta)$, but rather it's covariance matrix statistical properties. For the states with zero mean values, only the mean value of transmittance $\langle\eta\rangle$, and mean value of square root of transmittance $\langle\sqrt{\eta}\rangle$ are needed [108, 126], since after individual subchannel covariance matrix (2.23) is

$$\gamma^j_{AB} = \begin{pmatrix} V\mathbb{1} & \sqrt{\eta_j(V^2-1)}\sigma_z \\ \sqrt{\eta_j(V^2-1)}\sigma_z & (1+\eta_j(V-1)+\epsilon)\mathbb{1} \end{pmatrix}, \tag{2.23}$$

and after the overall channel covariance matrix averages to:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{1} & \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z & (1+\langle\eta\rangle(V-1)+\epsilon)\mathbb{1} \end{pmatrix}. \tag{2.24}$$

Relevant properties of $\tau(\eta)$ constitute the *fading variance*:

$$Var(\sqrt{\eta}) = \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2. \tag{2.25}$$

It was shown, that if parameters $\langle\eta\rangle$ and $\langle\sqrt{\eta}\rangle$ of the fluctuating channel are known to Alice and Bob, the channel can be considered as the one with fixed attenuation $\langle\sqrt{\eta}\rangle^2$, but additional variance-dependent excess noise $\epsilon_f(\tau(\eta), V_s, V_m) = Var(\sqrt{\eta})(V_s + V_m - 1)$ [108].

Composite channel is a combination of channels with fixed and fluctuating transmittances. While there can be numerous configurations of said channels, the overall

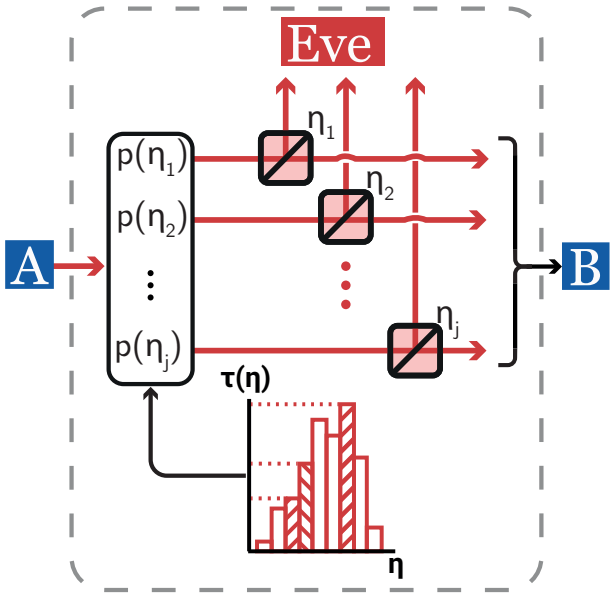


Figure 2.5: Non-Gaussian channel with transmittance fluctuations can be decomposed into a set of Gaussian subchannels $\{\eta_j\}$ according to transmittance probability distribution $\tau(\eta)$. The signal has the probability $p(\eta_j)$ to be transmitted via individual subchannel.

covariance matrix describing the state received by Bob is:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{1} & \langle\sqrt{\eta}\rangle\sqrt{\eta_{comb}(V^2-1)}\sigma_z \\ \langle\sqrt{\eta}\rangle\sqrt{\eta_{comb}(V^2-1)}\sigma_z & (\gamma_B - \mathbb{1})\langle\eta\rangle\eta_{comb} + (1+\epsilon_+)\mathbb{1} \end{pmatrix}. \tag{2.26}$$

where $\eta_{comb} = \prod_i^N \eta_i$ is product of all transmittance values of all N channels with fixed losses, $\langle\eta\rangle$ and $\langle\sqrt{\eta}\rangle$ are given by the overall transmittance probability distribution, and ϵ_+ is a total excess noise (being the sum of noises infused by each channel, and accounting for scaling within each channel), and received by Bob. Even though Alice and Bob may not be able to distinguish, and properly attribute losses and noise to each individual channel, they are only required to estimate each time the overall loss $\eta_{comb}\,\eta_j$, and total excess noise ϵ_+ imposed on the state that arrives to the Bob's side.

An example of such channel can be an urban QKD network that combines both types of channels, utilizing an atmospheric channel to connect two distant parties without the necessity of expensive fiber-optical infrastructure, and extending the network using fiber links where necessary.

Attack strategy

Overall eavesdropping strategies (depicted in Fig. 2.6) can be split into 3 classes: *individual* and *collective* attacks [51,78–80], and the most general *coherent* attacks [90,127,128]:

1. An *individual attack* corresponds to class of attacks when Eve interacts with each quantum state independently, stores her probe states in a quantum memory until the sifting step of the protocol, and further proceeds to individually measure each stored state in correct basis (quadrature).

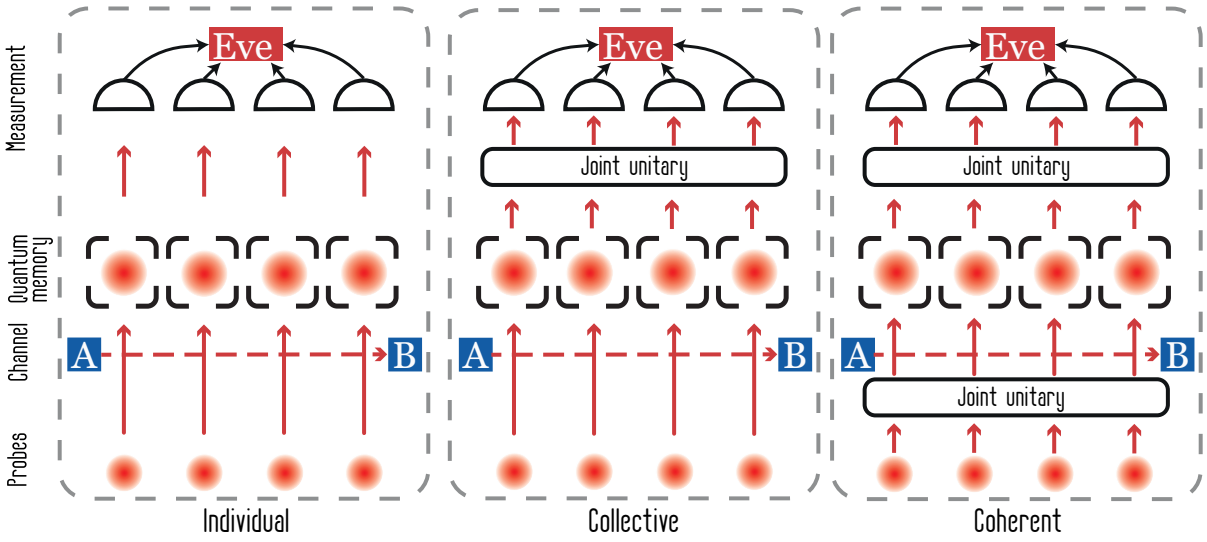


Figure 2.6: During individual attack (left) Eve prepares a sequence of probe-states that individually interact with the signal, then stored in quantum memory until Eve obtains additional information from eavesdropping the classical channel, and finally measures each probe individually. Collective attack (middle) allows Eve to perform global measurement over the whole ensemble of probe states, whereas coherent attack (right) additionally allows to prepare the probe states in a global optimal entangled state, and probe all signal states jointly.

2. During *collective attack* Eve interacts with each quantum state independently, stores the probes in a quantum memory, but can perform optimal collective measurement on the whole stored state (after post-processing has been commenced).

3. *Coherent attack* is the most general conceivable attack, where Eve is allowed to explore the entanglement of the states. Similarly to collective attack she can store the probes in a quantum memory and conduct collective measurement after post-processing step.

Attacks, stated above, do not presume any specific currently achievable implementations (nor any whatsoever), but rather they define the security bounds that can be in principle saturated by potential implementation [118, 129]. In case of individual attacks the optimal approach for Eve is a Gaussian attack, that can, in fact, be realized in numerous ways. A well-known example is an optimal *entangling cloner* attack [118], where Eve radiates an TMSV state of variance W in two modes $E_{1,2}$:

$$\gamma_{E_1E_2} = \begin{pmatrix} W\mathbb{1} & \sqrt{W^2-1}\sigma_z \\ \sqrt{W^2-1}\sigma_z & W\mathbb{1} \end{pmatrix}, \tag{2.27}$$

and forces one of the resulting modes E_1 (as depicted on upper left scheme in Fig. 2.7) to interact with the signal mode on BS that corresponds to channel transmittance η. This

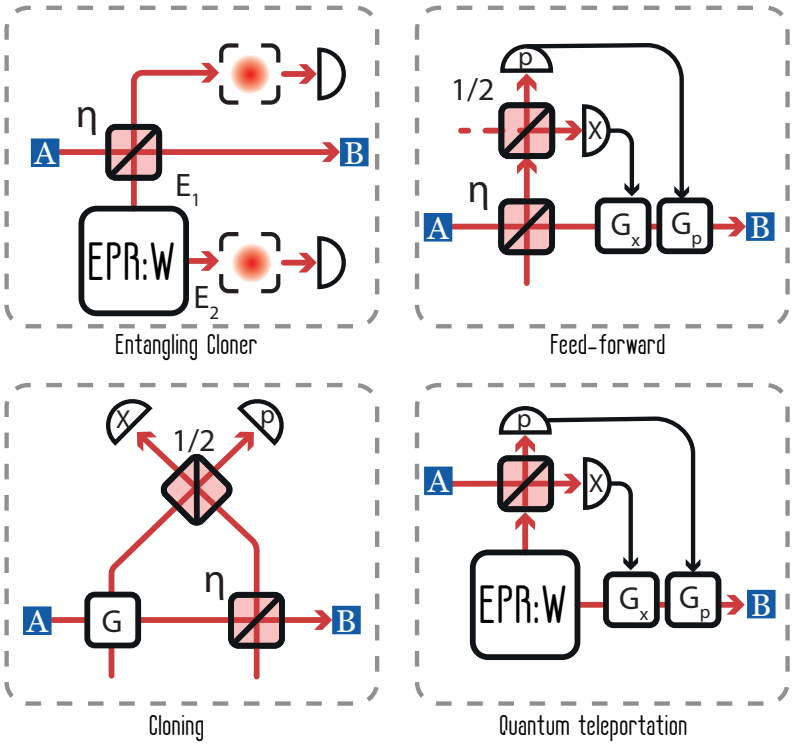


Figure 2.7: Examples of individual attacks: entangling cloner (top-left), feed-forward (top-right), cloning (bottom-left), and teleportation (bottom-right) attacks.

changes the trusted state to:

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{1} & \sqrt{\eta(V^2-1)}\sigma_z \\ \sqrt{\eta(V^2-1)}\sigma_z & (\eta V + [1-\eta]W)\mathbb{1} \end{pmatrix}. \tag{2.28}$$

Proper adjustment of the variance of Eve's state $W = 1+\epsilon/(1-\eta)$, would make Alice and Bob perceive the channel as the one with thermal noise ϵ, as in Eq.(2.23). During each round of the protocol Eve should also make use of the QM to store states in both modes until proper measurement basis would be disclosed via classical channel. Measurement of E_2 allows Eve to conditionally reduce the noise in the entangled mode E_1 ($W \to 1/W$). Such approach allows Eve to saturate the maximally achievable information for DR and RR scenarios, for both the squeezed- and the coherent-state protocols on Bob's side.

The entangling cloner, along with other examples of individual attacks, feedforward, cloning, and quantum teleportation attacks [130, 131], are depicted in Fig.(2.7). The feedforward attack relies on Eve tapping the channel, performing the heterodyne detection and based on the outcome applying adjustment to the signal mode. Cloning attack involves the use of phase-insensitive linear amplification, followed by attenuation and heterodyne detection. The quantum teleportation attack, similarly to entangling cloner, is based on the use of an EPR-source, one mode of which is coupled to the signal and heterodyned, while the other is linearly amplified (with gain in each quadrature governed by the measurement results) and sent to Bob.

Overall it is considered for coherent attacks to be the most powerful, with collective

attacks being less powerful, and individual the least efficient ones. However it was shown that collective attacks can be as effective as any coherent attack against certain QKD protocols [79–81,87,95]. In some channels optimal attacks are further reduced to individual, *e.g.* noiseless Gaussian channels in CV QKD (or depolarizing channels for BB84), however this is generally not the case.

The framework for operation of collective attacks has been successfully developed [132], and many experimental implementations claim the security against coherent attacks, however optimal approach for an adversary has not been identified yet, not to mention experimental implementations. Recently, based on entangling cloner, a hybrid attack, that combines individual and collective attacks, on coherent-state with heterodyne detection (no-switching) protocol has been devised [133]. It was shown that even without restrictions on the volume of Eve's QM, the reasonable assumptions regarding the storage time [134, 135] can remarkably force Eve to resort to individual attacks (which do not require QM for such protocol) thus significantly improving the expected security of the protocol.

Security analysis of individual attacks, even though being seemingly the weakest, can provide useful insights and verify that some protocols are not secure beyond complete break of entanglement. Despite the emergence of coherent attack analysis techniques [136], analysis of collective attacks is still crucial as it provides common ground for comparison of performance of main QKD protocols.

2.1.4 Security

Statement that QKD protocol is secure implies ϵ-*security*, meaning there's always a non-vanishing probability ϵ that the protocol does not abort during one of the steps *and* Eve obtains information on a shared key [89]. The joint state of the classical key S (given by the probability distribution P_S) and quantum system of the unauthorized party ρ_E^s (provided the key $S = s$ for any element s of the key space $\mathcal{S}$) can be written as:

$$\rho_{SE} := \sum_{s\in\mathcal{S}} P_S(s)|s\rangle\langle s| \otimes \rho_E^s, \tag{2.29}$$

with $\rho_S = \sum_{s\in\mathcal{S}} P_S(s)|s\rangle\langle s|$ being the operator representation of a classical distribution P_S [32] with respect to orthonormal basis $\{|s\rangle\}_{s\in\mathcal{S}}$ on Hilbert space $\mathcal{H}_S$ [94]. One can claim that the key S is uniformly distributed and independent of the adversary with probability $1-\epsilon$, if the similarity[12] between a real system ρ_{SE} and an ideal one, where (maximally mixed) key state $\rho_U = \sum_{s\in\mathcal{S}} \frac{1}{dim(\mathcal{S})}|s\rangle\langle s|$ on Hilbert space $\mathcal{H}_S$ is independent from an arbitrary state of the adversary ρ_E on $\mathcal{H}_E$:

$$\frac{1}{2}\|\rho_{SE} - \rho_U \otimes \rho_E\|_1 \leq \epsilon. \tag{2.30}$$

The definition (2.30), follows the universal composability framework [137] and has

[12]Here the similarity is meant as the trace norm $\|\rho\|_1 := \mathrm{tr}(|\rho|)$ of a hermitian operator ρ. Trace norm is a quantum equivalent of total variation distance between two probability distributions, also denoted as L_1-distance.

been presented by R. Renner in his PhD thesis [89]. Note that such definition applies to both DV and CV systems, since the keys of the latter are discretized and occupy a finite key space [89]. While previously used security definitions, based on accessible information [138], agree with Eq. (2.30), they were not sufficient to claim security in any arbitrary context, *i.e.* they were not *composably* secure [139]. The latter can be understood as the ability to establish a security bound on the protocol that consists of ϵ_i-secure subprotocols, so that the overall protocol is $\epsilon \leq \sum_i \epsilon_i$ secure.

In the current work we assume ϵ to be sufficiently small, and view the security of QKD protocol as the ability to extract fully secure key after all the steps of the protocol. Hence the security is defined in terms of positivity of the *key rate*:

$$R \equiv \frac{l_{final}}{N} > 0, \tag{2.31}$$

where, following previous notations, N is the amount of states sent (rounds of the protocol), and l_{final} is the size of the final (errorless and decorelated from the third party) secure key. Generally evaluation of ϵ-secure l_{final} requires the knowledge of smooth-min entropy relative to limited precision due to finite N value, however in asymptotic regime, where collective attacks have been shown (for majority of CV QKD protocols) to be optimal [79–81, 87], the key rate reduces to well-known [32] expression:

$$R_{coll.}^{assymp} = \max\left[0, I_{AB} - \chi_E\right], \tag{2.32}$$

where I_{AB} is the upper bound on the mutual information trusted parties can extract from the shared state (provided reconciliation is perfect), and χ_E is the quantum analogue of mutual information, Holevo bound, which upper limits the amount of information on the key that can be contained within the state of Eve. Provided Eve implements individual attacks, the key rate (2.32) can be further reduced to [140]:

$$R_{ind.}^{assymp} = \max\left[0, I_{AB} - I_E\right], \tag{2.33}$$

where I_E is the mutual information of Eve with respective trusted party. Proving security against individual attacks may not be sufficient, but it is useful to estimate security bounds and can provide valuable insights regarding the inapplicability of protocols in various conditions.

However, the bound on the mutual information set by I_{AB} is never reachable in practice, where error correction procedure unavoidably consumes part of the shared data, so the limited error-correction efficiency β (also referred to as post-processing efficiency) has to be introduced into the key rate bound as well, so that:

$$R_{coll.} = \max\left[0, \beta I_{AB} - \chi_E\right]. \tag{2.34}$$

Here $\beta \leq 1$ (in practice being close to 95% for Gaussian-distributed or approximately Gaussian-distribution data [141]) and illustrates inability to extract information at exactly the Shannon limit. Furthermore one can also account for speed α_s of error correction that

can deny real-time implementations, and the frame error rate (FER):

$$R_{coll.} = \max\left[0, \alpha_s(1 - \mathrm{FER})(\beta I_{AB} - \chi_E)\right].$$

Practically the speed factor is evaluated as ratio $\alpha = D_{EC_{out}}/D_{EC_{in}}$ between error correction output rate $D_{EC_{out}}$ and data output rate of the system *i.e.* the input of error correction [142]. Frame error rate is the probability of incorrect message decoding, that leads to data discard. Error correction speed and FER are linked since the increase of the latter enables the increase of the former [142]. However, it is commonly assumed for $\alpha_s(1 - \mathrm{FER}) = 1$, as it merely reduces the key rate and doesn't alter the dependencies on parameters of the protocol. There are other important effects that should be taken into account with the most essential being the finite-size effects (see Chapter 3.34).

The term βI_{AB} can be efficiently determined directly from data sets generated on trusted sides, with the $\beta = r^{\mathrm{code}}/C_{\mathrm{channel}}$, where r^{code} is the rate of the reconciliation code [142] and C_{channel} is the channel capacity that depends on SNR [143]. The main concern is actually the second term of Eq. (2.34), *i.e.* the Holevo bound. However, there's an elegant way of evaluation of the quantity that relies on the use of entanglement-based representation. In the most conservative approach all impurities of the trusted state ρ_{AB} are attributed to Eve, so that $\mathrm{tr}(\rho_{ABE}) = 1$. Utilizing the properties of the Von Neumann entropy (defined as $S(\rho) = -\mathrm{tr}[\rho \log_2 \rho]$), one can immediately claim $S(\rho_{AB}) = S(\rho_E)$ to be true, which implies that any information accessible to Eve is in fact given by the density matrix of the trusted state ρ_{AB}. Finding the explicit value of quantum mutual information of bipartite quantum system $S(a : b)$ is a non trivial task. Fortunately, making use of subadditivity of Von Neumann entropy, as well as, the fact that unitary interactions do not alter the entropy[13] one can show that quantum mutual information cannot exceed the Holevo bound $S(a : b) \leq \chi$ [144]. The latter is given by

$$\chi = S(x : Y) = S(\rho_Y) - \sum p(x) S(\rho_Y^x), \tag{2.35}$$

where ρ_Y^x is a state of system Y conditioned by the measurement on system x.

The assertion that optimal choice of states for an attack are, in fact, Gaussian states stems from the inequality

$$f(\rho) \geq f(\rho^G),$$

where f is a continuous, strongly superadditive and invariant under local unitaries function, while ρ^G is a *gaussified* version of ρ, *i.e.* Gaussian state with the same first and second moments as ρ. In terms of Von Neumann entropy the inequality turns to

$$S(\rho) \leq S(\rho^G),$$

meaning that Guassian states maximize the entropy. This notion is also known as *extremality of Gaussian states* [81]. Finally, one can use Williamson theorem [145] to reduce the problem to calculation of symplectic eigenvalues of finite covariance matrices and ob-

[13] Since eigenvalues of the density matrix of the state remain the sames under unitary operations

tain the upper bound on the knowledge Eve will have on the key shared by trusted parties. Since in the Gaussian approximation mean values of the states are irrelevant (as displacement is a unitary transformation), such method requires solely the reconstructed covariance matrix γ'_{AB} (after the interactions in the untrusted channel) for full security analysis.

Stated formulation of the security proofs suggests that a key is secure if trusted parties share more information between themselves than an eavesdropper can have with either of them. Since the flow of quantum states is from Alice to Bob, it is natural [51] for classical information to be transferred in the same direction (steps 4-7). The protocol where Alice is sending classical information to Bob, and the latter corrects his key elements, trying to infer the values originally encoded by the former, is called *Direct Reconciliation* (DR). In this case the lower bound on the key rate:

$$\begin{aligned} R^{\rightarrow}_{ind} &= \max\left[0, \beta I_{AB} - I_{AE}\right]; \\ R^{\rightarrow}_{coll} &= \max\left[0, \beta I_{AB} - \chi_{AE}\right]; \end{aligned} \tag{2.36}$$

However leaving Alice as a reference side allows Eve to easily compromise the security of CV QKD protocol when channel transmittance falls below $\eta < 0.5$. Since Eve gets to keep bigger part of every transmitted beam, it is clear she will then be able to infer more information than Bob.

A more robust approach would be to reverse the flow of classical information, and make Alice infer the value measured by Bob. The protocol where Bob is the reference side, and is sending the corrections to Alice is called *Reverse Reconciliation* (RR) [146]. In this case lower bound on the key rate becomes:

$$\begin{aligned} R^{\leftarrow}_{ind} &= \max\left[0, \beta I_{AB} - I_{BE}\right]; \\ R^{\leftarrow}_{coll} &= \max\left[0, \beta I_{AB} - \chi_{BE}\right], \end{aligned} \tag{2.37}$$

and it can be verified that CV QKD protocol can be in principle established over noiseless channel with arbitrary amount of loss.

Taking into account aforementioned purification of trusted state by Eve, and properties of Von Neumann entropy, the Holevo bound (2.35) can be rewritten as:

$$\begin{aligned} \chi_{AE} &= S(b:A) = S(AB) - S(B|A); \\ \chi_{BE} &= S(a:B) = S(AB) - S(A|B), \end{aligned} \tag{2.38}$$

where $S(AB)$ is the Von Neumann entropy of the shared trusted state ρ'_{AB}, and $S(A|B)$, $S(B|A)$ are, respectively, the entropies of $\rho_{A|B}$ and $\rho_{B|A}$, the states of a trusted subsystems, conditioned by the measurement performed on another trusted subsystem. The secure key rates in Eqs.(2.36,2.37) for collective attacks can therefore be expressed solely dependent on the covariance matrix γ'_{AB} of a state shared between Alice and Bob:

$$\begin{aligned} R^{\rightarrow}_{coll} &= \max\left[0, \beta I_{AB} - S(AB) + S(B|A)\right]; \\ R^{\leftarrow}_{coll} &= \max\left[0, \beta I_{AB} - S(AB) + S(A|B)\right]. \end{aligned} \tag{2.39}$$

The general approach to composable security estimation against coherent attacks on an arbitrary CV QKD protocol remains an open problem. One of the approaches employs entropic uncertainty principle to achieve composable security proof [90, 128], although it is applicable only to the squeezed-state protocol and requires intensity monitoring of the incoming signal [91]. Another approach, applicable to the coherent-state protocol with heterodyne detection, first proves the protocol is ε-secure against Gaussian collective attacks [94], and then employs Gaussian de Finetti reduction to prove that the same protocol is $\widetilde{\varepsilon}$-secure (where security parameter $\widetilde{\varepsilon}$ is polynomially larger than ε [133]) against general coherent attacks [95]. In the asymptotic regime the lower bound on the composable secret key rate for Gaussian collective and coherent attacks coincide [94]. The analysis of collective attacks continues to be a benchmark for comparison of the performance of various CV QKD protocols.

2.2 Gaussian protocols family

The choice of signal state, measurement on receiver side, as well as reconciliation direction spawns a family of 8 one-way Gaussian CV QKD protocols. All protocols can be described in terms of entanglement-based scheme as depicted in Fig.(2.8). In the following section we do not account for numerous effects influencing real protocols (*e.g.* limited post-processing efficiency, which is set to theoretical maximum $\beta = 100\%$) with a sole intent to briefly compare each protocol in terms of secure key rate dependency on the channel losses, and noise tolerance. We're interested not only in the maximal tolerable attenuation or noise, but also in the slope of the key rate function that determines tolerance to losses. Due to inherently different range of tolerable attenuation we separately compare direct and reverse reconciliation protocols.

2.2.1 Direct Reconciliation

Purely lossy untrusted channel.

Let us first look at the simplest case of noiseless channel $\epsilon = 0$, as depicted in Fig.2.9a. Such reconciliation imposes fundamental limitation on maximal loss since both Bob and Eve want to reconstruct encoded key data, and the advantage is granted to a party that collects bigger share of the signal state. Hence, if the channel attenuation reaches or exceeds $3dB$ (*i.e.* $\eta \geq 1/2$) no key can securely be generated between Alice and Bob.

If Alice decides to use the coherent state modulated in both quadratures during each round of the protocol (also known as no-switching protocol [130]), Bob's original incentive may be to measure both quadratures of the incoming state. However, the key rate of such protocol (dashed green line on Fig.2.9a) quickly diminishes with increasing loss and, even in such idealized conditions, no key can be generated if $\eta > 1.3dB$. This is due to inevitable (vacuum) noise addition during heterodyne detection that hinders the ability of the receiver side to reconstruct an encoded key data [104] (see Chap.3.3.5 for further details regarding detection noise). By resorting to homodyne detection (dashed orange

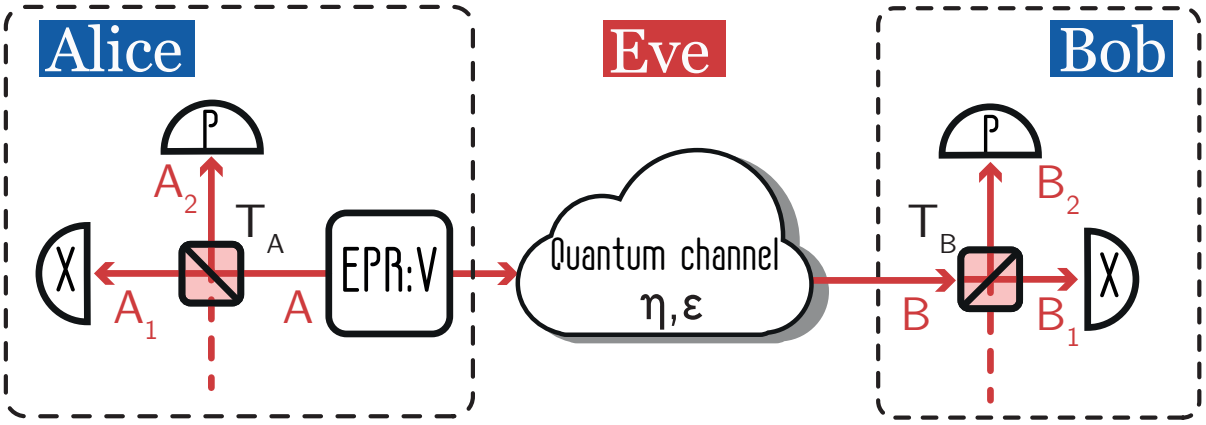
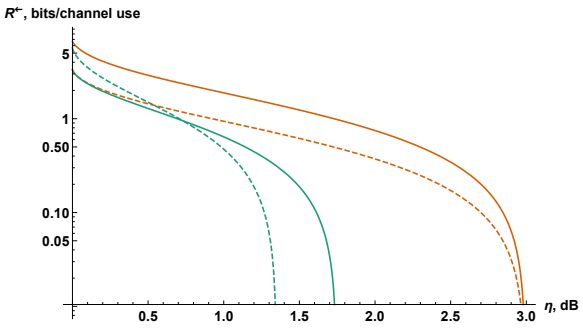


Figure 2.8: Entanglement-based scheme of a Gaussian CV QKD protocol. An *EPR* source radiates states into modes A and B, the states in the latter are sent through untrusted channel (where they are subjected to losses η and noise ϵ) to Bob. Beam-splitters on trusted sides can typically take values $T_{A(B)} = 1$ or $1/2$. Unity transmittance corresponds to the choice of homodyne detection of the incoming state. Interaction with a vacuum state on a balanced BS on trusted side implies the use of heterodyne detection, that is modeled as conjugate homodyne detection of both output ports of respective BS. Trusted parties can use either the squeezed-state protocol ($T_A = 1$), or the coherent-state protocol ($T_A = 1/2$), amassing the key data during each round from either single quadrature ($T_B = 1$), or both quadratures ($T_B = 1/2$). Additionally, trusted parties can agree beforehand on the reconciliation side (DR or RR), thus making 8 possible implementation of a CV QKD protocol.

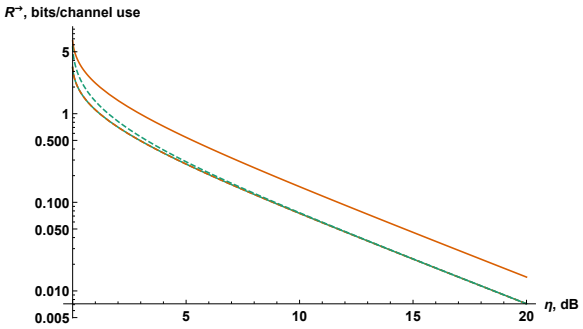
line) trusted parties lose the information from one of the quadratures, which in lossless channel would almost halve a secure key rate. However, avoiding additional noise on the receiver side proves to be beneficial with increasing losses and allows to ultimately tolerate up to the fundamental maximum of $3dB$.

Alternatively, Alice can choose to send to Bob a sequence of squeezed states each modulated in a single quadrature. In such scenario robustness to channel attenuation is again impaired by the noise added on the receiver side. The choice of heterodyne detection (solid green line) leads to a rapid decrease of the key rate with accumulating loss. Note that in low loss regime, unlike the coherent-state protocol, acquisition of information simultaneously from both quadratures of the squeezed state is not advantageous, since the measurement of the anti-squeezed quadrature does not contribute to the overall key rate, while the coupling to the vacuum state during heterodyne detection merely reduces the amount of squeezing in the contributing (squeezed) quadrature. Interestingly, in low loss regime the squeezed-state protocol yields smaller key rate than the coherent-state protocol with heterodyne detection, however the former proves to be more robust against losses than the latter. Lastly, the choice of squeezed states and homodyne detection (solid orange line) extends the applicable range of losses up to the fundamental maximum, and furthermore grants highest overall key rate and robustness against losses comparing to all other protocols.

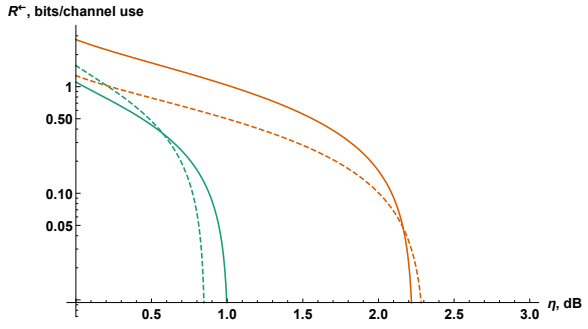
Noisy untrusted channel.



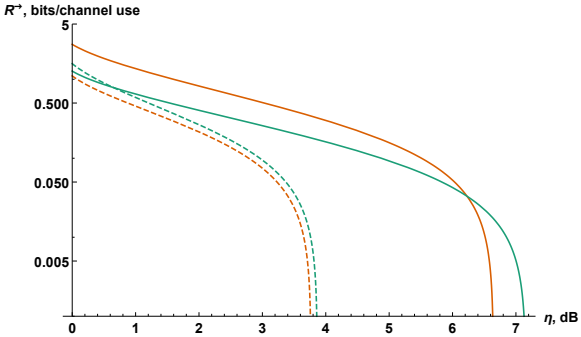
(a) DR protocols in noiseless channel



(b) RR protocols in noiseless channel



(c) DR protocols in noisy channel



(d) RR protocols in noisy channel

Figure 2.9: Comparison of the lower bounds on the key rate of CV QKD protocols with direct (left) and reverse (right) reconciliation in noiseless channel $\epsilon = 0$ (top) and noisy channel $\epsilon = 10\%$ (bottom). Protocols depicted are: the squeezed-state (solid lines), the coherent-state (dashed) protocol, with homodyne (orange lines) or heterodyne (green lines) measurement. State variance is close to asymptotic value $V = 100$ shot noise units (SNU), post-processing assumed to be perfect $\beta = 100\%$. In case of RR in noiseless channel, result for the squeezed-state protocol and heterodyne detection overlaps with the coherent-state protocol and homodyne detection.

Figure 2.9c shows the effect of the large excess noise $\epsilon = 10\%$ (at the receiver, *i.e.* not scaled by the channel transmittance) on DR CV QKD protocols. Evidently, such noise reduces tolerance to loss, and consequently the range of attenuation that permits secure key distribution.

The coherent-state protocol with heterodyne detection may yield comparatively high quantitative key rate in almost perfectly transmitting channel, but as transmittance diminishes so does the key rate (quickest than for any other protocol), ending up with the smallest tolerable attenuation. On the other hand, the choice of homodyne detection allows to avoid additional noise on the receiver side and hence retain tolerance (similar to the one in a purely lossy channel) to loss, resulting in highest maximum tolerable attenuation value among all protocols.

The heterodyne detection of squeezed states sent via noiseless channel will yield the lowest key rate comparing to any other choice of carrier states or detection in channels with high transmittance. The heterodyne measurement harms the mutual information between trusted parties, but does not affect Eve's information on Alice data, while measurement of the anti-squeezed quadrature has a negligible contribution. As the losses in the channel accumulate the rate rapidly drops, although, not as quickly as of aforementioned coherent-state protocol with heterodyne detection. This is mainly due to amount of mutual information trusted parties generate by measuring squeezed quadrature, variance of which remains of sub-shot noise level regardless of heterodyne detection by Bob.

As already mentioned, the choice of measuring a single quadrature allows to avoid additional noise (and observed squeezing reduction), and consequently maintain excess noise tolerance and robustness to losses provided by squeezed states. Said advantages support generation of more bits per channel use, although the rate drops quicker than that of the homodyned coherent-state protocol. The latter can be explained by higher noise tolerance of the coherent-state protocol as illustrated in Fig.2.10(left). The tolerance to noise, and subsequently maximal attenuation can be influenced by addition of a trusted noise on the sender side [104]. Such trusted preparation noise can improve the tolerance to untrusted channel noise, so that the closer the latter is to maximally tolerable level the more improvement in terms of secret key rate increase can be expected. For further details see Ch. 3.1.4.

2.2.2 Reverse Reconciliation

Purely lossy untrusted channel.

The optimal approach for trusted parties is to let Bob be a reference side *i.e.* for Alice to correct data on her side according to the measurement outcomes of the former. Such assignment of roles allows to maintain operation after arbitrary amount of loss in a noiseless channel, which can be seen in Fig.2.9b, where further increase of loss η would not lead to a security break regardless of the protocol used. Two protocols with the lowest key rate have fully equivalent loss tolerance and quantitative key generation rate: the coherent-state protocol with homodyne detection (dashed orange line) and the squeezed-state protocol with heterodyne detection (solid green line). The former does not utilize

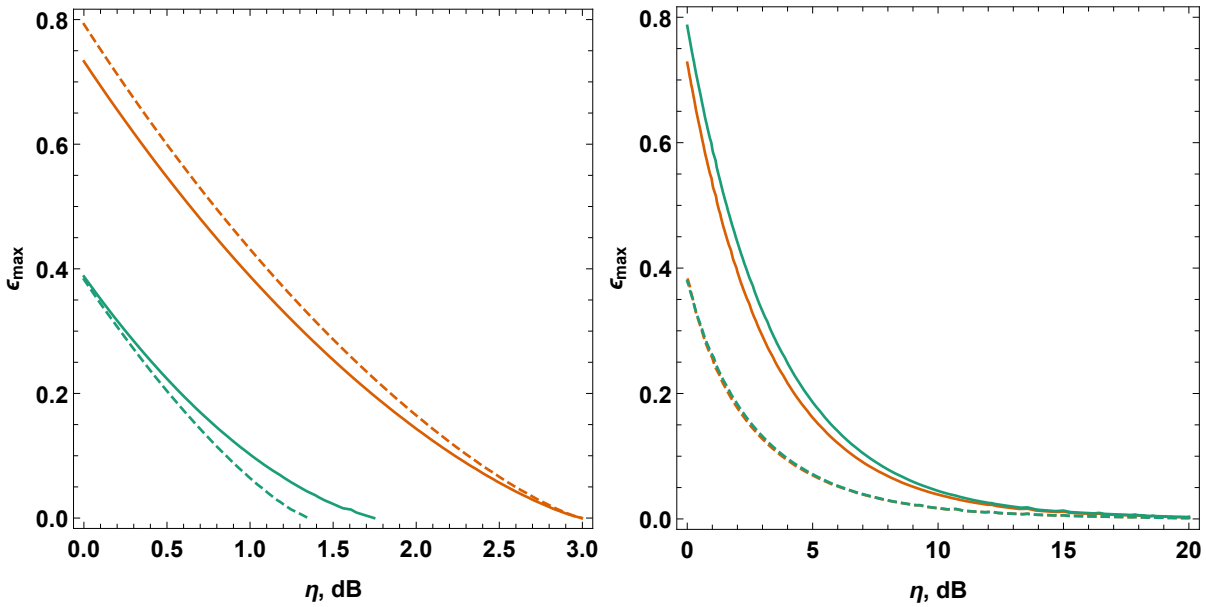


Figure 2.10: Maximal tolerable noise for CV QKD protocols with direct (left) and reverse (right) reconciliation. Protocols depicted are: the squeezed-state (solid lines), the coherent-state (dashed) protocol, with homodyne (orange lines) or heterodyne (green lines) measurement. $V = 100$ SNU.

simultaneous measurements of both quadratures to increase of the total bandwidth, and is thus an inferior version of the coherent-state protocol with heterodyne measurement. The squeezed-state protocol with heterodyne detection is a noisier version of the one with homodyne detection, since the key bit is carried only by a single (squeezed) quadrature and consequently only a single measurement result is used for key generation.

The no-switching protocol and the squeezed-state protocol with homodyne detection match in performance in an ideal channel ($\eta = 1$), but with increasing loss the key rate of the former, apparently, quickly decreases, approaches and eventually matches the rate of the coherent-state protocol with homodyne detection and the squeezed-state protocol with heterodyne detection. The squeezed-state protocol with homodyne detection in noiseless channel is unmatched in terms of key rate and noise tolerance.

Noisy untrusted channel.

The introduction of noise in the channel imposes a limit on tolerable loss, and the amount of such excess noise is detrimental to the performance of any CV QKD protocol. The protocols based on coherent states have identical excess noise tolerance, as illustrated in Fig.2.10(right), and display similar robustness to losses, as well as maximal tolerable loss (as shown in Fig.2.9d), with minor quantitative advantage of the no-switching protocol that makes use of enhanced bandwidth due to measurement of both signal state quadratures.

Employing squeezed states significantly improves tolerance to losses and can significantly improve the upper bound on maximal tolerable excess noise as shown in Fig.2.10 (right). Conducting homodyne measurement of squeezed signal states is again unmatched in terms of the amount of bits generated with each channel use, however only up to some

extent of channel loss, as seen in Fig.2.9d, where the key rapidly diminishes after 6 dB of loss. Remarkably, switching to heterodyne measurements (solid green line in Fig.2.9d) allows to extend the range of secure key generation, although it clearly yields subpar results in high transmittance links. This effect is explained by presence of trusted detection noise inevitably introduced during heterodyning [117]. Such trusted noise enhances the robustness to the excess noise, as evident from Fig. 2.10 (right), and ultimately allows to tolerate more loss. Despite the seeming advantages of the heterodyne detection, the measurement of the non-signal quadrature is redundant, while the amount of trusted detection noise that improves the lower bound on the secure key rate depends on the excess noise exhibited by the untrusted channel, and thus must be optimized. Additional details regarding trusted detection noise are given in section 3.3.5 (see also [104]).

Based on the presented analysis in further work we will focus on the squeezed-, and coherent-state protocols with homodyne detection keeping in mind that the performance of each protocols can potentially be improved upon introduction of trusted noise to appropriate trusted side.

2.3 Modified purification schemes

Conventional entanglement-based scheme is equivalent to a P&M scheme, however there is an important distinction, *i.e.* the former does not permit independent control of both displacement and squeezing because the level of squeezing V_s inherently depends on the size of the encoding alphabet V_m. A conventional EPR-based scheme is therefore sufficient for a basic analysis of idealized CV QKD protocols, however it may seize to be when complex issues (side channels, source attacks, etc.) are taken into account. In the following section we present two advanced entanglement-based schemes that allow to independently manipulate trusted resources such as squeezing and modulation, can incorporate additional effects and resources, and most importantly retain equivalent performance to a general P&M scheme.

2.3.1 Three-mode scheme

The following modified entanglement-based scheme, first introduced in [103] to access both displacement and squeezing independently (to study influence of limited reconciliation efficiency on the squeezed-state protocol), supposes that the shared trusted state is contained in three modes, as depicted in Fig.(2.11). Here Alice starts by preparing two (single-mode) states squeezed in the modes A and B, and couples them on a balanced BS. The state in the mode A further interact with the squeezed vacuum states in the mode C on a balanced BS and both output ports are measured by Alice on homodyne detectors $D1$, and $D2$ (conducting conjugate homodyning), while the states in the mode B are transmitted to and, respectively, homodyned by Bob. The state in the mode C is squeezed in the same quadrature as Alice's measurement basis, therefore states in the mode C define whether the coherent- or the squeezed-state protocol is performed and

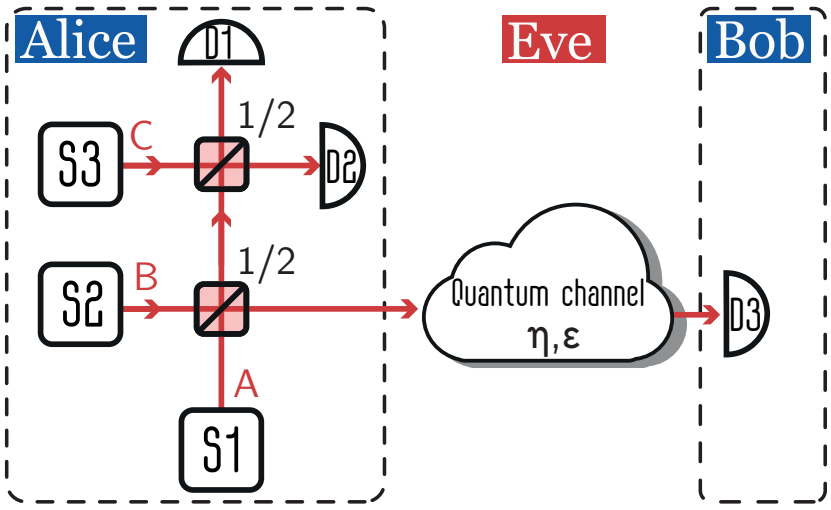


Figure 2.11: Modified (generalized) entanglement-based CV QKD scheme [103]. On trusted preparation side three single-mode squeezers are operating. The sources S_1 and S_2 generate oppositely squeezed states (in modes A and B, respectively) that are coupled on a balanced beamsplitter. Alice performs homodyne measurements on the output ports (D1 and D2) of another balanced beamsplitter on which A mode and squeezed vacuum mode C have interacted. The signal B is sent to Bob via untrusted channel. Bob conducts homodyne measurement (D3), obtaining correlated string of data with Alice, and they proceed to key sifting, error correction, and privacy amplification.

allow for a smooth transition between the two protocols. Provided the variances of the quadratures of the states in the modes A, B are

$$V_{A,B} = V_s + V_m^X \pm \sqrt{\frac{(V_s + V_m^X)(V_m^x + V_s V_m^p [V_s + V_m^x])}{1 + V_s V_m^p}}, \tag{2.40}$$

so that the signal state resulting from balanced mixing of V_A and V_B, is $V_B' = V_s + V_m^X$, where V_s is the variance of signal quadrature in P&M, and $V_m^{X(P)}$ is the modulation variance in respective quadrature in P&M. The variance of V_C is

$$V_C = \frac{V_s^2 V_m^P (V_s + V_m^x)}{V_m^x (1 + V_s V_m^p)}. \tag{2.41}$$

The system in Fig.2.11 is completely equivalent to P&M system with a single source and a modulator. The covariance matrix describing the prepared pure state before the untrusted channel has the form

$$\gamma'_{ABC} = \begin{pmatrix} \gamma'_A & \varsigma'_{AB} & \varsigma'_{AC} \\ \varsigma'_{AB} & \gamma'_B & \varsigma'_{BAC} \\ \varsigma'_{AC} & \varsigma'_{BC} & \gamma'_{AC} \end{pmatrix}, \tag{2.42}$$

where γ'_A, and γ'_C are the 2×2 matrices describing the states measured by Alice (assuming phase shift with respect to LO is absent, hence off-diagonal elements are zero)

$$\gamma'_A = \gamma'_C = \begin{pmatrix} \frac{(V_m^x+V_s)(V_m^x+V_m^p V_s[V_m^x+V_s])}{2(V_s V_m^p V_m^x+V_m^x)} & 0 \\ 0 & \frac{(V_m^p V_s+1)\left(V_m^x+V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s^2\left(V_m^x+V_s\right)} \end{pmatrix} \tag{2.43}$$

γ_B is the matrix of the state sent to Bob, that after applying Eqs. (2.40), and (2.41) becomes

$$\gamma'_B = \begin{pmatrix} V_s + V_m^x & 0 \\ 0 & 1/V_s + V_m^p \end{pmatrix} \tag{2.44}$$

and the matrices $\varsigma_{AB}, \varsigma_{BC}, \varsigma_{AC}$ describe correlations between respective modes:

$$\varsigma_{AB} = \begin{pmatrix} -\sqrt{\frac{\left(V_m^x+V_s\right)\left(V_m^x+V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s+2}} & 0 \\ 0 & \frac{\left(V_m^p V_s+1\right)\sqrt{\frac{(V_m^x+V_s)\left(V_m^x+V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s+2}}}{V_s\left(V_m^x+V_s\right)} \end{pmatrix}, \tag{2.45}$$

$$\varsigma_{BC} = \begin{pmatrix} \sqrt{\frac{\left(V_m^x+V_s\right)\left(V_m^x+V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s+2}} & 0 \\ 0 & -\frac{\left(V_m^p V_s+1\right)\sqrt{\frac{(V_m^x+V_s)\left(V_m^x+V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s+2}}}{V_s\left(V_m^x+V_s\right)} \end{pmatrix}, \tag{2.46}$$

$$\varsigma_{AC} = \begin{pmatrix} \frac{1}{4}\left(\frac{2V_m^p\left(V_m^x+V_s\right)V_s^2}{V_m^p V_s V_m^x+V_m^x} - 2V_s - 2V_m^x\right) & 0 \\ 0 & \frac{\left(V_m^p V_s+1\right)\left(V_m^x-V_m^p V_s[V_m^x+V_s]\right)}{2V_m^p V_s^2\left(V_m^x+V_s\right)} \end{pmatrix}. \tag{2.47}$$

After the preparation, trusted parties can proceed to execute further steps of the CV QKD protocol. Presuming $V = V_s + V_m$ and $V_s = 1/V$, the mutual information between trusted parties can be found using respective elements of the covariance matrix describing the state after channel interaction:

$$I_{AB} = \frac{1}{2}\log_2\left[\frac{V_A}{V_{A|B}}\right] = \frac{1}{2}\log_2\left[\frac{V_{A_1}}{V_{A_1|B}}\right] = \frac{1}{2}\log_2\left[\frac{\eta(V+\varepsilon)+h_B}{\eta(V^{h_A-1}+\varepsilon)+h_B}\right], \tag{2.48}$$

where $h_{A(B)}$ depends on the choice of measurement, on the sender side or the receiver side: $h = 0$ for homodyne, and $h = 1$ for heterodyne detection, and $\varepsilon = (1-\eta+\epsilon)/\eta$ is the overall noise added to the transmitted state, with η being channel attenuation and ϵ being excess noise. The obtained mutual information exactly corresponds to the mutual information in entanglement-based scheme of a respective Gaussian CV QKD protocol.

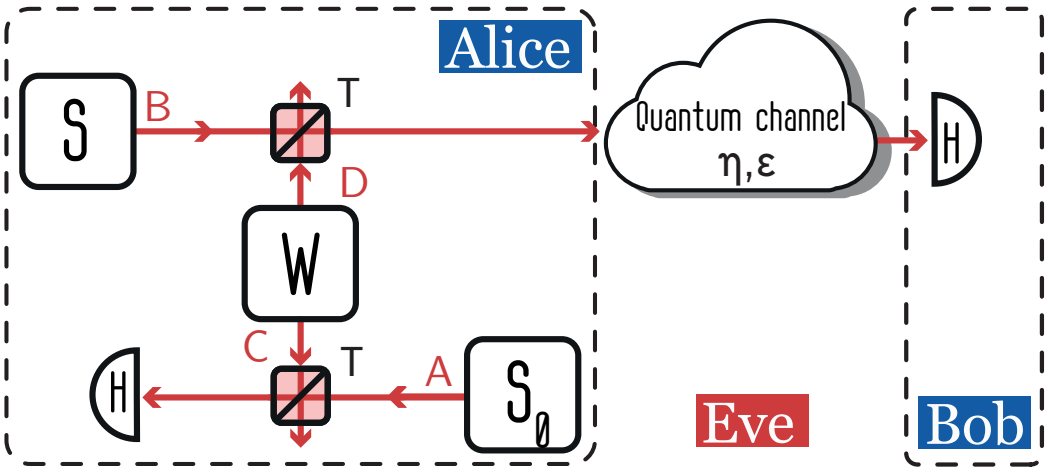


Figure 2.12: Modified scheme of a Gaussian CV QKD protocol. Source S radiates signal (mode B) that, using entangled source W (mode C, D), receives amplitude and phase modulation (via interaction on T), and is sent to Bob, that conducts homodyne detection H. Source S_0 (mode A) generates strongly squeezed states and is kept on the preparation side. Losses η and noise ϵ in untrusted channel (mode E) are attributed to Eve. Unlike previous scheme, this one supports an analysis of imperfections present at every stage of the preparation step of the protocol.

Bounds on Eve's accessible information under assumption of either individual I_E (2.33) or collective attacks χ_E (2.32), can be evaluated based on elements of full post-channel covariance matrix γ''_{ABCE}. Resulting key rate corresponds to the one obtained using conventional entanglement-based CV QKD scheme (provided aforementioned condition is respected: $V_s = 1/V$, $V_m = V - 1/V$, where V is the variance of EPR source in the latter scheme).

In summary the scheme allows to separate the squeezing of the initial signal state and the modulation, just as in P&M scheme, but maintaining the completeness of the analysis of the entanglement-based scheme. This is useful when various additional parameters of the protocol can impose limitations on state variance in the signal quadrature. Consequently this scheme allows to investigate the optimization strategies upon presence of imperfections, *e.g.* side channels, limited post-processing efficiencies, phase-dependent noise, transmittance fluctuations, etc.

2.3.2 Four-mode scheme

Another scheme, which is useful for detailed analysis of Gaussian CV QKD protocols, first introduced in [1] to analyze side channels present on preparation side prior to signal displacement (see also Ch. 3.1.5). It utilizes two single-mode squeezers and an EPR source on trusted preparation side, as depicted in Fig.(2.12). Here, Alice operates an EPR source W that radiates into modes C and D, source S that produces signal state in the mode B

with variance V_s, and the source S_0 that produces strongly squeezed state in the mode A (variance denoted by V_{S_0}). States in the modes produced by EPR source have variance $W = V_M/(1-T)$ and are respectively coupled to modes from other two sources on strongly unbalanced beamsplitters T, where $V_M > 1$ is the variance of Gaussian modulation. The signal first interacts on T with mode D, and is further sent to the untrusted channel where it suffers from losses η and noise ϵ. Mode A carrying infinitely squeezed state (to simulate the modulation on trusted side) interacts with the mode C on another strongly unbalanced beamsplitter characterized by the same value of transmittance T.

After the preparation, the overall 4-mode state on the preparation side can be described by the following covariance matrix:

$$\gamma_{ABCD} = \begin{pmatrix} \gamma_A & \varsigma_{AB} & \varsigma_{AC} & \varsigma_{AD} \\ \varsigma_{AB} & \gamma_B & \varsigma_{BC} & \varsigma_{BD} \\ \varsigma_{AC} & \varsigma_{BC} & \gamma_C & \varsigma_{CD} \\ \varsigma_{AD} & \varsigma_{BD} & \gamma_{CD} & \gamma_D \end{pmatrix}. \tag{2.49}$$

The respective submatrices are given as follows:

$$\gamma_A = \begin{pmatrix} TV_{S_0} + V_m & 0 \\ 0 & \frac{T}{V_{S_0}} + V_m \end{pmatrix} \tag{2.50}$$

$$\gamma_B = \begin{pmatrix} (TV_s + V_m - 1)\eta + 1 + \epsilon & 0 \\ 0 & \left(\frac{T}{V_s} + V_m - 1\right)\eta + 1 + \epsilon \end{pmatrix} \tag{2.51}$$

$$\gamma_C = \begin{pmatrix} V_{S_0} - TV_{S_0} + \frac{TV_m}{1-T} & 0 \\ 0 & \frac{(T-1)^2 + TV_{S_0}V_m}{V_{S_0} - TV_{S_0}} \end{pmatrix} \tag{2.52}$$

$$\gamma_D = \begin{pmatrix} V_s - TV_s + \frac{TV_m}{1-T} & 0 \\ 0 & \frac{(T-1)^2 + TV_mV_s}{V_s - TV_s} \end{pmatrix}, \tag{2.53}$$

and correlations[14] between respective states are:

$$\varsigma_{AB} = \begin{pmatrix} (1-T)\sqrt{\eta}\sqrt{\frac{V_m^2}{(1-T)^2} - 1} & 0 \\ 0 & -(1-T)\sqrt{\eta}\sqrt{\frac{V_m^2}{(1-T)^2} - 1} \end{pmatrix} \tag{2.54}$$

$$\varsigma_{AC} = \begin{pmatrix} \frac{T[V_m - (1-T)V_{S_0}]}{\sqrt{(1-T)T}} & 0 \\ 0 & \frac{T(T + V_{S_0}V_m - 1)}{V_{S_0}\sqrt{(1-T)T}} \end{pmatrix}, \tag{2.55}$$

$$\varsigma_{AD} = \begin{pmatrix} \sqrt{(1-T)T}\sqrt{\frac{V_m^2}{(1-T)^2} - 1} & 0 \\ 0 & -\sqrt{(1-T)T}\sqrt{\frac{V_m^2}{(1-T)^2} - 1} \end{pmatrix}, \tag{2.56}$$

[14] All correlations are real since the modulation variance is $V_M > 1$.

$$\varsigma_{BC} = \begin{pmatrix} \sqrt{(1-T)T\eta}\sqrt{\frac{V_m^2}{(T-1)^2}-1} & 0 \\ 0 & -\sqrt{(1-T)T\eta}\sqrt{\frac{V_m^2}{(T-1)^2}-1} \end{pmatrix}, \tag{2.57}$$

$$\varsigma_{BD} = \begin{pmatrix} \frac{T(V_m-(1-T)V_s)\sqrt{\eta}}{\sqrt{(1-T)T}} & 0 \\ 0 & \frac{T(V_mV_s+T-1)\sqrt{\eta}}{\sqrt{(1-T)T}V_s} \end{pmatrix}, \tag{2.58}$$

$$\varsigma_{CD} = \begin{pmatrix} T\sqrt{\frac{V_m^2}{(1-T)^2}-1} & 0 \\ 0 & -T\sqrt{\frac{V_m^2}{(1-T)^2}-1} \end{pmatrix}. \tag{2.59}$$

In the limit $T \to 1$ (and $V_{S_0} \to 0$) this setup corresponds to a conventional P&M scheme, where the signal state has initially variance V_s, and after amplitude and/or phase Gaussian modulation $V_s + V_m$, hence the mutual information between Alice and Bob is identical to Eq. (2.48). After evaluating the bounds on Eve's accessible information during individual I_E or collective attacks χ_E (2.35), one can also readily verify that the secure key rates (2.36, 2.37) obtained using four-mode purification scheme correspond to the rates of the conventional entanglement-based scheme (as long as $V_s = 1/V$, $V_m = V - 1/V$, where V is the variance of EPR source in the latter scheme), provided modes C and D are under full control of the trusted parties.

This modified scheme, comparing to the three-mode scheme, while being more complex, yields identical results, and provides more flexibility in analysis of possible information leakage and/or attacks on the sender side of the protocol, *e.g.* presence of side channels between generation and modulation steps of the protocol.

3 Issues of practical implementation

In practice, the security of all quantum key distribution protocols relies on numerous assumptions. Even disregarding errors due to human factor and denial of service attacks, there are numerous ways for an adversary to compromise the security of a practical QKD system. Real-world implementations are therefore exposed to risk of flaws of design and/or equipment. A thorough analysis of all aspects of protocols operation can nevertheless reveal the security threats and is required to validate the assumptions, and consequently to guarantee key security based on the laws of physics.

In the following chapter we will shortly examine each step of the protocol, starting from the preparation of quantum states, transmission though a quantum channel, detection, and lastly classical post processing. On each step we will highlight possible implementation issues and their respective impact on the security.

3.1 State preparation

In this section, the starting point of any QKD protocol, that is the generation of courier states, is discussed. CV QKD protocols operates with multiphoton Gaussian states: coherent or squeezed. The former can be reliably and efficiently generated, however some implementations may involve preparation noise. The generation process of the latter has faced a tremendous progress since the very first generation of the squeezed state [147], however still has limited range of accessible squeezing values and suffers from impurities and preparation noise. Sensitivity required by gravitational-wave detectors [148] stimulated the rapid development of squeezed light generation, with currently maximal achieved squeezing being -15 dB [149], and, separately the purest strongly squeezed states exhibit 89% purity (with -10 dB and +11 dB of squeezing and anti-squeezing respectively) [149].

The quality (preparation noise and squeezing level) of the carrier state can have various ramifications for the security of CV QKD protocols depending on reconciliation, untrusted channel properties, type of attack, and even encoding alphabet size [15]. For optimization, and realistic predictions of CV QKD protocols performance it is vital to recognize feasible squeezing rates, thus notable experimental generations of squeezed-states are listed, as well. Further we describe the modulation stage and discuss the related loopholes, such as encoding of information onto additional degrees of freedom or modulation in excessive

[15] Assuming the aim is to recreate the entanglement-based scheme where squeezing is interlinked with displacement variance, as described in Ch.2.1.2.

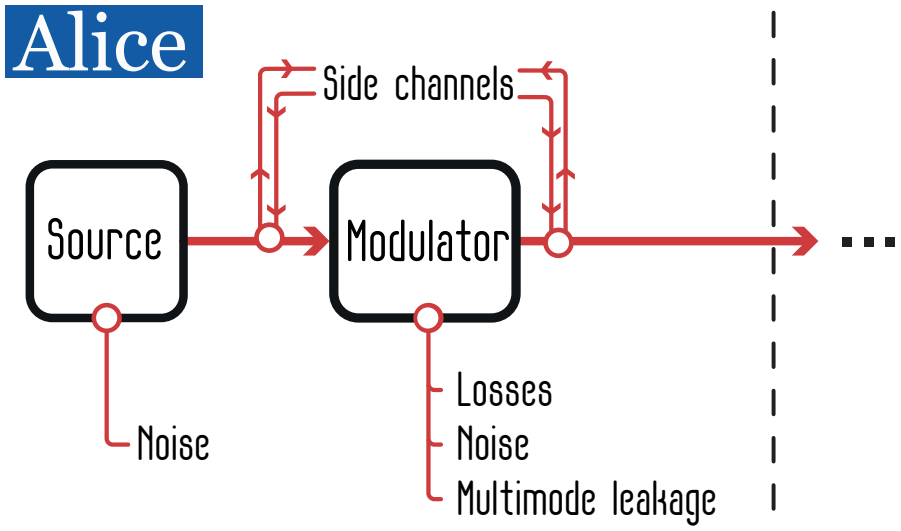


Figure 3.1: Preparation side of the CV QKD P&M protocol. The loopholes that can provide additional additional information to an attacker can be present on each stage of the quantum state preparation. At the very start the *source* may generate initially noisy quantum states, while during the *modulation* step additional noise may also be present, or the modulation can be partially or fully applied to excessive modes, causing an information leakage and potentially leading to zero-error security break. Additionally side channels may be present before and/or after the modulation step of the state preparation, leaking the information about prepared state or the encoded key to an eavesdropper (indicated by arrows pointing *from* the signal arrow), or add more noise to the signal(indicated by arrows pointing *to* the signal arrow).

modes. Origins of main issues during preparation step are illustrated in Fig.3.2.

3.1.1 Source

Here we focus on the generation of quantum states required for execution of the CV QKD protocols. Both coherent and squeezed (single- and two-mode) states are essential tools and are extensively used in any Gaussian CV QKD protocol, mostly as courier states (2.5), for constructing TMSV states, but are also involved in various optimization and modulation techniques.

Lasers

The generation of shot-noise limited coherent states is considered to be a benchmark in the industry. However some implementations, such as QKD system integrated into a chip, may relax requirements on the noise of the initial state, due to *e.g.* manufacturing cost limitations.

An example of noise occurring in radiated coherent states is the relative intensity noise (RIN). This noise is caused by the laser power fluctuations, which depend on the properties of the laser, back reflection, cavity vibrations, fluctuations of laser gain medium, etc. Dominant contribution is the interference between the signal mode and spontaneous

light emission [150]. By definition RIN is the ratio of the variance to the average laser intensity [151]. One of the approaches to measuring RIN is to time sample the output current of a photo-detector and transform this data set into frequency with a fast Fourier transform [152]. Such noise is typically independent of laser power and can affect the performance of CV QKD scheme. More specifically, in terms of quadrature of the Gaussian states it contributes to the noise (within bandwidth of $1\,Hz$) as [153]:

$$\epsilon_{RIN} = 2\langle n\rangle\sqrt{RIN}, \tag{3.1}$$

where the mean number of photons $\langle n\rangle = V_M/2$ is determined by the variance of the signal modulation V_M. However, typically such noise is small (*e.g.* $RIN = 8\times10^{-11}\,\mathrm{Hz}^{-1}$ [153]), and therefore does not significantly influence the security of CV QKD protocols.

Nevertheless, instead of considering individual contributions to noise, for the purpose of security analysis it is sufficient to generalize and estimate constrains on the overall *preparation noise* ε_{prep} characteristic to the source (see further details in Sec. 3.1.4). This may, however, lead to more constrained security bound estimates. The security of coherent-state CV QKD protocols in presence of trusted noise was considered in [102, 117, 154], and the noise has been shown to be having different effect depending on the choice of reconciliation, and in some scenarios even helpful up to some extent. Noisy coherent (thermal) states are also relevant in the microwave regime where generation of pure signal states at room temperature is unattainable, due to non negligible background noise that is inevitably present at longer wavelengths [105, 155].

Squeezers

Physically the generation of the squeezed states relies on pumping of medium possessing nonlinearity of second (or third) order. The very first squeezed states were generated using a medium with third order nonlinearity via four-wave mixing process [147]. Since then experimental endeavors kept a remarkable pace of developing new techniques for the squeezed-state generation, and improving the existing ones. Currently, the most prominent technique is the optical parametric oscillator (OPO), while other notable ones include optical parametric amplifier (OPA) and spontaneous parametric down-conversion [156].

The main method used for state generation in CV QKD is parametric down convertion [157]. The process employs a strong pump beam to create a non-linear polarization via the second-order polarizability and induce an amplification in the medium at a signal, as well as at idler wavelengths [158]. Conservation of energy requires the sum of frequencies of the signal and idler to be equal to the pump. Furthermore, conservation of momentum (also referred to as phase mismatch) is needed to ensure significant energy transfer (for detailed theoretical description of parametric down convertion see [156, 159]).

The squeezing that can be achieved after single pass of the pump laser beam through nonlinear crystal is small, mainly due to low effective nonlinear susceptibility $\chi^{(2)}$. One solution (OPA) is to use ultrashort laser pulses with high power to increase the pump

amplitude. The very first OPA system had generated squeezed states with - 0.6 dB below shot-noise limit [160]. Later the result was surpassed, with - 2 dB [161] and - 5.8 dB [162] squeezed states. The latter result still holds the record as the highest one among single-pass pulsed OPA systems.

Another solution is to place the nonlinear crystal inside a cavity, and proves to be more efficient. The cavity can be tuned to resonate the pump and/or signal beam, which allows to enhance the pump power, and/or increase the interaction time (effectively improving the nonlinearity of the medium), respectively. The very first experimental implementation of an OPO had generated single mode squeezed vacuum state with - 3.5 dB of squeezing [163]. Squeezing level was later improved to - 3.8 dB [164], and up to -7 dB [165, 166]. Gradually achievable squeezing levels were increasing, up to -12.7 dB (and +19.9 dB in conjugated quadrature) [167], with the most recent record being -15 dB (and +21dB in conjugated quadrature) [149], both in a continuous-wave source.

An ideal parametric down convertion system can in theory generate infinitely squeezed states, however real systems are always limited by phase noise, and losses that occur at the mirrors and various optical elements inside the cavity. Phase noise can be reduced by means of pump beam filtering [168] and improvement of feedback systems [169]. Intracavity losses are suppressed by using antireflecting-coated crystal, and low-loss coatings on mirrors [167]. Aside from squeezing an important figure of merit is the noise in an anti-squeezed quadrature, which can also influence the performance of the protocol (see Ch. 3.1.4). A complete characterization of the state is required for correct estimation of channel parameters. Furthermore thorough source description, and correct attribution of losses and noise, allows to avoid underestimation of information accessible to the eavesdropper. For rigorous description of generation of squeezed states see [170–172] or recent reviews [173, 174].

3.1.2 Modulation

The goal of the modulation step is to encode key bits onto the carrier states. During this step of the protocol, in P&M scenario, Alice draws random normal variables from independent (close approximation) Gaussian distributions $\mathcal{N}(0, V_m^x)$ and $\mathcal{N}(0, V_m^p)$ for respective quadrature, and displaces a signal state in one or two quadratures (depending on the protocol) the quantum state according to the drawn variables. In EPR-based scenario instead of direct encoding Alice performs homodyne or heterodyne measurement (depending on the protocol) on one of the modes of two-mode squeezed state, therefore conditionally preparing the signal states.

Direct preparation of the state can be performed using acousto- and electro-optical modulators (AOM and EOM, respectively) [175]. The former allows to modify the refractive index of the medium by creating a mechanical strain caused by acoustic wave, the effect referred to as photoelasticity. EOM, on the other hand, utilizes the linear dependency of refractive index on applied electric field in nonlinear mediums, also known as Pockels effect. The effect allows to vary the voltage across the medium and modify the phase of the transmitted light. The strength of the effect can be different for or-

thogonal polarization components, thus upon proper alignment of the birefringent crystal and polarizers, polarization, amplitude and phase of the output light can be modified. Phase modulators are also used in the arms of (conventional or nested) Mach-Zehnder interferometer which can give the trusted preparation party control over both amplitude and phase of the state at the output.

Due to discreteness of voltage used for modulation of the signal, as well as finite range of accessible intensities, quadrature distributions in realistic implementation will deviate from ideal Gaussian distribution from which random variable was drawn. However, provided discretization step is small enough comparing to the shot noise value, trace distance between intended state and the actual modulated state will be negligible [122] [16]. In practice, the security is assessed on the gaussified data, and such assumption is valid since the key rate is minimized for the Gaussian states with given statistical moments (covariance matrix) [81]. Nonetheless, there are other numerous implementation issues connected with the modulation stage of the protocol. First of all, the signal is subjected to losses due to reflection, absorption and scattering within the crystal. Secondly, parameters of the medium are sensitive to the temperature, and to avoid phase noise one may need to account for heating, caused by the energy of the driving field, by re-aligning the crystal. Driving field voltage fluctuations are also an issue since they directly translate into modulation noise [153]. Phase mismatch, and ripples in modulation can as well deteriorate the expected performance of the modulator and have to be characterized by Alice. Feedback systems can be used to control the modulation process and to maintain proper hardware performance [61].

Realistic modulation can also be subjected to phase noise, which can lead to an increase of the overall variance of the signal state. This noise represents the finite certainty of Alice of the output state and it can be modeled as noisy (homodyne for squeezed-state protocol, and heterodyne for coherent-state protocol) detection on Alice's side in EPR-based representation of a CV QKD protocol. Such phase noise decreases the correlations between trusted parties and therefore can deteriorate the mutual information between them. Furthermore, such noise in classical data can lead to an incorrect channel estimation [122]. In a more conservative scenario even small values of phase noise is attributed to the eavesdropper (along with other imperfections) can significantly reduce achievable secure distance [122, 177].

3.1.3 Multimode structure

The QKD security analysis is usually performed presuming single-mode approximation, however both sources and modulators have in general multimode structure. Non-signal modes (be it in spectral, or spatial domain, or in any other degree of freedom) can carry the information regarding the signal, it's modulation basis, etc. , hence can be exploited by an eavesdropper. In DV QKD protocols, for example, the multimode generation can affect the distinguishability of signal and decoy states [178] and thus has to be properly accounted for.

[16] Howbeit, incorporation of this effect remains an open problem for composable security proof [122,176].

With the advent of multimode quantum sources [179–181] eligible for use in CV QKD protocols, and possible leakage of encoded information into non-signal modes during modulation stage (of single-mode CV QKD), it is especially necessary to analyze repercussions of multi mode presence. Provided trusted parties are fully aware of the mode structure of the source and perform measurement of each mode, cross-talk between modes still causes deterioration of the entanglement of states in trusted modes and requires optimization of the signal [123]. However if additional modes carry even partial information about the transmitted key, and are directly accessible to Eve, this may result in zero-error security break. Generally such leakage not only increases the sensitivity to losses and excess noise in quantum channel, but also limits the range of applicable values of state modulation V_M and initial signal state variance V_S. Rigorous analysis of preparation equipment and subsequent optimization of encoding alphabet and squeezing are required to maintain positive key rate [2]. More detailed summary of security analysis of the CV squeezed-state and coherent-state QKD protocols with multimode information leakage can be found in Ch. 5, originally published in [2] (see also Ch. 8). This modulation noise is the main reason to consider trusted preparation noise in the protocols, especially, if the modulation has a large variance.

Information leakage due to multimode modulation can also be seen as a Trojan horse attack, where Eve can actively send a quantum state into the preparation side and extract additional information about the transmitted key (for the analysis of the attack on the coherent-state protocol see [182]). In this scenario Eve is assumed to be fully controlling the infused state and by sending the squeezed state Eve can improve the precision of the readout of the encoded information. The attack does not influence the signal state and consequently is undetectable unless Alice monitors all modes that are entering and exiting the trusted preparation side.

3.1.4 Preparation noise

Generalizing and joining together all possible sources of imperfections on the trusted preparation side allows one to simplify the security analysis. The noise occurring on Alice's side can be treated as either mere consequence of trusted equipment imperfections, or attributed directly as the influence of an adversary, thereby imposing stricter limitations on security conditions. The latter corresponds to adoption of an exceedingly conservative approach attributing all noise as the deliberate intrusion, however this can be very limiting for a protocol implementation as well as underestimate the security of the protocol. It is therefore more practical to estimate precisely which parts can be trusted than to be very conservative and pessimistic.

The P&M and entanglement-based models are shown in Fig. 3.2. The source $EPR : V_A$ allows to purify the preparation noise, and depending on assignment of the modes analyze trusted or untrusted preparation noise. Furthermore the noise can be split into two more categories: phase-sensitive, and phase-insensitive. The former incorporates the noise that is relevant only for a single quadrature, while the latter is symmetrical on phase-space and contributes to both quadratures equally.

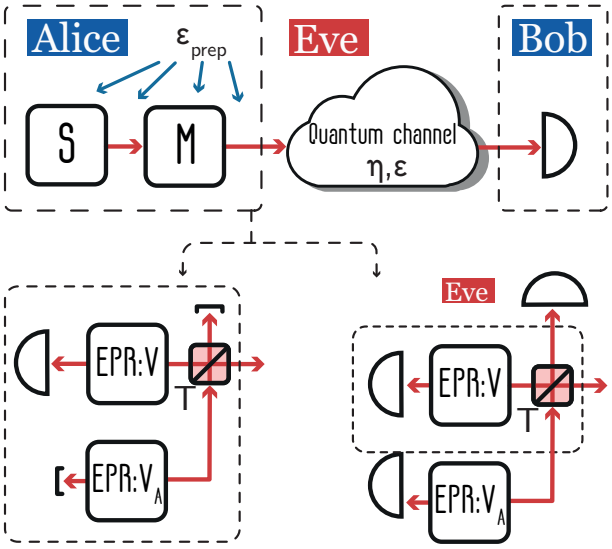


Figure 3.2: Preparation noise (which can be present on all the stages of modulated state preparation) in case of P&M (top) and equivalent EPR-based (bottom) schemes. With $V_A = \epsilon_{prep}/(1-T)$, and coupling of the respective mode with the signal mode on the unbalanced BS: $T \to 1$, the equivalence of EPR-based scheme and the P&M scheme can be established. The preparation noise is trusted (I) if it is purified by Alice, *i.e.* she controls both modes of EPR: V_A source (bottom left), or is untrusted (II) if Eve holds the purification (bottom right).

Phase-insensitive noise

The preparation noise ϵ_{prep} does not affect the data that Alice encodes, nor the correlations between Alice and Bob, but rather the state sent to Bob, which is now described, in the context of a P&M scheme shown in Fig.3.2 (top), by the following covariance matrix:

$$\gamma_B = \begin{pmatrix} V_S + V_M + \epsilon_{prep} & 0 \\ 0 & \frac{1}{V_S} + V_M + \epsilon_{prep} \end{pmatrix}. \tag{3.2}$$

Employing the purification-based scheme, as in Fig.3.2 (bottom) yields the following description of the preparation noise source:

$$\gamma_{CD} = \begin{pmatrix} V_A \mathbb{1} & \sqrt{V_A^2 - 1}\sigma_z \\ \sqrt{V_A^2 - 1}\sigma_z & [V_A + (1-T)V]\mathbb{1} \end{pmatrix}, \tag{3.3}$$

so that overall trusted state is now described by a 4-mode covariance matrix γ_{ABCD}. Adjusting the variance of V_A source achieves the equivalence with P& M scheme

$$V_A = \frac{\epsilon_{prep}}{1-T}. \tag{3.4}$$

After taking into account the main channel effect, γ_{ABCD} can be further used to calculate both the mutual information I_{AB} (2.48) and the Holevo bound (2.35) and estimate the secure rate of the CV QKD protocol in presence of the preparation noise. If the preparation

noise is considered trusted, then the theoretical purification of the noise is given to the trusted parties, or even to a untrusted third party - Eve [183, 184] (which anyway leads to the same results). If both modes of the entangled source $EPR : V_A$ are controlled by the eavesdropper (as in Fig.3.2 bottom, right), such noise is equivalent to the additional untrusted channel noise (scaled by losses).

In the limit of infinite encoding alphabet $V_M \gg 1$, and perfect post-processing efficiency $\beta = 1$, and purely lossy channel $\varepsilon = 0$ secure key rate of CV QKD protocol with RR under collective attacks converges to [104]:

$$R_{RR}|_{V_M \gg 1} = \frac{1}{2}\left\{\log_2\left[\frac{1}{1-\eta}\right] - \log_2\left[\eta(V_S + \epsilon_{prep}) + 1 - \eta\right]\right\}. \tag{3.5}$$

Evidently the security of the RR CV QKD protocol is lost if $1/(1-\eta) = \eta(V_S+\epsilon_{prep})+1-\eta$, and this leads to the following constrain on the phase-insensitive trusted preparation noise:

$$\epsilon_{prep} < \frac{2-\eta}{1-\eta} - V_S. \tag{3.6}$$

At long distances (or in the channel with strong losses), where $\eta \to 0$, Eq.(3.6) shows the upper bound on the tolerable preparation noise for the coherent-state protocol to be $\epsilon^{coh}_{prep} = 1$, while protocol based on infinitely squeezed states can tolerate up to $\epsilon^{sq}_{prep} = 2$. Note that the key rate in Eq. 3.5 can be further optimized by increasing the squeezing [103]. The evaluation of respective security bound can be performed using three-mode purification scheme, as described in Ch.2.3.1.

Surely the tolerance towards preparation noise is increased when operated in channels with higher transmittance, however presence of excess noise ϵ and realistic processing efficiency $\beta < 1$ significantly decreases the tolerance.

Aside from equipment characterization and control [185], a viable strategy to partially negate (or in case of boundless modulation, completely eliminate) the effect of such noise is to perform noise filtering. The latter can be done by introducing attenuation of the signal prior to the quantum channel [102, 117].

Contrary to the case of RR protocol, where preparation noise contributes to the information gain of an eavesdropper, in case of DR CV QKD protocol [105,155], the preparation noise can lead to the decrease of the Holevo bound. Provided the excess noise and channel attenuation level are low, the preparation noise has harmful influence on the secure key rate, however as the excess noise is increased, the preparation noise allows to "fight the noise with noise", *i.e.* improve the key rate of the protocol established over noisy channel by introducing additional noise. The preparation noise does indeed effectively increase the key rate, though only provided the excess noise is close to the maximally tolerable. If environment is also noisy and attenuation is low, such noise can even lead to positive secure key rate recovery. Furthermore, the preparation noise can improve the robustness to detection noise [104]. To maximize the benefit one should optimize infused preparation noise.

The difference in the influence of the preparation noise on RR and DR protocols can be

intuitively understood since addition of (unknown, but trusted) noise to the reference side can be more harmful for Eve than for the trusted parties. Mutual information between trusted parties is reduced, while simultaneously the Holevo bound is increased in case of RR protocol, and respectively decreased in case of DR protocol. This holds true in the channels with transmittance fluctuations (Ch.2.1.3) as well.

Phase-sensitive noise

The state described by Eq.(3.3) is symmetrical in a sense of equal variance in both quadratures, which means both quadratures of the signal state are facing the same preparation noise. This is a valid assumption for modelling, but may not hold true in general especially if phase noise is present in the system. The squeezed state are well known to be generated as mixed states, and while for majority of applications only the quadrature with sub-shot-noise level is relevant, it is important to question the effect of increased variance in conjugated quadrature on the security of the protocol. Furthermore, the modulation can impose different levels of preparation noise on both quadratures, which makes phase sensitive noise relevant in the coherent-state protocol as well.

To model such noise one can substitute an EPR source (3.3) with two single-mode squeezed states mixed on a balanced BS. Altering the squeezing in each initial mode allows to shape the state γ_{CD} that with proper adjustment allows to control the amount of preparation noise in each quadrature, resulting in the state received by Bob to be:

$$\gamma_B = \begin{pmatrix} V + \epsilon^x_{prep} - 1 & 0 \\ 0 & V + \epsilon^p_{prep} - 1 \end{pmatrix}, \tag{3.7}$$

The noise in non-signal quadrature surely does not affect the mutual information between trusted parties I_{AB}, however it can, actually, increase or decrease the Holevo bound χ_E regardless of the protocol employed.

As one would expect, if such noise is regarded as untrusted then it, similarly to phase-insensitive noise, can be treated as excess noise at the input of an untrusted channel, and it effectively increases the information accessible to an eavesdropper. On the other hand, provided the noise is trusted, it can improve the performance of majority of CV QKD protocols.

The squeezed-state protocol (which is modulated in a signal quadrature only) can always benefit from presence of preparation noise in non-signal quadrature regardless of the reconciliation choice. While such noise does not alter the robustness to channel noise, it can improve the key rate leading to minor improvement of the secure distance (at the order of hundreds of meters in standard telecom fiber upon RR). Preparation noise, if present only in the signal quadrature, is helpful once DR is performed, and decreases the key rate for RR, similarly to the aforementioned phase-insensitive trusted noise.

For the coherent-state protocol the effect of preparation noise foremost depends on the measurement on the receiver. For homodyne-based protocol the noise has a two-sided effect. In non-signal quadrature of the carrier state it is helpful, however the choice of more

noisy quadrature is less beneficial for trusted parties. For heterodyne-based protocol such asymmetrical noise will always impact the security. During DR, the noise can improve the performance of the protocol, although requires optimization over the parameters of the channel. In the RR scenario any amount of noise regardless of the quadrature will deteriorate the performance of the protocol.

3.1.5 Side channels

Generally a side channel in QKD can be defined as an auxiliary adversary channel with either input or output controlled by a trusted party but, respectively, output or input by an eavesdropper (see Fig. 3.3). Such definition allows to distinguish side channels (and their influence) from the main untrusted channel, where quantum ancillas are prepared by Eve, and simultaneously, after the interaction with the signal they are stored in her quantum memory, *i.e.* Eve controls both input and output of her channel mode. The side channels are the generalization of the various effects that can occur in classical or quantum domain providing an eavesdropper with additional information advantage by means of either disruption of the trusted party or benefiting from information leakage. In other words, we model side channels as Eve attacking the optical mode, yet her additional information advantage can emerge from non-optical parts of the experiment (*e.g.* electric current). From Eve's point of view side channels give way for either noninvasive (passive) attacks, where Eve can only receive the information *i.e.* control only the output of the side channel, or Eve can resort to interfering with the operation of trusted equipment (active attack), *i.e.* control the input of the side channel. If more side channels are present Eve can control input/output of them separately. We refer to the side channels on the preparation side as to **type-A** side channels. On Alice's side there can be two points of side-channel intrusion: pre-, and post-modulation.

Pre-modulation channel

The main consequence of the pre-modulation side channel presence is the corruption of the initial cryptographic resource - signal state. Such side channel can be modeled as an interaction of the signal with mode E_1 on BS η_{E_1}, as in Fig.3.3 (left). The variance of the state received by Bob will change to $V_B = [\eta_{E_1}(V_S - 1) + V_M]\eta + 1 + \epsilon$. The coherent-state protocol is unaffected by such leakage, while the squeezed-state protocol effectively looses squeezing $V_s \to 1$, and also its purity, as the coupling of the side channel to signal increases $\eta_{E_1} \to 1$, and the state eventually is reduced to the coherent state. Nevertheless, the performance of the squeezed-state protocol remains superior to the coherent-state protocol.

In a scenario when Eve tries to infuse the noise onto the preparation side using pre-modulation side channel (with state variance at the input V_{E_1}) both the coherent- and squeezed-state protocol will face the repercussions, as the signal carrier state becomes more noisy $V_B = [\eta_{E_1}V_S + (1-\eta_{E_1})V_{E_1} + V_M - 1]\eta + 1 + \epsilon$. The presence of pre-modulation type-A side channel can be viewed as preparation noise 3.1.4, however an important

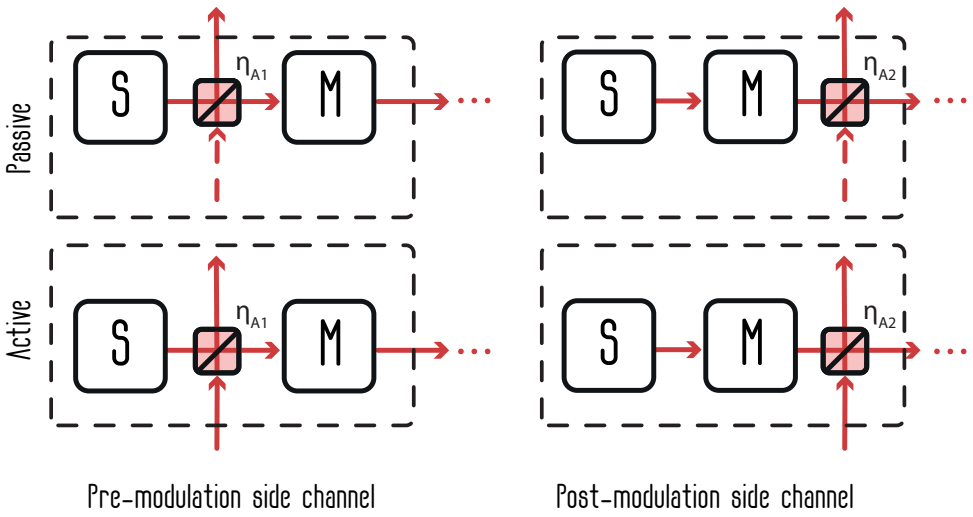


Figure 3.3: Models of side channels on preparation side (type-A) of the P&M CV QKD protocol. Eve can employ a side channel in either a passive manner (top row), which allows her to gain benefit from the information leakage, or actively (bottom row), where Eve sends a state into the trusted preparation station. Additionally, the side channel can be present directly after the source - pre-modulation (left column), or already after the modulation - post-modulation (right column).

distinction is that the side channel is also correlated to the signal. The latter implies an increase in the entropy of Eve's state and consequently of the Holevo bound.

Overall pre-modulation side channel does decrease the key rate (secure distance) and robustness to the excess noise in untrusted channel ϵ for the squeezed-state protocol. Yet it does not lead to a security break (assuming trusted parties confirm the variance of the signal is within the reasonable range *i.e.* no additional noise is infused), as one would expect, since no actual information has been encoded into the states yet. The worst case scenario for trusted parties is substitution of the initial carrier state by the coherent state ($V_S = 1$), hence the performance of the squeezed-state protocol is reduced to one of the coherent-state protocol with homodyne detection.

Post-modulation channel

The side channel, present after the modulation, has completely different effect on the security of a CV QKD protocol than the channel before the modulation, as Eve can already obtain additional information regarding the encoded key. While active use of such side channel (Fig.3.3 bottom right) is equivalent to the additional noise in the untrusted channel [186], leakage from a passive side channel ((Fig.3.3 top right)) can increase the overall noise imposed on the signal and provide the adversary with additional insights regarding prepared state. Both interactions limit the robustness against losses and noise, hence limiting the security of the protocol.

Assuming the equipment cannot be shielded from post-modulation side channel, and information leakage cannot be entirely eliminated, Alice can infuse the input of the side

channel with properly engineered state to partially or even completely negate the effect of its presence. To achieve the latter, correlated (to the signal) modulation of a single-mode squeezed state is required. By optimizing the modulation, side channel can be fully decoupled from the signal and any negative repercussions completely eliminated. Therefore, as long as Alice is aware of the type-A side channel and can properly characterize it, she can completely counteract its influence.

We address side channels on receiver side (type-B) in Sec.4.2.2, and outline the modeling and the effects of all side channels, along with compensation methods in Ch. 4.

3.2 Untrusted channel

In the following section we discuss challenges related to transmission of the signal (and phase reference beam unless the "local" local oscillator scheme is implemented) through an untrusted quantum channel.

A common issue of coherent detection schemes, which is highly relevant for CV QKD as well, is phase noise [187]. While the phase difference between the quantum signal and LO initially depends only on the encoded information, the difference value will inevitably drift during data accumulation process [62, 188]. To compensate the drift, the trusted parties need to estimate its value based on a number of reference signals. However, due to limited precision of the estimation and subsequent compensation, the residual phase noise will accumulate in the system and will contribute to the excess noise [65]. Phase noise was shown to be limiting maximal secure distance [177], and for highly lossy channels (*i.e.* for long distances) the requirements on precision of compensation are stronger, calling for high-precision compensation schemes [44, 65].

Another major challenge of long-distance CV QKD is the need to maintain strong LO after the channel with high amount of loss, given that increase of LO powers leads to an increase of LO leakage into the weak quantum signal, and consequently to increase of the excess noise [188]. The leakage can be suppressed by filtering using combination of polarization and frequency multiplexing [62], by employing highly sensitive homodyne detector with lower requirement of LO power [44], or by avoiding sending LO altogether, and generating LO at the receiver station [114, 189, 190].

3.2.1 Fiber channel

Aside from equipment, a significant share of the cost of establishing a QKD-secured communication is allotted to an untrusted channel. Foremost approach is to deploy a dedicated optical fiber link. Deploying a standard telecom fiber one can expect an average attenuation of 0.2 dB/km at 1550 nm (2.22). However, one can also employ ultra low loss Pure Silica Core fibers [191] which exhibit - 0.15 dB/km. Deployment of the link allows to ensure the minimization of excess noise in given environmental conditions. Nevertheless, such approach is expensive and time consuming.

An alternative is to use an already deployed (commercial) communication network. There are two options available to users: to rent a dark fiber (an unused fiber link), or to co-propagate the QKD signal with classical signals. Regardless of the chosen option, there's a number of concerns that has to be addressed. Firstly, software and hardware have to be adjusted in order to operate within existing standards of telecomm equipment [192]. Secondly, expected transmittance in deployed commercial dark fibers is lower (than of the optical fibers in the laboratories) due to inter-fiber coupling, splices, or sharp bends [193]. Furthermore, environmental perturbations can also contribute to loss and noise, as well as induce fluctuations of fiber optical length [46]. Recently a continuous operation of the coherent-state CV QKD protocol has been successfully established over two commercial dark fiber links of 30 and 45 km (both $\approx 12\,dB$) in metropolitan areas for a duration of 24

hours each, and achieved 5.91 and 5.77 kbps of secure key rate, respectively, in finite-size regime [193].

Co-propagation of a quantum signal and classical data transmission in the same fiber can be achieved using wavelength-division multiplexing (WDM) [192, 194]. Such architecture involves several sources of noise affecting the quantum channel: photon leakage from classical channels, four-wave mixing, spontaneous Raman scattering (SRS), and amplified spontaneous emission (ASE) caused by classical optical fiber amplifiers [195]. The photon leakage originates from limited isolation during demultiplexing, and it contributes to non-signal modes in the quantum channel, and thus can be filtered by LO [195]. Although, if trusted parties conduct spatial mutiplexing of quantum signals and WDM classical signals, a cross-talk at the same wavelengths can inhibit secure key generation, which, however, can be circumvented by proper wavelength spacing between quantum and classical carriers [124]. Noise contribution due to four-wave mixing was shown to be relevant at short distances and at relatively high powers of the classical channel ($>10mW$), however at practical fiber lengths ($>1\ km$) such noise diminishes [196]. Furthermore, polarization multiplexing and increasing wavelength spacing can aid in further noise suppression [197].

Both SRS and ASE can directly contribute to the signal mode and act like thermal excess noise [195]. Yet, the noise caused by SRS was proven to be negligible even in presence of 100 co-propagating classical channels [198]. On the other hand, ASE limits the performance of CV QKD protocol, and can even lead to a security break [198]. Proper band filtering of the noise prior to multiplexing of quantum and classical channels allows to minimize the influence of ASE and restore secure QKD within the shared optical fiber network. [198].

3.2.2 Atmospheric channel

Unlike fiber, free-space links may avoid the necessity of using existing infrastructure, as they require only a line of sight between two trusted stations, and thus are portable, and can be quickly established in metropolitan area or difficult terrain. Such flexibility opens the way for mobile QKD networks that can especially be useful in airport traffic control, ship-to-ship communication, or between autonomous vehicles. Most importantly, free-space links can exhibit considerably lower amount of losses over the long links, since attenuation on higher altitudes can be substantially lower (*e.g.* at 2.4 km above sea level it can reduce to 0.07 dB/km [199], while outside Earth's atmosphere can become completely negligible) than in standard fiber channels. However, modeling the beam propagation through the atmosphere is more involved, as it depends on weather conditions, altitude, location, and length of the link. The modeling is especially important for CV QKD protocols, where both losses and noise must be carefully estimated.

Characterizing free-space QKD channel is a nontrivial task as an atmospheric turbulence causes beam wandering [200], beam distortion [201], and scintillation [202], all of which lead to spatial and temporal variations of the transmittance in the channel. Luckily, for the evaluation of security, rather than exhaustively describing the transmittance probability distribution $\tau(\eta)$, it is sufficient to properly estimate only the mean

value of transmittance $\langle\eta\rangle$, and mean value of square root of transmittance $\langle\sqrt{\eta}\rangle$ [126] (see Sec. 2.1.3). Nevertheless, it is crucial to predict the expected transmittance based on the weather conditions and location of the link. We summarize three often used models for turbulent channel characterization: log-normal, beam-wondering and elliptical [6, 203, 204]. The choice of the model foremost depends on the nature of channel, and may require adjustment for specific weather conditions. Furthermore, some channels may involve additional considerations, *e.g.* gravity effects for satellite-based channels [205], or sea surface deflection and refraction for composite satellite-to-submarine channel [206].

Log-Normal distribution

There are many approaches for description of free-space channels (*e.g.* negative-exponential [207], or gamma-gamma distributions [208]), and the log-normal distribution [209]. The latter is often used to characterize beam propagation through long, horizontal atmospheric channels [203]. Validity of the distribution fit was experimentally verified on weak coherent states propagation in free-space 143 *km* long optical link between Canary islands [199, 210, 211]. The log-normal probability distribution of transmittance in an atmospheric channel can be written as [202, 212]:

$$\mathcal{P}_{LN}(\eta) = \frac{1}{\eta\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(\ln\left[\langle\eta\rangle^2/\sqrt{\langle\eta^2\rangle}\right] - \ln\eta)^2}{2\sigma^2}\right], \tag{3.8}$$

where

$$\sigma^2 = \ln\left[\frac{\langle\eta^2\rangle}{\langle\eta\rangle^2}\right]. \tag{3.9}$$

Both Eqs. (3.8,3.9) depend on first and second moments of transmittance η, which are given by:

$$\langle\eta\rangle = \int_{\mathcal{A}} d^2\mathbf{r}\,\Gamma_2(\mathbf{r}), \tag{3.10}$$

$$\langle\eta^2\rangle = \int_{\mathcal{A}} d^2\mathbf{r_1} d^2\mathbf{r_2}\,\Gamma_4(\mathbf{r1}, \mathbf{r2}), \tag{3.11}$$

where integration is carried out in the aperture area $\mathcal{A}$, $\mathbf{r} = (x\,y)^T$ (while z coordinate is given by the distance between input and output apertures) and Γ_2 and Γ_4 are the field correlation functions. Functions Γ_2 and Γ_4 can be numerically evaluated using a set of following parameters: wave number k, beam-spot radius W_0, propagation distance L, wavefront radius at the aperture, and structure constant of the refractive index of the air C_n^2.

As mentioned previously, in order to reconstruct the covariance matrix (2.24) knowledge of $\langle\eta\rangle$ and $\langle\sqrt{\eta}\rangle$ is required. The former can be obtained directly from Eq.(3.10),

while the latter using $\mathcal{P}_{LN}(\eta)$ (3.8)

$$\langle\sqrt{\eta}\rangle = \int_0^1 d\eta\sqrt{\eta}\mathcal{P}_{LN}(\eta). \tag{3.12}$$

Despite its popularity, the log-normal distribution may predict transmittance in weakly turbulent channels with non-negligible discrepancy from the experimental data [6]. Furthermore, $\mathcal{P}_{LN}(\eta)$ has low-probability "tails", which do not confine $\eta \in [0,1]$ within physical values, hence some of the channel properties can be incorrectly estimated even in conditions of strong turbulence [6]. Overestimation of transmittance values is the main reason why log-normal has not been used in the works described in Chapters 6 and 7.

Beam-wandering model

One of the major contributions to signal losses in free-space channel is beam wandering, which is induced by turbulence and/or source adjustment instability [200]. Beam wandering is characteristic for short links with weak absorption. In such channels, signal loss occurs mainly as a consequence of beam-spot truncation at the receiving aperture. The repercussions of such effect and it's influence on the channel transmittance, as well as quantum properties of light, have been studied [204] and have been formulated as the beam-wandering model. Transmission efficiency (being a square of transmission coefficient $T^2 = \eta$) of the (normalized in XY) Gaussian beam, emitted at aperture with area $\mathcal{A}$, and propagating along z, generally can be written as [204]:

$$T(k)^2 = \int_{\mathcal{A}} dxdy\,|U(x,y,z,k)|^2, \tag{3.13}$$

where k is the wave number. Assuming dominance of the carrier wave number $\eta \approx \eta(k_0)$, Eq.(3.13) can be simplified to incomplete Weber integral and even further to the following analytical expression [213]:

$$T^2 = T_0^2 \exp\left[-\left(\frac{r_0}{R}\right)^{\lambda}\right], \tag{3.14}$$

determined using distance from the beam-spot center to aperture center r_0, as well as maximal transmittance (within the beam-spot) η_0. The latter is given as:

$$T_0^2 = 1 - \exp\left[-2\zeta^2\right], \tag{3.15}$$

where $\zeta = a/W$ is the ratio between receiving aperture and beam-spot radii. Now, respectively, shape and scale parameters are given by:

$$\lambda = 8\zeta^2 \frac{\exp\left[-4\zeta^2\right] I_1(4\zeta^2)}{1 - \exp\left[-4\zeta^2\right] I_0(4\zeta^2)} \left(\ln\left[\frac{2\eta_0}{1 - \exp\left[-a\zeta^2\right] I_0(a\zeta^2)}\right]\right)^{-1}, \tag{3.16}$$

$$R = a\left(\ln\left[\frac{2\eta_0}{1-\exp[-4\zeta^2]I_0(4\zeta^2)}\right]\right)^{-1/\lambda}, \tag{3.17}$$

where $I_n(x)$ is the modified Bessel function of the respective order [214].

The probability distribution of the transmittance is determined by a beam-spot, centered around the point on distance d from the aperture center, which is normally distributed with variance σ^2[17], and is given by log-negative generalized Rice distribution. The generalized Rice distribution can be written as follows:

$$\begin{aligned}\mathcal{P}(T)_{Rice} =& \frac{2R^2}{\sigma^2\lambda T}\left(2\ln\frac{T_0}{T}\right)^{(2/\lambda)-1} \mathrm{I}_0\left(\frac{Rd}{\sigma^2}\left[2\ln\frac{T_0}{T}\right]^{(1/\lambda)}\right) \\ & \times\exp\left[-\frac{1}{2\sigma^2}\left\{R^2\left(2\ln\frac{T_0}{T}\right)^{(2/\lambda)}+d^2\right\}\right]\end{aligned} \tag{3.18}$$

If the beam is properly aligned and beam-spot variance is centered around the center of the aperture $d = 0$, distribution (3.18) simplifies to log-negative Weibull distribution [215].

$$\mathcal{P}(T)_{Weibull} = \frac{2R^2}{\sigma^2\lambda T}\left(2\ln\frac{T_0}{T}\right)^{(2/\lambda)-1} \times\exp\left[-\frac{1}{2\sigma^2}R^2\left(2\ln\frac{T_0}{T}\right)^{(2/\lambda)}\right] \tag{3.19}$$

Both transmittance moments required for the security analysis $\langle\eta\rangle = \langle T^2\rangle$ and $\langle\sqrt{\eta}\rangle = \langle T\rangle$ can be obtained from Eqs.(3.18,3.19) in a similar way as in Eq.(3.12).

The beam wandering model has been successfully applied to assess the attenuation in short atmospheric channels with weak turbulence [108, 216, 217] and to study beam-broadening technique for transmittance stabilization, described in Ch. 6. Furthermore, the model was used to estimate feasibility of CV QKD protocols in significantly longer (vertical) links where beam broadening is main factor determining the overall transmittance of the link. Such long links include satellite-to-ground [218–220] and satellite-to-submarine [206].

Elliptic-beam model

Beam-wondering model is applicable only for the links with dominant beam wandering, however in general turbulence can cause beam broadening and deformation, as well as beam wandering. Elliptical-beam model has been developed [6] to account for these effects, and it can successfully be applied for channels with weak, or strong turbulence.

The model takes into account a turbulence induced deformation of the beam-spot shape from circular to elliptical, described by semi-axes $W_{1,2}$, and angle $\phi \in [0, \pi/2)$ between semi-axis W_1 and x-axis. The distance vector between aperture and beam-spot

[17] Both atmospheric turbulence (characterized by Rytov parameter) and source-deflection variance contribute to σ^2.

ellipse centers is given by (T indicates the transpose)

$$\mathbf{r_0} = (x_0,\, y_0)^T = (r_0 \cos\varphi,\, r_0 \sin\varphi)^T.$$

The transmittance in the channel can be approximated as [6]:

$$\eta = \eta_0 \exp\left[-\left(\frac{r_0}{aR\left[2/W_{\text{eff}}(\phi - \varphi_0)\right]} \right)^{\lambda[2/W_{\text{eff}}(\phi-\varphi_0)]} \right], \tag{3.20}$$

where η_0 is the transmittance at the center point $r_0 = 0$

$$\begin{aligned} \eta_0 = 1 - I_0 \left(a^2 \left[\frac{1}{W_1^2} - \frac{1}{W_2^2} \right] \right) \exp\left[-a^2 \left(\frac{1}{W_1^2} + \frac{1}{W_2^2} \right) \right] \\ - 2 \left(1 - \exp\left[-(a^2/2) \left(\frac{1}{W_1^2} - \frac{1}{W_2^2} \right)^2 \right] \right) \\ \times \exp\left[- \left(\frac{\frac{(W_1+W_2)^2}{|W_1^2 - W_2^2|^2}}{R\left(\frac{1}{W_1^2} - \frac{1}{W_2^2} \right)} \right)^{\lambda\left(\frac{1}{W_1^2} - \frac{1}{W_2^2} \right)} \right]. \end{aligned} \tag{3.21}$$

Provided $W_1 = W_2$ Eq.(3.20) reduces to Eq.(3.14). Now, the W_{eff} in Eq.(3.20) is the effective circular beam-spot, calculated using a, W_1, W_2, ϕ, φ:

$$W_{\text{eff}} = 2a \left(\mathcal{W} \left[\frac{4a^2}{W_1 W_2} \exp\left(\frac{a^2}{W_1^2}\{1 + 2\cos^2[\phi - \varphi_0]\} + \frac{a^2}{W_2^2}\{1 + 2\sin^2[\phi - \varphi_0]\} \right) \right] \right)^{-1/2}, \tag{3.22}$$

and λ, R are, similarly to Eqs.(3.16,3.17), shape and scale parameters, respectively:

$$\lambda(\xi) = 2a^2\xi^2 \frac{e^{-a^2\xi^2} I_1(a^2\xi^2)}{1 - e^{-a^2\xi^2} I_0(a^2\xi^2)} \left[\ln\left(2 \frac{1 - e^{-a^2\xi^2/2}}{1 - e^{-a^2\xi^2} I_0(a^2\xi^2)} \right) \right]^{-1}, \tag{3.23}$$

$$R(\xi) = \left[2 \frac{1 - e^{-a^2\xi^2/2}}{1 - e^{-a^2\xi^2} I_0(a^2\xi^2)} \right]^{-1/\lambda(\xi)}. \tag{3.24}$$

To acquire transmittance probability distribution one needs to know the distribution of key components: deviation of the beam-spot from the aperture center r_0, rotation angle of the deformed beam-spot ϕ, and radii of the beam-spot semi-axes $W_{1,2}$. The latter can also be represented through the relation to W_0 - the initial beam-spot radius, as $W_{1,2}^2 = W_0^2 \exp\Theta_{1,2}$. The angle ϕ and φ_0 are assumed to be distributed uniformly, r_0 according to Rayleigh distribution, and $\Theta_{1,2}$ normally. The set of parameters form a

vector $\mathbf{v}$, that governs $\eta(\mathbf{v})$ in Eq.(3.20) which in turn can be used to define the probability distribution:

$$\mathcal{P}_{\text{elliptical}}(\eta) = \frac{2}{\pi} \int_{\mathbb{R}^4} d^4\mathbf{v} \int_0^{\pi/2} d\phi \, \rho_G(\mathbf{v}, \mu, \Sigma) \delta \left[\eta - \eta(\mathbf{v})\right], \tag{3.25}$$

where $\rho_G(\mathbf{v}, \mu, \Sigma)$ is the Gaussian probability density of the vector $\mathbf{v}$, mean μ and covariance matrix Σ.

In the conditions where beam distortions becomes small or negligible, *i.e.* beam-spot remains circular, the elliptical-beam reduces to beam-wandering model. However, generally the elliptical-beam approximation allows to achieve more accurate predictions of the transmittance in channels with weak and weak-to-moderate turbulence than those based on beam wandering or log-normal distributions [6]. Furthermore, the model can also be efficiently adapted to incorporate additional weather effects such as haze and rain [7]. We use the model to study the role of squeezing on the security of CV QKD protocol established in short, atmospheric, urban links in Ch.7.

Improvement methods

In certain settings, transmittance of the free-space channel can indeed be lower than that of the fiber channel of equal length, however due to constant change of weather conditions expected attenuation and turbulence induced effective noise may variate significantly. The duration of uninterrupted free-space QKD link operation as well as the secure key rate, are highly dependent on the atmospheric conditions. To enhance and stabilize the performance of the QKD protocol over the free-space channel one can employ the following techniques: equipment improvement (*e.g.* to decrease beam divergence, or to reduce losses by increasing the size of the receiving aperture) [221], adaptive optics [222], beam tracking [223], optimization of the signal state and applied modulation, and post-selection [108, 186].

The improvement of the quantum signal propagation quality depends on beam tracking method and accuracy, however there is a limit of tracking technique precision [18]. Estimation of beam displacement deviation depends foremost on a probe state (whether it is a mixture of coherent state, or spatially and/or temporally entangled state) and its modal structure [225]. Optimal probe also requires appropriate receiver, and both, in fact, have already been designed in Gaussian domain (multimode squeezed state and homodyne-type measurement) [226].

Another approach to stabilize channel transmittance fluctuations suggests decreasing the ratio between aperture and beam radii $\zeta = a/W$. By expanding the beam one actually decreases the mean transmittance, but at the same time maximizes the probability of (partial and full) incidence, thus reducing transmittance fluctuations. The technique has been tested in 1.6 *km* urban free-space link in Erlangen (Germany) [3]. It was shown

[18] CubeSat Quantum Communication Mission was limited to 3 μrad of pointing [224], while mechanical adjustments of the telescope position, and piezo fast steering mirrors allow to enhance pointing precision to 0.6 μrad [77]).

to be advantageous, but requires beam optimization and adjustment according to given conditions.

Instead of, or in conjunction with active techniques for influencing the channel properties (such as by beam tracking or beam expansion), one can also disregard the data corresponding to lower values of transmittance [108, 186]. Such post-selection allows to decrease fluctuations of channel attenuation (or in other words the fading variance $Var(\sqrt{\eta})$, as in Eq. 2.25), which consequently leads to quantitative improvement of the secure key rate (see Sec. 2.1.3). For channels exhibiting strong turbulence, *i.e.* high transmittance fluctuations, post-selection can even restore the security of the CV QKD protocol. Post-selection has been shown to be effective for sufficiently large blocks of data, even if composable security is taken into account [227, 228].

3.3 Detection

CV QKD relies on the coherent detection (homodyne or heterodyne) to measure modulated quadratures of the incoming light field. The coherent detection enables to implement protocols using off-the-shelf optical communication components [43,61,64]. Furthermore, LO employed in the detection process acts as an extremely selective and effective filter, allowing to establish CV QKD protocols over channels with significant amount of background noise (non-signal mode) photons, *e.g.* free space atmospheric channels, or simultaneously with intense classical channel in telecom fiber networks [229, 230]. Strong LO also allows to suppress the influence of detector electronic noise [231, 232]. Aside from imperfections (imbalance of the optical beam splitter, imperfect detector quantum efficiencies, etc.), there are numerous implementation issues connected with the receiving trusted station such as side channels, or susceptibility to attacks via tampering with LO that is transmitted simultaneously with the signal through untrusted channel [233]. Receiving side is also exposed to additional light from the untrusted channel, allowing for potential attacks on detectors or side channel noise infusion [234]. In current section we described repercussions of aforementioned weaknesses and mention possible counteracting strategies.

3.3.1 Sources of noise

High efficiency of the detectors used in homodyne detection is one of many incentives for adopting CV QKD. Nevertheless, the detectors are still not perfect. Realistic detectors can be modeled by means of linear-optic interaction, *i.e.* by addition of an attenuator prior to the ideal detector, described by transmittance value η_{HD} [119]. Another optical component crucial for implementation homodyne detection is a balanced optical BS, used for coupling of the signal mode and LO. Slight deviation from 50:50 transmittance - reflectance ratio can lead to additional noise in the measured data [232]. Such deviations cannot be compensated by attenuating classical amplified photocurrents, since CV QKD detection requires a time resolution of individual laser pulses, and avoidance of the low frequency noise influence (hence a flat amplification profile over the whole frequency range) which imposes limitations on the design of the electro-optical scheme (*i.e.* subtraction has to be performed prior to the amplification) [235, 236]. Hence, both BS imbalance and discrepancy between detector efficiencies are balanced by introducing variable optical attenuator into one of the arms of a homodyne detector [232, 237].

Electronic noise

Electronic components and amplifiers involved in homodyne detection exhibit thermal noise that contributes to the measurement outcomes. Such noise with variance N_{el} is independent both from the measured signal quadratures, and from the power of LO. The proportionality of the electronic signal to the quadrature value fluctuates due to the electronic noise and thus such noise contributes to the measured quadrature values.

In order to eliminate electronic noise one calibrate the measurement setup, *i.e.* sample a vacuum state (by sending only the LO to the homodyne detector) and acquire the relation between experimental data and theoretically defined vacuum fluctuations level - shot-noise unit [153]. Since the relation has to be known for the whole data set and Eve can attack the calibration procedure, repeated calibration is needed to circumvent Eve's attacks on calibration during key generation [233]. Subsequently the values of calibration factor are used to correct the actual signal data [233].

Electronic noise (assuming it is trusted[19]) can be treated as additional trusted losses or lower detection efficiency: $\eta'_{HD} = \eta_{HD}/(1+N_{el})$ [238]. The equivalence stems from the calibration, which rescales the measurement outcome to cancel out the electronic noise, similarly to rescaling due to optical loss. After the calibration, the measured value can be treated as obtained from the detector with effective efficiency η'_{HD}, and no electronic noise $N_{el} = 0$ [238]. Typically electronic noise does not translate into a significant loss of the detector efficiency, *e.g.* electronic noise level of 13 dB below shot noise (at LO with 8.5×10^8 photons per pulse) is equivalent to $\eta'_{HD} = 95\%$ (assuming $\eta_{HD} = 1$) [232].

Electrical pulse overlap

One can expect the generated key rate to be directly proportional to the operation rate, however in practice finite bandwidth of the electronics in homodyne detector can introduce limitations [239]. Repetition rate of the source should be optimized according to detector bandwidth, to minimize the overlap between consequent electrical pulses at the output of the detector. As the repetition rate is relatively low so is the probability of contribution of adjacent pulses to measured value. However maintaining low repetition rate naturally imposes limitation on the achievable secret key rate. Yet, if the repetition rate would be relatively high the noise caused by the overlap can be significant. In terms of security analysis, the overlap translates into additional variance-dependent excess noise $\varepsilon_{\text{overlap}} = 2Ve^{B^2/R^2}$, governed by the ratio between the bandwidth B and the repetition rate R [232]. Optimal approach is to tune the repetition rate according to the bandwidth so that the noise remains negligible, while the key rate is almost proportional to the repetition rate [240].

3.3.2 Local Oscillator attacks

It is assumed that power fluctuations of the LO are being canceled out during subtraction, but due to discrepancy between photodiodes, or amplifier parameters (efficiencies, response time, etc.) residual influence of the fluctuations may persist [241][20]. Similarly to the signal laser, the relative intensity noise is as well exhibited by the LO, and contributes to excess noise proportionally to the quadrature variance of the measured signal [153]. In practical implementations LO power fluctuations are assumed to be low and hence the

[19] Untrusted electronic noise is attributed to the channel influence as additional loss or noise.

[20] Again, the discrepancies cannot be eliminated electronically in a time domain homodyne detection where amplification follows signal subtraction [235].

influence on the resulting key is negligible. However, it is still required to monitor LO intensity, as in principle the fluctuations can be induced by the adversary (without affecting LO phase), and exploited for the LO intensity attack [242]. During the attack Eve can induce LO fluctuations using a variable attenuator, and since the output of homodyne detector is proportional to the power of LO, can directly influence the data recorded by Bob. Alternatively, *calibration attack* can alter the LO pulse shape to achieve the same result [233]. Both LO intensity and calibration attacks affect the estimation of the shot-noise and consequently forces Alice and Bob to underestimate the channel excess noise and, respectively, bound on int1ercepted information allowing Eve to acquire the key remaining undetected. To avoid the calibration attack one can perform real-time measurement of the shot noise [233]. Intensity attack can be prevented by stabilizing the LO intensity [243]. Furthermore, proper tuning of the LO can effectively add trusted noise to the reference side of the protocol and hence improve the key rate.

The vulnerability of the LO is a backdoor for numerous other types of attacks. Eve can, for example, exploit wavelength dependency of the beamsplitters used on Bob's side to disguise the channel excess noise caused by the intercept-resend attack. Such approach is also known as *wavelength attack* [244–246]. Using wavelength tunable laser diodes and intensity modulators, Eve can adjust the properties of resent signal and LO (along with supporting auxiliary state), and consequently control the coupling ratios on Bob's side to ensure that the outcome of the heterodyne measurement exactly corresponds to the data on her side. The attack cannot be avoided in all-fiber system by using practical wavelength filters, but rather by utilizing wavelength-independent BS.

A solution to vulnerabilities of a transmitted LO has been suggested in a form *local local oscillator* (LLO) [114, 189, 239]. In such configuration, strong reference beam for the measurement on Bob's side is generated by Bob himself. To actually generate the key, instead of LO, Alice sends to Bob a sequence of phase reference pulses, and both of them apply phase correction on the signal data. This implies that without involved phase correction process, to account for relative phase drift, Bob's measurement results are *a priori* decorrelated from Alice's data [190]. The main experimental challenge is maintaining a low phase noise caused by the drift of the relative phase between two remote lasers (on Alice and Bob's sides respectively). Nevertheless, LLO is a feasible solution for avoiding the possibility of majority of attacks, especially considering new and more affordable implementation designs [190].

3.3.3 Detector attacks

Aside from the calibration and the wavelength attacks associated with LO vulnerability, there are other attacks that rely on a finite range of linear response of the electronics involved in the homodyne detection. For the security analysis only second moments of the quadratures are relevant, while the mean values are typically not monitored by trusted parties, thus Eve is free to displace all signal states, altering the mean value without provoking an abortion of the protocol. The *saturation attack* [234] commences with a intercept-resend attack, but the displacements of re-sent states are chosen to partially fall

outside the linear response range of the detectors. When a quadrature value is actually outside the region, Bob's measurement yields a saturated value. By properly adjusting the applied displacement, Eve can therefore control the variance of the measured state and bias the estimation of the excess noise in the channel, therefore inducing a zero-error security break.

A more advanced *blinding attack* utilizing detector saturation has been recently suggested [247]. While also relying on coherent displacement of the re-sent states it also exploits a loss imbalance between two ports of the practical homodyne detector. The latter aspect significantly improves the feasibility of the attack, and distinguishes it from the saturation attack, which required phase locking to the Alice's laser. Furthermore, since the attack targets the detector itself rather than the LO, it can be successfully applied to the protocols based on LLO generation. A counteracting measure can be issued in a form of additional postprocessing to ensure the data falls within precalibrated security thresholds [247].

3.3.4 Multimode detection

A common approximation in CV QKD analysis is an assumption of single mode generation and detection. Aforementioned information leakage into auxiliary modes was shown to be a certain security threat (see Sec. 3.1.3). But even if the additional modes do not carry relevant information [21], it is important not to dismiss the multimode nature of the incoming states, as it can have negative repercussions for security of CV QKD protocols and can even lead to a security break [248].

Multimode detection implies the preparation of corresponding number of LO modes, *i.e.* distinguishable modes carrying states with strong amplitude, and all states sustaining identical phase. Whether or not trusted parties are aware of the modal structure determines the employed measurement, as well as the ability to discern the source of resulting noise bearing extensive security implications. If Alice and Bob do not take into account multimodal structure then the effect of auxiliary modes is equivalent to additional losses introduced in both arms of an EPR source. Now the influence of auxiliary modes can be either attributed to Eve (untrusted scenario) or assumed to be unavailable to Eve (trusted scenario). The former is security breaking even under the most optimistic conditions of individual attacks and perfect untrusted channel ($\eta = 1$, $\varepsilon = 0$). The latter is equivalent to addition of trusted preparation noise (see Sec. 3.1.4) and detection noise (see Sec. 3.3.5), which nevertheless can still lead to a security break [104].

The influence of multimode structure can be negated by symmetrization of the auxiliary modes, and partial or ideally complete knowledge of the detection structure and consequent multimode detection [248].

[21] Additional modes can be unoccupied, carrying vacuum states, however generally source may emit in some or all modes, with a thermal state variance in each independent mode [180].

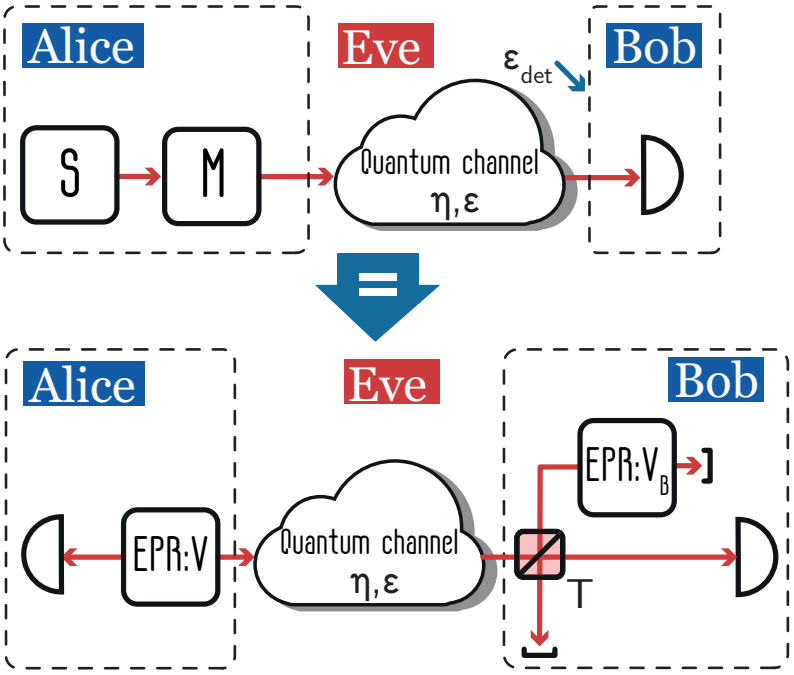


Figure 3.4: Detection noise in case of P&M (top) and equivalent EPR-based (bottom) scheme. With $V_B = \epsilon/(1-T)$, and coupling of the respective mode with the signal mode on the unbalanced BS: $T \to 1$, the equivalence of EPR-based scheme and the P&M scheme can be established.

3.3.5 Detection noise

The approach taken for the analysis of the noise on Bob's side of the protocol is identical to the previously discussed preparation noise, *i.e.* all sources of imperfections are generalized, with losses and noise modeled as linear interaction (see Fig.3.4) of the signal with a thermal noise mode (purified by the source $EPR : V_B$) on a BS with a fixed coupling ratio T. Just as with the preparation noise one can differentiate by attributing the purification of the noise to either Bob or Eve between trusted and untrusted noise respectively. The robustness to and influence of the detection noise on the security of coherent- or squeezed-state protocols is determined by the type of reconciliation used.

The model of the detection noise for both P&M and equivalent EPR-based schemes is shown in Fig.3.4. In P&M scheme (top) the noise alters the signal, so that the covariance matrix of the state measured by Bob reads

$$\gamma'_B = \begin{pmatrix} 1+\eta(V_S+V_M-1)+\epsilon_{det} & 0 \\ 0 & 1+\eta(\frac{1}{V_S}+V_M-1)+\epsilon_{det} \end{pmatrix}. \tag{3.26}$$

In an EPR-based scheme (Fig.3.4, bottom) the noise is considered to be a contribution from an EPR source that radiates states with variance V_B into modes C and D. Setting the variance $V_B = \epsilon_{det}/(1-T)$ establishes full equivalence between schemes. The covariance

matrix of the two signal modes therefore becomes:

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{1} & \sqrt{(V^2-1)\eta}\sigma_z \\ \sqrt{(V^2-1)\eta}\sigma_z & (1+[V-1]\eta+\varepsilon+\epsilon_{det})\mathbb{1} \end{pmatrix}, \tag{3.27}$$

where $\mathbb{1}$ is 2×2 unity matrix, and σ_z is the Pauli matrix (Eq. 2.14). A four-mode trusted state is now sufficiently described by the covariance matrix γ_{ABCD}. Reconstructing the latter allows to evaluate both the mutual information I_{AB} and the Holevo bound χ. If Eve controls both the output modes of the source V_B, the noise is effectively equivalent and contributes to the channel excess noise, while the scenario, where Eve controls only one of the modes, is treated as a type-B side channel, discussed later.

As already shown for the preparation side in Sec. 3.1.4, (optimized) trusted noise at the reference side can be beneficial for the security of the protocol. Hence, one can expect that trusted detection noise would be damaging for the DR-based protocol, since it decreases the mutual information between trusted parties, but does not influence accessible information of Eve. In optimistic conditions of infinite alphabet size $V_M \gg 1$, perfect post-processing $\beta = 1$, and purely attenuating channel $\varepsilon = 0$ the key rate reads

$$R_{DR}|_{\beta=1}^{V_M\gg 1} = \frac{1}{2}\left[\log_2\frac{\eta}{1-\eta} - \log_2\frac{V_S\eta+1-\eta+\epsilon_{det}}{V_S(1-\eta)+\eta}\right]. \tag{3.28}$$

which bounds tolerable detection noise $\epsilon_{det} < (2\eta-1)/(1-\eta)$. The tolerance to noise does not depend on the parameters of the protocol that are under control of the trusted parties, but rather on the parameters of the channel.

If properly adjusted, the noise can be advantageous for RR protocols. The reason is that the detection noise obstructs Eve's ability to recover the data obtained at the receiver side. However, the noise also decreases the mutual information between parties, and therefore must be optimized in order to be advantageous. Furthermore, the utility of the detection noise is limited to noisy channels, as it effectively improves the tolerance to channel noise. Provided the excess noise is high, addition of detection noise can even restore the security of the protocol [104].

The effect of such noise can also explain the advantages of CV QKD protocols with heterodyne detection on the receiver side in the RR scenario, since added vacuum noise acts as detection noise and consequently can enhance the robustness of the protocol. However, the noise in this case is not optimized, and usually more noise is required to significantly affect the performance of the protocol. While for the RR homodyne detection and optimized controlled detection noise is preferable for maximization of the secure key rate, heterodyne detection also allows to avoid the sifting stage of post-processing and doubles the key data generation speed [119].

3.3.6 Side channels

Trusted receiver side, similarly to the sender side, as discussed in Sec.(3.1.5), is susceptible to existence of side channels. Such side channels can either effectively increase main

channel losses, or infuse noise. The latter threatens the security of the protocol, as it deteriorates the key rate and leads to security break even in purely attenuating untrusted channel ($\epsilon = 0$) [1]. If the channel noise is present $\varepsilon \neq 0$, the side channel noise makes the protocol more susceptible to it, hence further limiting the range of secure conditions. The bound on the tolerance against such noise is ultimately determined by the coupling ratio of the side channel to the signal.

The effect of side channel noise can be destructive for the security of a CV QKD protocol, but it can be partially negated, and upon proper data manipulation even fully eliminated [1]. The method for achieving this relies on the knowledge of side channel coupling ratio η_B and performing interferometric coupling of the signal and output of the side channel. Performing weighed subtraction of the data after the measurement can completely remove the negative impact of the channel. For further details of security analysis and decoupling method see Ch.4.1.

Another approach aimed at complete elimination of side channels of the measurement side of the protocol and closing the loopholes on the receiving end of the protocol is achieved by the MDI QKD protocol [121]. The protocol involves the use of entangled sources by both trusted parties and delegate the measurement to an untrusted relay, hence allowing Alice and Bob to reliably shield their stations. The measurement results on the relay are combined and announced via classical public channel, and allow trusted party to decode each others initial variable. MDI QKD protocols have been successfully tested on the CV basis [249, 250], however the applicability of the protocol is limited, mainly due to secure distance restrictions. Despite limitations, increased security spurred active advancements of the protocol. Currently, along with improved security proofs [136], the protocol feasibility has been investigated for space-based QKD [251], and entanglement distillation (via photon subtraction) has been applied to extend the secure distance [252], although the performance of even improved protocol does not reach the fundamental limit of repeaterless quantum communications [253].

3.4 Classical data processing

In addition to quantum communication, CV QKD protocols require authenticated classical communication and involved classical processing [254–256] of the data amounted on trusted sides (after satisfactory amount of protocol rounds were performed) in order to obtain from partially correlated strings of data a universal composable secure key [36, 37][22]. The efficiencies of realistic classical algorithms involved vary and unavoidably some data will have to be sacrificed in order to generate the secure key. Consequently, in a real implementation, Alice and Bob can expect to use only a part of initially shared information, which is usually expressed as a fraction $\beta \in [0, 1]$ of mutual information I_{AB} (see Sec. 3.4.6). Post-processing efficiency was limiting the range of CV QKD protocols and, despite the improvement of existing and invention of novel algorithms, still plays an important role in determination of achievable performance of CV QKD protocols.

In the following section we will give a brief description of various techniques involved in classical post processing, and possible contributions to the overall post-processing efficiency β. Additionally, the correction to the accessible secure key rate due to operating with data blocks of finite size is mentioned at the end of the section.

3.4.1 Sifting

During this step, trusted parties eliminate the errors caused by inevitable mismatch in basis selection. Alice and Bob via classical authenticated channel, without disclosing any actual information, announce the encoding or the measurement basis used for each signal state. Since Alice can encode the letter of the alphabet into $\hat{x}$ or $\hat{p}$ quadrature with equal probability, as well as Bob who has a 50% chance to guess the correct quadrature to measure, approximately half of the data on each side will be discarded during this step[23]. The amount of discarded data can in principle be reduced or eliminated entirely, provided Bob has access to quantum memory with sufficient capacity, quality and storage life-time, as it would allow him to conduct measurement after Alice reveals sequence of correct encoding bases. However, experimental implementation of quantum memories are extremely challenging and expensive, and lack satisfactory characteristics [257, 258], thus it is currently an unfeasible solution for improvements of sifting procedure.

3.4.2 Authentication

One of the fundamental requirements for security of one-time pad encryption technique (and secure communication in general) is the ability to exchange authenticated messages. Generally this means that trusted party upon receiving the message can verify that is was indeed sent by the party with confirmed identity. In case of QKD protocols, Alice and Bob are presumed to share an authenticated classical channel that is fully resistant

[22] By being universal composable, successfully generated secure key ensures a secure realization of a larger protocol, that consists of other universal composable secure subroutines.

[23] CV QKD protocols that employ heterodyne detection on receiver side do not require sifting.

to tampering [259]. The authentication ensures the protection against man-in-the-middle attacks, and it is achieved by using *e.g. message authentication code* algorithms [260] based on cryptographic hash functions, block cipher algorithms, or Universal$_2$ hashing [261].

The capability to establish such authenticated channel implies pre-shared secure, or at least partially correlated secret information [262,263]. Furthermore, maintaining trustworthiness of a classical channel requires consumption of secret information. Usually in each QKD generation session a part of the key is reserved for authentication of a consecutive one.

3.4.3 Parameter Estimation

Crucial step for security analysis of any CV QKD protocol is the quantum channel estimation. For correct assessment of the upper bound on the information accessible to Eve, the trusted parties have to reconstruct full covariance matrix. However, knowing channel transmittance η and excess noise ε (due to optimality of Gaussian collective attacks) allows to evaluate the maximal information available to Eve in channel with given parameters once collective attacks are assumed. In order to avoid external manipulation, Alice and Bob must employ probe pulses that must be indistinguishable from the signal states. Commonly part of the transmitted correlated data is used instead. The data is disclosed via classical channel, and consequently must be discarded. The quality of the estimation depends on frequency of probe pulses, or on fraction of transmitted data used for channel estimation. In recent experimental implementations half of all signal pulses measured have been utilized solely for estimation [64].

Following the parameter estimation procedure shown in [264], for each pulse, the values x_S, x_0, and x_E are unknown (hence can all be treated as noise), while Alice has access only to x_M, and Bob, respectively, to the directly measured x_B. Due to this fact, the value, obtained by Bob, can be treated as:

$$x_B = \sqrt{\eta} \cdot x_M + x_N, \tag{3.29}$$

where the last term on the right side x_N refers to the overall noise, and has variance $V_N = \eta V_S + (1 - \eta) + \varepsilon$, where V_S is the variance of the initial carrier state (in respective quadrature), η is the channel transmittance, and ε is the excess noise. After sifting (3.4.1) both Alice and Bob have strings of data of length n, and their covariance is $C_{AB} = \sqrt{\eta} \cdot V_M$. Maximum likelihood estimator of the covariance can be calculated as:

$$\hat{C}_{AB} = \frac{1}{n} \sum_{i=1}^{n} (x_M \cdot x_B)_i, \tag{3.30}$$

where $(x_M \cdot x_B)_i$ is the pair of corresponding sent and received values, and $i \in [1, n]$. Now

using Eq.(3.30) one can calculate the estimate of η:

$$\hat{\eta} = \frac{1}{V_M^2}\hat{C}_{AB}^2. \tag{3.31}$$

Now using maximum likelihood estimator of V_N and Eq.(3.31) one can assess $\hat{\varepsilon}$:

$$\hat{\varepsilon} = \frac{1}{n}\sum_{i=1}^{n}(x_{B,i} - \sqrt{\hat{\eta}} \cdot x_{M,i})^2 + \hat{\eta}(1 - V_S) - 1. \tag{3.32}$$

The most pessimistic scenario is usually assumed and therefore within the confidence interval lower bound on transmittance η, and upper bound on ε are taken. Note that preceding procedure has to be performed for all variables and respective elements of the covariance matrix.

Surely, the increment of estimation efficiency limits the maximal speed of the information distribution for the given channel, however one can optimize the fraction needed for estimation over the parameters of the protocol [264]. The optimization becomes even more important taking into account finite-size effects, and limitations on encoding alphabet size imposed by other realistic effects, such as limited efficiency of post-processing $\beta < 1$, or transmittance fluctuations in atmospheric channels. The requirement for accurate estimation is elevated even further in the latter.

However, it has been shown, that the whole raw keys can be simultaneously used for both channel estimation, and further secure key extraction. This can be achieved by *e.g.* modulating the signal states twice, with the second modulation used solely for estimation purposes [264], or performing error correction prior to parameter estimation [94]. In MDI CV QKD protocols the estimation can be avoided as the parameters and covariance matrix can be directly inferred from relay measurements outcomes [250, 265].

3.4.4 Error correction

At this stage, the trusted parties start with a correlated sequence of continuous (approximately) Gaussian variables and their task is to end up with an errorless discrete key. Even though it may seem more intuitive to use continuous key due to the nature of carrier states and encoded information, it would also imply the usage of continuous version of one-time pad, which is feasible, but can be challenging to implement with sufficient noise resistance [266]. The usage of noisy continuous data may also introduce additional complications during authentication stage. Lastly, error-correction algorithms are faster and more efficient in case of discrete data.

As mentioned previously, there are two directions of reconciliation, depending on the choice of the reference side - *direct reconciliation*, where Bob is forced to infer the values originally encoded by Alice, and *reverse reconciliation*, where Alice is the one to correct her classical data according to the measurements outcomes on the Bob's side. While the use of RR allows trusted parties to potentially (in noiseless channels) tolerate arbitrary amounts of losses, DR approach limits QKD protocols to $\eta > -3dB$ channels. However,

DR is still a viable option (*e.g.* for infrared to microwave quantum cryptography [155]) due to increased robustness against preparation noise (see Sec. 3.1.4). The choice of reconciliation direction can also influence the choice of error correction algorithm.

Efficient error correction was the main limitation of early implementation of CV QKD [58, 129]. On top of limited reconciliation efficiency, the raw key rate is also affected by error-correction output rate and frame error rate. The former is connected with computational time of the algorithm, which can create a bottleneck for protocol output, and the latter is connected with the probability of incorrect message decoding, which may cause additional reduction of the generated key length.

Important codes used for reconciliation are polar [267], and low-density parity check codes (LDPC) [268, 269]. The latter are used in sliced [59] and multidimensional [270] reconciliation algorithms. One or multiple LDPC may be used to create a compressed version of the reference side data. This compressed version is then sent via authenticated classical channel and decoded. Decoding speed heavily depends on various parameters *e.g.* number of iterations, or number of terms in parity-check equations. Optimization of decoding procedure is a nontrivial task as generally the parameters of the code are highly interdependable, *i.e.* higher efficiency codes (that operate closer to Shannon limit) may have lower number of required iterations, but at the same time bigger size of parity-check equations [129]. In state-of-the-art CV QKD implementations, multi-edge type LDPC are being used in channels of 120 km length with feasible physical parameters [271].

After successful decoding both parties should have identical raw keys on their sides. To verify this, without disclosing any further information, they can use a hash function [272] (which would act as an error amplifier, making any discrepancies between data sets apparent). The latter is chosen with uniform probability from the family of hash functions, and used on both data sets. The hash value is then exchanged and compared, if the values are different, the protocol is aborted, and keys are discarded. In case the values match, Alice and Bob are confident (up to some probability that depends on the type of the hash function used) that shared keys are identical.

3.4.5 Privacy Amplification

The last step of classical processing is privacy amplification. The goal of this step is to eliminate partial knowledge of an eavesdropper on the shared corrected key, and consequently, to distill the secure key. Typically it is achieved using a family of universal hash functions that receive on the input, aside from the original data string, a random seed and output (possibly shorter) sequence with higher entropy, than the input string. The quality of such seeded randomness extractors is determined by the collision probability which is the probability for an eavesdropper, using different input, to obtain the same output, as the trusted parties would. The collision probability depends on the length of the input, the output, and on the hash function itself. One of the widely used hash functions is based on (modified) Toeplitz matrix [273], which requires short seed length, has relatively low complexity and allows for high-speed implementation [47, 113].

Alternatively to employing classical processing one can reduce (and possibly elimi-

nate completely) Eve's correlations with the signal states by performing entanglement distillation. However, the latter require non-Gaussian operations [54, 274] and can be experimentally challenging [275, 276].

3.4.6 Limited post-processing efficiency

Taking into account the effects of various algorithms with finite efficiencies, used in classical post-processing, it is evident, that trusted parties cannot operate in the Shannon limit and extract exactly mutual information I_{AB}, but merely the fraction of it. To account for this during estimation of lower bound on the security 2.34 β is introduced:

$$R = \beta I_{AB} - \chi_E.$$

The values of β range from 0 to 1, where $\beta = 0$ means trusted parties do not extract any information at all, while $\beta = 1$ is the theoretical limit of perfect post-processing. The efficiency can be defined as [271]:

$$\beta(s) = \frac{R_C}{C(s)}, \tag{3.33}$$

where s is a signal-to-noise ratio (SNR), R_C is the rate of code used, and C is the channel capacity. The codes are designed for a specific type of channel, but, most importantly, depend on the signal-to-noise ratio. Typical values of expected efficiency now range $\beta = [0.93, 0.98]$ [61, 65, 255, 271]. In practice the efficiency β is not known prior to actual key distribution [65], and may deviate from expected value given by Eq. 3.33. Despite the existence of codes with high achievable efficiency and close to the theoretical limit, they, nevertheless, impose threshold on the variance of the modulation of the protocol.

After a certain value the modulation variance increase starts to contribute more to the accessible information of the adversary than to the the information between trusted parties reducing the gap between trusted mutual information I_{AB} and the Holevo bound χ_E on Eves information regarding the key on the respective reconciliation side. As illustrated in Fig. 3.5, for lower values of β in DR scenario, the coherent-state protocol cannot generate secure key at all, and requires either to employ algorithms with even higher efficiencies or resort to the squeezed-state protocol. The latter can still provide a secure key even with moderate squeezing $-3dB$. In RR scenario, the coherent-state protocol is still viable, however allows for a very limited modulation variance.

Despite the reconciliation direction or the variance of the initial carrier state, variance of the signal modulation must be optimized. The squeezed-state protocol can additionally be improved by increasing squeezing, which in high loss channels translates in (almost) linear increase in tolerance towards the excess noise, and most importantly allows to use higher range of modulation values, thus increasing the size of the encoding alphabet (see [103] for more detailed description and treatment of limited post-processing effects). Moreover, optimal modulation of squeezed states up to a shot-noise unit in principle allows to eliminate information leakage in purely attenuating channels [277], which theoretically allows key distillation from any non-zero mutual information upon arbitrarily low β .

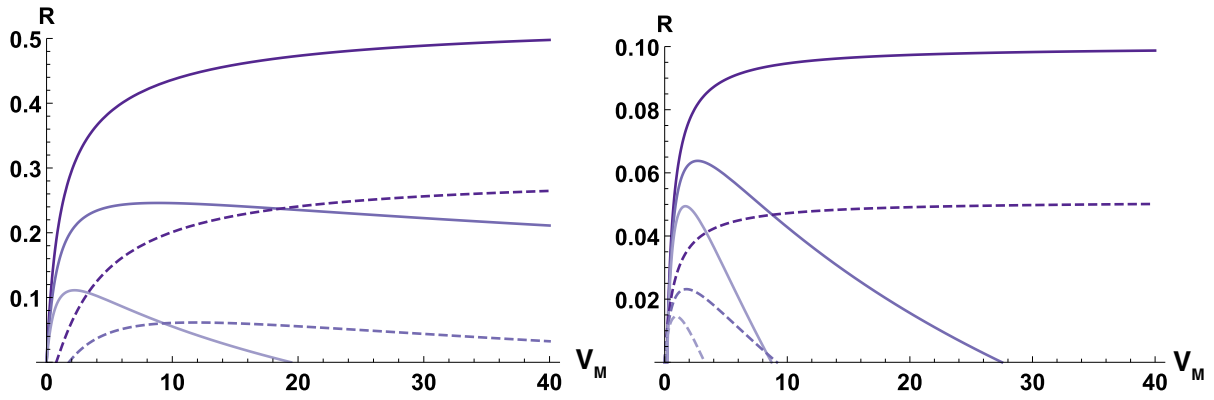


Figure 3.5: Secure key rate dependence on the modulation V_M of CV QKD protocol with direct reconciliation (left) and reverse reconciliation (right). Post-processing efficiency (starting from bottom) $\beta = 80\%, 90\%, 100\%$. Solid lines correspond to the squeezed-state protocol ($V_S = 1/2$) in the channel with $\eta = 0.1$, and dashed lines correspond to the coherent-state protocol ($V_S = 1$) in the channel with $\eta = 0.6$. Excess noise $\epsilon = 0$. Limited post-processing limits encoding alphabet in both DR and RR scenarios. Furthermore, low efficiency β renders the coherent-state protocol insecure, thus requiring squeezing applied to the carrier states.

3.4.7 Finite-size effects

One of the typical assumptions of security proofs of QKD systems is operation in asymptotic regime, in which Alice and Bob exchange infinite amount of signals. In realistic implementations, this assumption of course does not hold true, and one has make adjustments to reachable performance of QKD protocols. The formalism used for correction of secure key rate is based on smooth min-entropy [89], and it was successfully applied in DV systems [278, 279], and later in CV systems as well [127, 267]. The CV QKD protocol under assumption of collective attacks, taking into account finite-size effects, can output secure key rate:

$$R_{DR(RR)} = \frac{n}{N}[\beta I_{AB} - \chi^{\varepsilon_{PE}}_{AE(BE)} - \Delta(n)], \tag{3.34}$$

where $\chi^{\varepsilon_{PE}}_{AE(BE)}$ is the *maximum* of the Holevo bound obtained using the estimated parameters, that are correct with the probability at least $1 - \varepsilon_{PE}$ [127, 264]. Now, n is Eq.(3.34) is the amount of signals actually used for formation of key, while N is the total amount of signals received and measured. Parameter estimation technique, that allow to use the data for both parameter estimation and key extraction, can potentially achieve $n = N$.

While in asymptotic scenario the generated keys are considered to be perfectly secure, in realistic scenario there is always a probability of failure ε_F (even though it can be made arbitrary small at the cost key length reduction):

$$\varepsilon_F = \varepsilon_{PE} + \varepsilon_{EC} + \varepsilon_{PA} + \bar{\varepsilon}, \tag{3.35}$$

where individual terms correspond failure probability on the stage of *parameter estimation*, *error correction*, *privacy amplification* respectively, while $\bar{\varepsilon}$ is the smoothing param-

eter. Upper bound on the information, obtainable by Eve is influenced by the precision of parameter estimation, hence in Eq.(3.34) is denoted by $\chi_{AE(BE)}^{\varepsilon_{PE}}$. Lastly the term is determined by the security of the privacy amplification:

$$\Delta(n) = (2\mathrm{dim}\mathcal{H} + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2\left(\frac{1}{\varepsilon_{PA}}\right), \tag{3.36}$$

where $\mathcal{H}$ is the Hilbert space of the encoded variable (for CV protocols where raw key is encoded into bits $\mathrm{dim}\mathcal{H} = 2$ [127, 280]). One can see, that the last term in Eq.(3.34) does not contribute significantly to $\Delta(n)$, given that ε_{PA} is a virtual parameter and can be optimized in the computation. Taking this into account, the value is mainly determined by the speed of convergence of the smooth min-entropy of the independent and identically distributed state towards the von Neumann entropy [127]:

$$\delta(n) \simeq 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}. \tag{3.37}$$

The correction value $\Delta(n)$ strongly depends on the block size, *e.g.* if the CV QKD protocol yields the key rate $R \leq 10^{-3}$ the block size has to be at least 2 billions to maintain the security [127].

4 | Side channels in Gaussian CV QKD protocols.

The following chapter presents the main results of two articles [1, 2] that explore the influence of side channels on the security of CV QKD protocols and suggest possible methods of compensation of negative effect of such channels (see Chapter 8 for copies of the published articles).

We investigate the impact of channels that are under partial control of an adversary, the so-called *side channels* on the security and robustness of the CV QKD protocols. We define a side channel as an auxiliary channel that may have either input or output controlled by a trusted party and output or input, respectively, controlled by an eavesdropper. The side channels represent means of information leakage from, or information distortion on presumably trusted side of the protocol, and stem from device imperfections, along with weaknesses in experimental design and/or explicit implementation of a protocol. The sender-side leakage can take place in particular in the case of imperfect modulation, *e.g.*, when the signal is mixed with a temporal, spectral,polarization, or spatial mode, which then leaves the sender station. The receiver-side noise infusion may, *e.g.*, be caused by imperfect light collection from a free-space channel with a background radiation.

From Eve's point of view, the side channels give way for either passive (noninvasive) attacks, where Eve can only receive the information *i.e.* control only the output of a side channel, or Eve can resort to interfering with the operation of the QKD protocol, *i.e.* control the input of a side channel.

4.1 Model

To accommodate a side channel into security analysis, and study their effects, we make adjustments (based on the linear-optical mode interactions) to the standard entanglement-based representation of a protocol on either sender or receiver side. To gain insights in security conditions we start the analysis of each individual side channel with the individual attacks, and then proceed to the optimal collective attacks. The side channels on the preparation side are referred to as **type-A** side channels, while those on the Bob's side

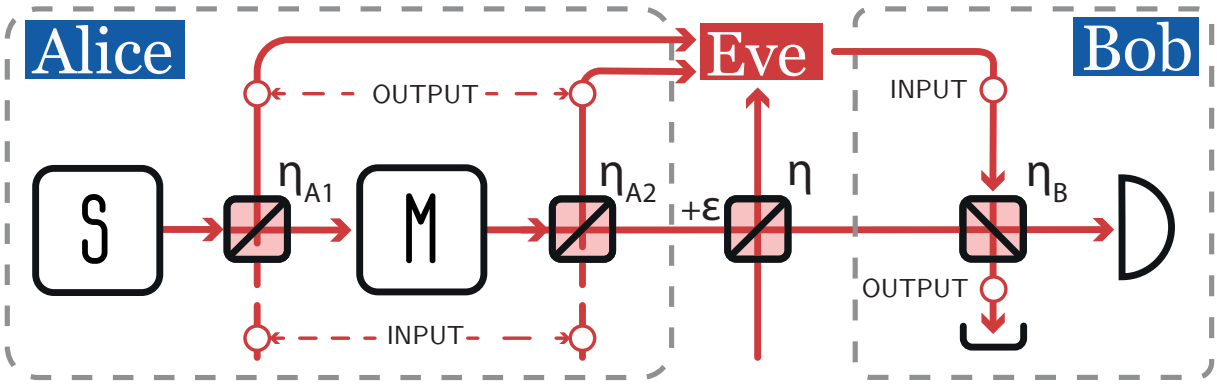


Figure 4.1: The model of a CV QKD protocol with side channels. All sides channels are modeled as a linear interaction with an auxiliary mode on a BS, on preparation side at η_{A1} or η_{A2}; on receiver side at η_B. The latter is referred to as type-B side channel, while others belong to type-A category. Generally the effect of Eve can be either passive (if she controls the output of the side channel) or active (if she controls the input of the side channel).

are referred to as **type-B** side channels, as depicted respectively in Fig. (4.1). We assume various scenarios of awareness of trusted parties regarding the side channel presence from an ignorant scenario, when side channel presence is not accounted for, to the case when side channels are partially controlled by trusted parties, and they perform a counteraction measure. In either scenario nor trusted parties nor the adversary can control the coupling ratio of a side channel to the signal, $\eta_{A_1,A_2,B}$ in Fig.4.1.

4.1.1 Type-A side channels

On Alice's side there can be typically two distinct points of intrusion: pre-, and post-modulation. Both of them have different effects on the tolerance of the protocol against channel losses and noise. While post-modulation channel can be accounted for by minor modification of an entanglement-scheme, the pre-modulation channel requires different purification-based schemes for proper incorporation.

Pre-modulation channel

For comprehensive security analysis we adopt a four-mode purification scheme, as described in details in Ch. 2.3.2. The side channel presence is modeled as a coupling between the signal mode B (prior to its interaction with mode D on T_1) and the side-channel mode F on BS η_{A_1} (see Fig.4.2). We consider two scenarios: when Eve controls the input of a side channel, injecting a thermal state of variance V_F, so that $\gamma_F = V_F\mathbb{1}$, while Alice controls the output; and an opposite case, when the input is attributed to Alice (then $V_F = 1$), and Eve (after the interaction with the signal) only receives the

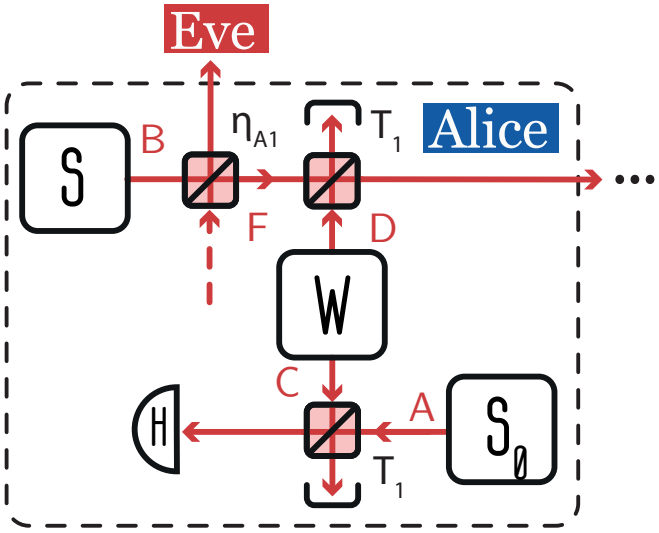


Figure 4.2: The preparation side of a CV QKD protocol in purification-based representation with the pre-modulation side channel.

side-channel output. The overall pure state before the channel is therefore described by a 5-mode covariance matrix γ'_{ABCDF}, where the mode leaked to Eve is described by the diagonal matrix $\gamma'_F = \mathrm{diag}[V_S\eta_{A_1} + (1-\eta_{A_1})V_F, 1/V_S\eta_{A_1} + (1-\eta_{A_1})V_F]$.

Post-modulation channel

Since the post-modulation side channel leaks the information regarding both the initial signal state and applied modulation, for a comprehensive security analysis it is sufficient to adjust the standard entanglement-based scheme by coupling the prepared signal (prior to the untrusted channel) on η_{A_2} with a side channel, as shown in Fig. 4.1. If the input of such semitrusted channel is the noise attributed to Eve, it is equivalent to the increase of excess noise in the untrusted channel, hence we focus on the case of input being in a vacuum state and possibly controlled by Alice. While Alice cannot modify the η_{A_2} value, or block the side channel completely, she can manipulate the state at it's input. We consider three types of states for Alice's use: a thermal state, a modulated pure Gaussian state independent from the signal, and a modulated (proportionally to the signal encoding) pure Gaussian state correlated with the signal.

4.1.2 Type-B side channel

As shown in Fig. 4.1, we consider Eve's intrusion at Bob's side before the balanced BS that splits the signal mode and forwards it along with LO towards detectors. Again, similarly to the case of type-A side channel we model the channel by interaction on BS η_B, and assume the coupling ratio is preset, known to trusted parties and cannot be changed by the adversary. The side-channel loss on the receiver side (symmetrical to the type-A side-channel loss on the sender side) is equivalent to increase of the overall channel loss,

hence we focus on the scenario of noise infusion onto the Bob's side, *i.e.* Eve is attributed full control over the input of the respective side channel.

Although Eve does not gain additional insights regarding the measurement outcome on Bob's side, she does affect the mutual information between the trusted parties, as the state received and measured by Bob turns to $V_B' \to V_B'\eta_B + (1-\eta_B)V_N$, where V_N is the variance of the state injected by Eve. Due to such deterioration of the measured state, on can expect such side channel to be a security threat already in a purely lossy channel.

4.2 Main results

4.2.1 Type-A side channel

Premodulation channel

The main consequence of the pre-modulation side channel presence is worsening of the initial cryptographic resource - a signal state. Assuming Eve takes a passive approach, side channel effect reduces to the losses on the BS η_{A_1} (see Fig. 4.1 for P&M scheme). Immediately apparent is the tolerance of the coherent-state protocol to such side channel, as pure losses do not alter the relevant properties of the coherent state and do not establish correlations between the signal and the leaking mode. The squeezed-state protocol, on the other hand, is impacted by such losses, as the signal effectively losses squeezing $V_s \to 1$, which leads to decrease of the mutual information between trusted parties, and correlations are established between the leaking mode and the signal state. Provided the input of the side channel is controlled by Eve, both the coherent- and squeezed-state protocol are facing the repercussions, as the signal state becomes thermal. While the presence of pre-modulation type-A side channel can be viewed as preparation noise 3.1.4, an important distinction is that the side channel also provides an eavesdropper with additional correlations with the signal. The difference between the key rates for the protocols with premodulation leakage R_F, and for the protocols with preparation noise $R_\Delta V$ is the highest for low loss main channel $\eta \to 1$ and is given by

$$R_F - R_{\Delta V} = \frac{1}{2}\log_2\left[\frac{1+V_M+\eta_{A_2}(V_S-1)}{V_M+V_S/\left(\eta_{A_2}+V_S-\eta_{A_2}V_S\right)}\right], \tag{4.1}$$

where V_S is the variance of the carrier signal state, and V_M is the variance of the encoding modulation. Even though additional correlations can effectively increase the Holevo bound, the increase is minor. The main effect on the security is played by the increased variance of the signal state, hence, the noise.

Overall pre-modulation side channel does decrease the key rate (secure distance) and tolerance to the excess noise in untrusted channel ϵ, but it does not lead to a security break (provided trusted parties confirm the variance of the signal does not deviate from predetermined value), as one would expect, since no actual information has been encoded into the states yet. Interestingly, pre-modulation channel can be reduced to the case

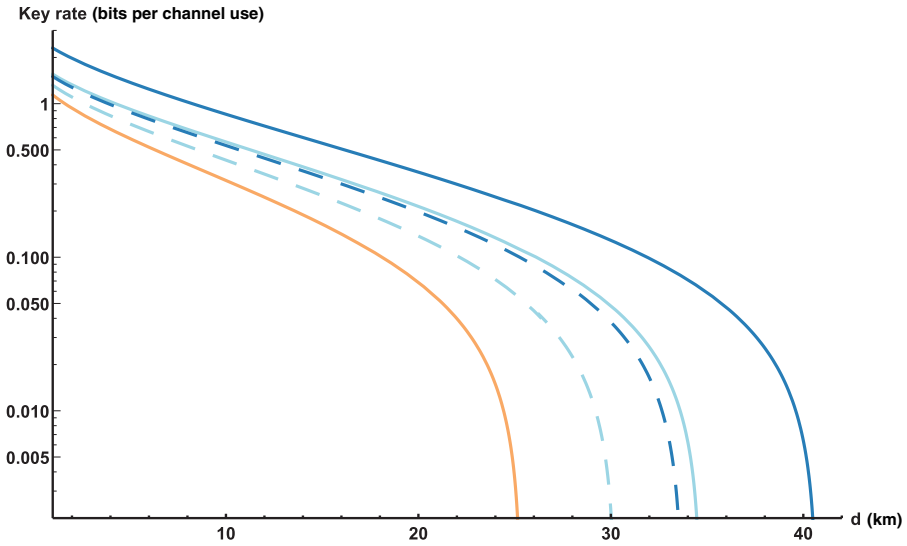


Figure 4.3: The key rate (in bits per channel use) versus distance d (in kilometers) in a standard telecom fiber (with attenuation of -0.2dB/km) in the case of collective attacks on the coherent-state protocol (orange, lower line) and the squeezed-state protocol with $V_S = 1/10, 1/2$ (upper dark blue and middle light blue, respectively). The premodulation channel coupling ratio $\eta_{A_2} = 0.5$ (dashed lines) and 1, *i.e.*, the absence of the side channel (solid lines). Modulation variance is optimized for given parameters, $\beta = 97\%, \varepsilon = 5\%$.

of further discussed post-modulation channel, assuming an appropriate scaling of the modulation [1].

Post-modulation channel

The side channel present after the modulation has completely different effect on the security of a CV QKD protocol than the channel before the modulation, as Eve can already obtain additional information regarding the encoded information. The first major effect of such side channel (depicted as BS η_{A_2} in Fig. 4.1) is an effective decrease of the channel transmittance η. Even under individual attacks, idealized conditions ($\beta = 1$, $\varepsilon = 0$), and in the limit of infinite modulation $V \gg 1$, the secure key rate reduces to:

$$R_{V\gg 1} = h \log_2 \frac{1}{1 - \eta_{A_2}\eta}, \tag{4.2}$$

which, evidently, scales down the channel transmittance ($h = 1$ or $1/2$ for the infinitely squeezed-[24], or the coherent-state protocol, respectively). However, the protocol remains secure, as one would expect in a noiseless channel.

If the channel noise is actually present, the tolerance of the protocols to the excess noise ε is substantially decreased. *e.g.* for the protocol under individual attacks, applying strong modulation $V_M \to \infty$ and facing low channel transmittance $\eta \ll 1$, the value of maximal tolerable excess noise ε_{max} is reduced to the value proportional to η_{A_2}, namely

[24] The squeezing of the protocol under consideration is not optimized.

$\varepsilon_{max} = \eta_{A_2}$ for the squeezed-state protocol. For the coherent-state protocol under same conditions this value is halved $\epsilon_{max} = \eta_{A_2}/2$ [1].

Assuming the equipment cannot be shielded from post-modulation side channel, one can infuse the input of the side channel with properly engineered state to partially compensate the effect of presence, or even fully restitute the secure key rate of a CV QKD protocol. The use of a thermal state does indeed diminish Eve's information (decreasing the Holevo bound), but also acts as preparation noise, and therefore limits the mutual information between parties.

Alternatively, Alice can send an independent and displaced state to the input of the side channel. This allows her to improve the correlations between trusted parties, and, simultaneously, reduce the correlations between signal and output of side channel. Under strong enough channel losses $\eta < 0.8$ and optimized modulation of the side-channel input state, Eve's advantage from access to side channel lessens, leading to improvement of the secure distance and robustness against channel noise.

Lastly, we suggest the method of (classically) correlated modulation on the input of the side channel. Such method fully decouples and decorrelates the side channel from the signal. Weighed displacement of the input allows to achieve destructive interference, resulting in complete absence of any information about the signal at the output of type-A post-modulation channel [1]. To achieve this effect for the squeezed-state protocol an additional squeezing of the side-channel input is required. Therefore, as long as Alice is aware of the type-A side channel, can properly characterize it and perform manipulations on the side-channel input, she can completely negate it's influence without relying on the channel estimation, or resorting to the use of entanglement or non-Gaussian operations.

4.2.2 Type-B side channel

Unlike type-A side channels, that contribute to Eve's knowledge about the generated key, but allow to maintain the security in optimistic conditions, the noise infusion on the receiver side via type-B side channel can lead to security break even in purely attenuating untrusted channels ($\varepsilon = 0$). In the limit of strong attenuation and infinite alphabet size (and individual attacks), the bound on infused noise variance was shown to be [1]:

$$V_N^{\max}|_{\eta \ll 1}^{V \gg 1} = \frac{1}{1 - \eta_B}. \tag{4.3}$$

In noisy channels the tolerance to excess noise ε_{max} is decreased as the consequence of side channel noise infusion, considerably limiting the security region.

We suggest a method for compensation of the negative effects by monitoring the output of such channel, and consequent proper manipulation of the data. More specifically, the method for achieving this relies on the knowledge of side channel coupling ratio η_B and performing interferometric coupling of the signal and output of the side channel. Bob must conduct homodyne detection of each mode and perform weighed subtraction of the data after the measurement. An optimal choice of weights can clear the generated key data from the added noise, hence completely removing the negative impact of the channel,

and restituting the performance of the protocol. For further details of security analysis and decoupling method see [1]. Note, that optimal applied weights depend on the coupling ratio η_B, which, according to initial assumptions, is always known to the trusted parties.

Summary

We present a concept of a side channel - a semitrusted auxiliary adversary channel that either leaks the information regarding the transmitted key to an eavesdropper, or obstructs the ability of trusted parties to grow a secret key. Such channel is distinct in its effect on the security of CV QKD protocols from previously studied losses or noise [104] (see also Ch.3.1.4 and 3.3.5). The effect of side channel on the security of CV QKD protocol greatly depends on the trusted side it appears on (type-A or type-B), point of intrusion (*i.e.* at which operation step the channel manifests itself), and attribution of the channels input/output.

For security analysis, we model side channels using existing entanglement-based schemes and linear-optical interactions, and investigate optimal strategies employed by Eve, assuming her access to a particular side channel, and show security conditions. Side channels were shown to be negatively influencing CV QKD protocols, they degrade the key rate and decrease the robustness to channel noise. Furthermore, side-channel noise infusion is security breaking even for a trusted receiver.

Aside from showing the repercussions of a side channel presence, it is important to develop counteracting strategies, aimed at negating introduced negative effects. The threat of security break can be alleviated by employing suggested compensation methods for respective side channel: modulating the input of post-modulation type-A side channel, and monitoring the output of type-B side with consequent data manipulation. Moreover, suggested methods can be combined with other performance improvement techniques, do not rely on the channel estimation, or resort to the use of additional sources of entanglement or to non-Gaussian operations.

5 | Multimode leakage from state preparation

This chapter contains a concise summary of main results obtained during the investigation of multimode modulation of CV QKD protocols (see [2] or Chapter 8 for a copy of a full article).

Here we consider the protocol, that follows the standard steps, as described in Sec. 2.1.1, however a crucial difference is generation of N independent, non-signal **leakage** modes during *State generation* step, and consequent modulation of the respective modes during *Modulation* step. The modes of interest are those that were not blocked or filtered out by trusted parties, *i.e.* the modes that are in full access of an eavesdropper.

5.1 Model

In order to conduct security analysis we start by establishing relations between all output modes of the preparation side. The scheme of the model is shown in Fig. 5.1. States in signal mode are initially characterized by a pair of quadrature values $Q_B = \{X, P\}$, and covariance matrix $\gamma_B = \mathrm{diag}[V_S, 1/V_S]$. N additional modes are present, with each mode $L_n \in \{L_1, \cdots L_N\}$ being described by $Q_{L_n} = \{X, P\}_{L_n}$, and covariance matrix $\gamma_{L_n} = \mathrm{diag}[V_{S,L_n}, 1/V_{S,L_n}]$. After the displacement Q_M the quadratures of the signal state become $Q'_B = Q_S + Q_M$ with covariance matrix $\gamma'_B = \mathrm{diag}[V_S + V_M, 1/V_S + V_M]$, while states in each additional mode $Q'_{L_n} = Q_{L_n} + k_n Q_M$, with respective covariance matrices $\gamma'_{L_n} = \mathrm{diag}[V_{S,L_n} + k^2 V_M, 1/V_{S,L_n} k^2 V_M]$, where $k_n = V_{M,L_n}/V_M$ is the ratio between variance of the modulation applied to an additional mode V_{M,L_n} and variance of modulation applied to the signal V_M ($k \geq 0$). Now, the initial covariance matrix, being $\gamma_{BL_1 \cdots L_N} = \gamma_B \oplus \gamma_{L_1} \oplus \cdots \oplus \gamma_{L_N}$, after the same ($k_{1 \cdots N} = k$) modulation has been applied to all leakage modes turns to

$$\gamma'_{BL_1\cdots L_N} = \begin{pmatrix} \gamma'_B & kV_M\mathbb{1} & \cdots & kV_M\mathbb{1} \\ kV_M\mathbb{1} & \gamma'_{L_1} & \cdots & k^2V_M\mathbb{1} \\ \vdots & \vdots & \ddots & \vdots \\ kV_M\mathbb{1} & k^2V_M\mathbb{1} & \cdots & \gamma'_{L_N} \end{pmatrix}. \tag{5.1}$$

After all states have been emitted, all leakage modes are assumed to be immediately intercepted by an adversary, while the signal proceeds to the untrusted channel where it is scaled by transmittance (for the sake of simplicity we start the analysis with noiseless channels), so that $\gamma''_B = \mathrm{diag}[\eta\,(V_S + V_M - 1) + 1, \eta\left(1/V_S + V_M - 1\right) + 1]$, and the covariance matrix describing the output of the preparation side and an Eve's mode γ'_E reads

$$\gamma''_{BL_1\cdots L_NE} = \begin{pmatrix} \gamma''_B & kV_M\sqrt{\eta}\mathbb{1} & \cdots & kV_M\sqrt{\eta}\mathbb{1} & -\sqrt{(1-\eta)\eta}\mathbb{1} \\ kV_M\sqrt{\eta}\mathbb{1} & \gamma'_{L_1} & \cdots & k^2V_M\mathbb{1} & -kV_M\sqrt{1-\eta}\mathbb{1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ kV_M\sqrt{\eta}\mathbb{1} & k^2V_M\mathbb{1} & \cdots & \gamma'_{L_N} & -kV_M\sqrt{1-\eta}\mathbb{1} \\ -\sqrt{(1-\eta)\eta}\mathbb{1} & -kV_M\sqrt{1-\eta}\mathbb{1} & \cdots & -kV_M\sqrt{1-\eta}\mathbb{1} & \gamma'_E \end{pmatrix}. \tag{5.2}$$

Though $\gamma''_{BL_1\cdots L_NE}$ 5.2 may be sufficient for basic analysis of some protocols, for comprehensive analysis, an entanglement-based scheme is required, and according to aforementioned description, it should satisfy following conditions:

1. Neither states sent by Alice nor states received by Bob nor correlations between them should be dependent on modulation (kQ_M, with variance k^2V_M) applied to the states in leakage modes.

2. Ratio between leaking modulation and signal should be $k \geq 0$ and it's values can exceed 1, since generally the variance of the modulation applied can be greater than that of applied to the signal mode.

3. The ratio k cannot be influenced by a trusted preparation party leaving only two parameters under Alice's control: signal modulation Q_M and amount of squeezing in the state Q_S produced by the source.

4. The optical configuration should be scalable considering the fact that trusted source can have an arbitrary multimodal structure.

One of the solutions that can satisfy all required conditions is provided by Bloch-Messiah decomposition theorem, that says that multimode evolution of an optical system governed by the linear Bogoliubov transformations can be decomposed into a combination of linear and non-linear optical components (multi-port interferometers, and single-mode squeezers) [97].

The security analysis can be significantly simplified by showing that a scenario with an arbitrary number of non-signal modes radiated from the preparation side can be reduced

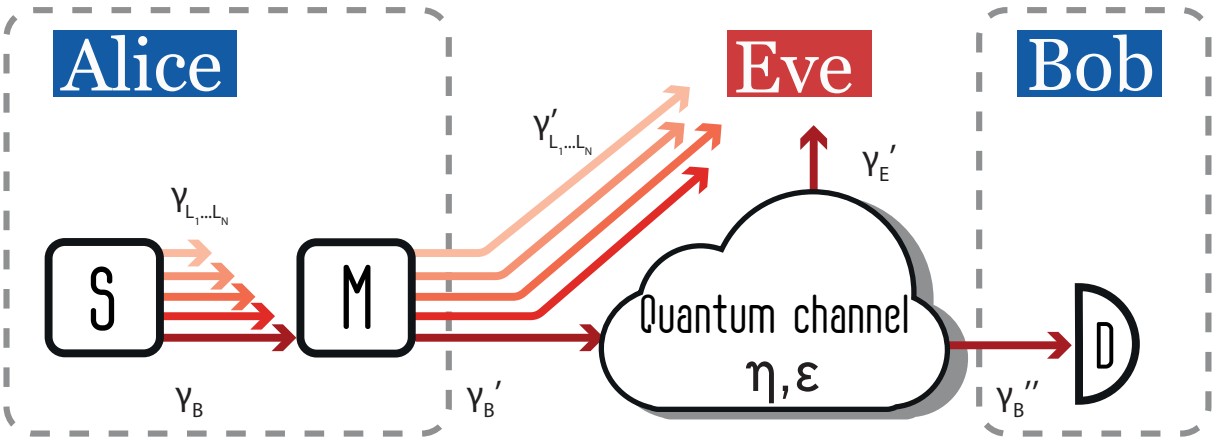


Figure 5.1: Prepare-and-measure scheme of the multimode leakage. The source S emits independent states into a signal mode, and into N additional modes. Each additional modes receive a separate displacement on the modulator M, however all displacements are correlated to the one applied to the signal state. The latter travels through the quantum channel to Bob, who measures the state on the homodyne detector D and records the output. All additional, unfiltered modes, are immediately intercepted by Eve. Note, that if a part of the signal is detectable, one can apply measurement of the residual light as in [281] in order to compensate for the negative impact of excessive modulation, taking into account the analysis of CV QKD over amplifying channels [282].

to the scenario where the signal and only a single effective leakage mode, described by the variance

$$V_{L_{eff}} = \frac{N}{\sum_n^N V_{L_n}^{-1}}, \tag{5.3}$$

and receiving the modulation with effective ratio

$$k_{eff} = k\sqrt{N}, \tag{5.4}$$

are emitted by the source. The Eqs. 5.3, 5.4 are applicable only for the protocol under individual attacks (See Sec. 2.1.3). Reduction to a single effective mode can also be numerically done in the most general case of collective attacks and independent and dissimilar initial variances of states in all modes V_{S,L_n}, and independent k_n.

5.2 Main results

We start the initial analysis with the individual attacks in noiseless channel, as they allow to assess essential security conditions in analytical form. Under direct reconciliation (with security defined as in Eq. 2.36) leakage via multimode modulation implies direct disclosure of the encoded key value, which quickly deteriorates the secure key. This can be illustrated

by the following expression for the key rate

$$R_{DR}|_{\eta\to 1}^{ind} \approx \frac{1}{2}\left(\frac{(\eta-1)V_M}{V\log[2]}\frac{(2k^2V_M+V)^2}{k^2V_M+V}+\log_2\left[\frac{V_M+V}{k^2V_M+V}\right]\right), \tag{5.5}$$

which is obtained provided the channel exhibits low loss $\eta \to 1$ and variances of all states are identical $V = V_S = V_{L_{eff}}$. Despite optimistic channel conditions, it is apparent, the security is lost if an adversary receives an exact copy of the modulation as the signal $k = k_{eff} = 1$. This situation is a CV analogue of the photon-number splitting attack in DV QKD [28, 283]. The security break can also occur even if the leakage modes are thermal $V_L \geq 1$.

The protocols utilizing reverse reconciliation (with the key rate defined as Eq.2.37) are not bounded by certain k value, and depending on parameters of the protocol can tolerate even $k > 1$. In the limit of strong modulation $V_M \to \infty$ the key rate becomes

$$R_{V_M\to\infty}|_{RR}^{ind} = -\frac{1}{2}\log_2\left[\left(1-\eta+\frac{\eta k^2}{V(1+k^2)}\right)(1+\eta[V-1])\right], \tag{5.6}$$

while the maximal tolerable leakage ratio k_{max} is

$$k_{max}|_{V_M\to\infty} = \sqrt{\frac{V(\eta-2+V-\eta V)}{(\eta-1)(V-1)^2}}. \tag{5.7}$$

The latter shows that there are several conditions for tolerance of an arbitrary leakage: either the untrusted channel is lossless $\eta = 1$, or the coherent-state protocol is employed. Alternatively, if squeezing value is set to $V = k^2/(1+k^2)$ the performance of the squeezed-state protocol becomes identical to that of the coherent-state protocol. However, the robustness against leakage can be further increased by squeezing optimization. The latter is independent of the channel parameters and is, in fact, given as

$$V^{opt}|_{V_M\to\infty} = \sqrt{\frac{k^2}{1+k^2}}. \tag{5.8}$$

With the increase of modulation ratio $k \gg 0$, the optimal squeezing V^{opt} does reduce and approaches shot-noise level, but generally squeezing always improves the secure key rate of the protocol.

Evaluation of initial influence of signal leakage is further supported by the results obtained from the study of collective attacks in realistic conditions, *i.e.* noisy channels $\varepsilon > 0$, and post-processing algorithms having limited efficiency $\beta < 1$. We therefore fix the former at feasible $\varepsilon = 1\%$; and optimize the modulation variance V_M due to requirements imposed by the latter condition. Fig. 5.2 depicts the comparison between the coherent- (dotted lines), and the squeezed-state protocols for various settings of modulation leakage $k = 0, 1, 1.5$ (blue, light blue, light green lines, respectively). Not only does the modulation leakage limit the secure distance of all protocols, but it can also render (provided strong leakage $k > 1$) the squeezed-state protocol (with fixed squeezing value) inferior, in terms

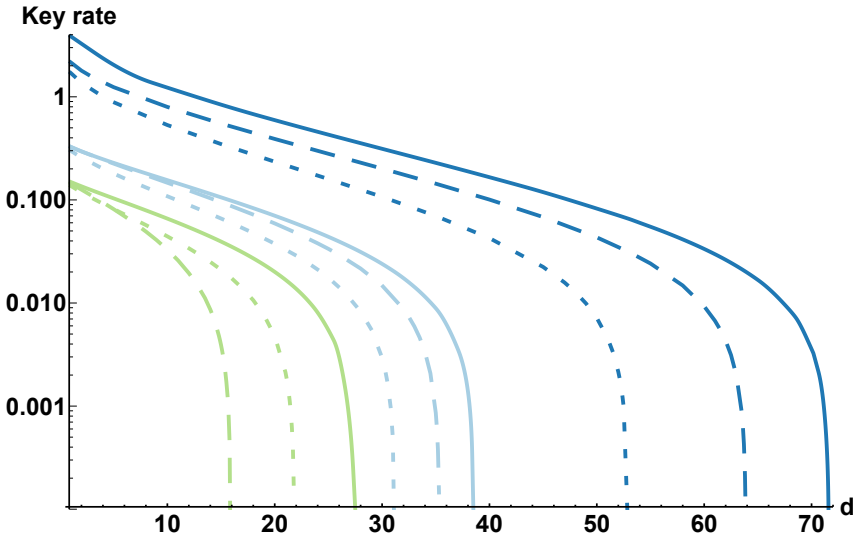


Figure 5.2: Key rate (in bits per channel use) versus distance d (in kilometers) in a standard telecom fiber (with attenuation of $-0.2dB/km$) under collective attacks in the case of modulation leakage for different values of ratio between additional and signal states modulation variances $k = 0$ (blue, upper lines), 1 (light blue, middle lines), 1.5 (light green, lower lines) for optimized squeezed-state protocol (solid lines), squeezed-state protocol (dashed lines) with $V_L = V_S = 1/2$ and coherent state protocol with $V_L = V_S = 1$ (dotted lines). $\beta = 97\%$.

of secure key rate, comparing to more accessible coherent-state protocol. Despite this, reasonable fixed squeezing can still outperform the coherent-state protocol in certain range of modulation leakage $k \leqslant 1$. Clearly, squeezing optimization always provides longer secure distances and is suggested for any value of modulation leakage k[25].

The protocols employing higher levels of squeezing, while being robust to noise and losses, also exhibit elevated susceptibility to leakage, as depicted in Fig. 5.3, where we examine the dependency of the key rate on the modulation leakage k, for a range of squeezing values V_S and different setting. Introduction of noise in the channel eliminates tolerance for arbitrary amounts of leakage. Under realistic conditions, security is lost when the leakage mode receives an identical or almost identical copy of the encoded key $k \approx 1$, even if the leaking information is carried by vacuum or thermal modes straight to an adversary.

Summary

All CV QKD protocols are sensitive to multimode modulation leakage, even in optimistic scenarios. It is especially devastating for CV QKD protocols employing direct reconciliation (which are important for implementations requiring tolerance to high levels of preparation noise [105]), as the security is lost if an eavesdropper receives a copy of the signal modulation.

[25]For $k = 0$ setting, squeezing optimization reduces to maximizing the available squeezing.

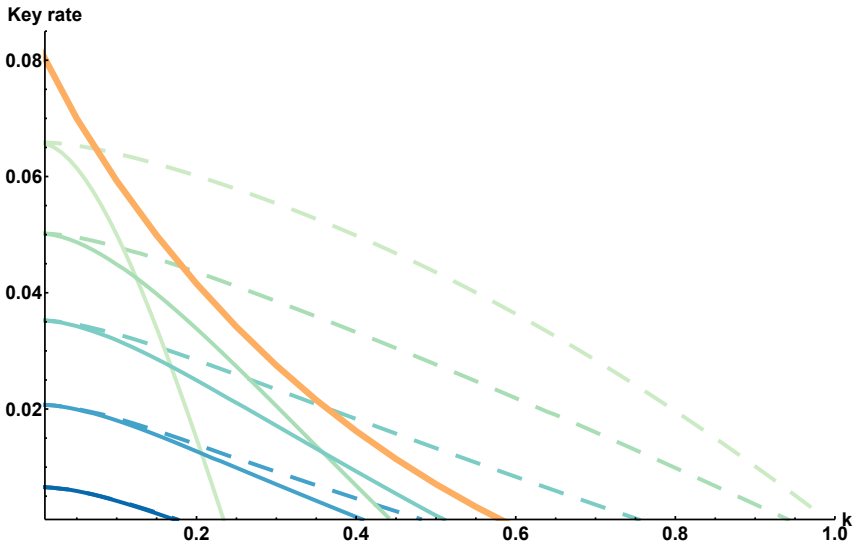


Figure 5.3: Performance of the squeezed-state protocol with a leakage from the modulator under collective attacks for different values of squeezing (starting from top) V_S=0.1, 0.3, 0.5, 0.7, 0.9 SNU ($\beta = 95\%$, $\eta = 0.1$). All solid lines display key rate with symmetry of signal and leakage variances ($V_L = V_S$). Thick (orange) line illustrates the key rate of protocol with both modulation V_M and signal squeezing V_S optimized. Dashed lines display the case when leakage mode input is fixed and independent of the signal ($V_L = 1$). Lowest solid and dashed lines, corresponding to $V_S = 0.9$, overlap. Evidently, if the leakage modes are initially independent from the signal, more modulation can be leaked without loosing the security of the protocol. Higher levels of squeezing directly translate into higher tolerance to the leakage and consequently to higher key rate. If the leakage modes are initially identical to the signal, the leakage is more detrimental to the security overall. Higher levels of squeezing do not necessarily improve the key rate and leakage tolerance. Squeezing optimization is required to improve the performance of the protocol.

For reverse reconciliation, the security break is observed already under an individual attack and in a purely lossy channel. Surprisingly, coherent state protocol can tolerate arbitrary amounts of leakage, though only in noiseless channel. On the other hand, security of squeezed-state protocol, with increase of modulation leakage, quickly becomes compromised without the need for an untrusted party to resort to any additional manipulations onto the trusted side. We show that squeezing, however, can be optimized in order to improve the tolerance for multimode modulation leakage and channel noise. The optimized squeezed-state protocol then overcomes the coherent-state protocol at any parameters.

The study of multimode modulation leakage is particularly important for multimode quantum sources eligible for use in CV QKD protocols [179, 181]. The results are stimulating for an experimental test of the macroscopically multimode protocols [180, 284].

6 Stabilization of transmittance fluctuations in a free space atmospheric link

This chapter outlines the main results of the published article where the transmittance fluctuations of the article that explores the applicability, and the extent of optimization of the squeezed-, and coherent-state Gaussian CV QKD protocols that involve propagation via free space atmospheric channels (see [3] or Chapter 8 for a copy of the article).

In this paper we focus on a 1.6 km free-space atmospheric channel where variations of attenuation are caused predominantly by beam wandering (see Sec. 3.2.2). We experimentally test the conjecture that beam wandering induced transmittance fluctuations can be stabilized by expanding the beam size. To confirm it, we measure transmittance in a real free-space atmospheric channel at different settings (in terms of aperture-to-beam size ratio $a/W = 0.25, 0.35, 0.39, 0.75$) of beam width. Beams with a wider spot area (*i.e.* lower a/W) cover the aperture more consistently, hence encounter attenuation fluctuations of lower magnitude, but simultaneously endure significantly higher attenuation, as bigger part of the signal beam is not captured by the aperture. We assess whether the trade-off between more stable channel at the cost of additional losses can be successfully used to enhance the performance of the coherent-state CV QKD protocol.

6.1 Model

We study the effect of the beam expansion method on the entanglement (in terms of logarithmic negativity) of a two-mode squeezed vacuum state, and on the security of the coherent-state CV QKD protocol with homodyne detection. The analysis of the latter assumes collective attacks, realistic post-processing $\beta < 1$, and is based on purification using an entanglement-based scheme.

During the experimental test, a grating stabilized continuous wave diode laser has been used to emit light at $809nm$. The width of the beam has been first adjusted with the sender telescope and then sent through a free-space channel of 1.6 km length to the receiver. The

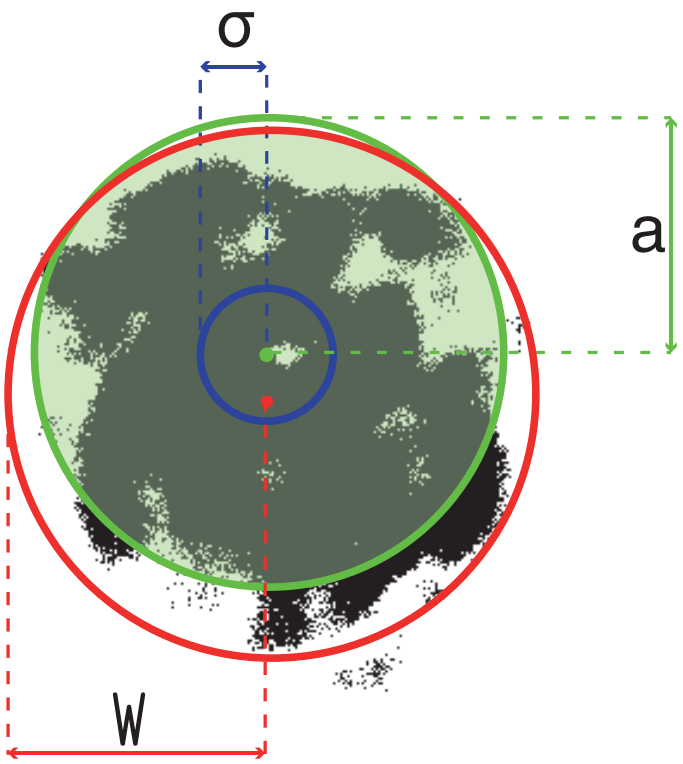


Figure 6.1: An example of analysis of a single frame from a CCD camera footage. Green circle represents the aperture area with radius a. The beam spot area is approximated by a circle with radius W. Blue circle shows the deviation of centers of all deflected beam spots captured by the CCD camera. Center of shown beam spot is within 1 standard deviation σ from the aperture center (green dot).

measurement of the incoming signal on the receiver side has been alternated between a PIN photodetector, which monitored the transmittance of the atmospheric channel, and CCD camera that recorded the beam width and fluctuations. The latter, although approximately, provides an assessment of the parameters of probability distribution that governs the beam-deflection distance fluctuations (σ^2 in Eq. 3.19). Estimated parameters are consequently used for the theoretical description of the channel transmittance fluctuations due to beam wandering.

Assuming center of the beam is normally distributed around the point at distance d from the aperture center with variance σ, variation of the beam-deflection distance r is determined according to Rice distribution $\mathcal{P}_{\text{Rice}}(d, \sigma)$. The distribution can be reduced to log-negative Weibull distribution provided the beam is properly aligned relative to the aperture center $d = 0$, which in terms of transmission coefficient T (the transmittance, or transmission efficiency is given by $\eta = T^2$) is described by Eq. (3.19). Weibull distribution is governed by the aperture size a, beam spot size W, and variance of the beam spot center σ^2. Further details regarding evaluation of the Weibull probability distribution are provided in Sec. 3.2.2.

The footage from CCD has been analyzed to acquire an estimate value of beam spot

variance σ^2, during each setting of a/W. An example of the frame analysis is presented in Fig. 6.1. To determine the beam spot size we initially discard pixels with low intensity in each image. A single intensity threshold used for all frames (and all a/W settings) is chosen empirically with the aim to maintain the normal distribution of the beam center, maximize the distinguishability of the beam spot, and to preserve the maximum amount of the data points. Chosen intensity threshold allowed to completely eliminate the cases when two distinct beam spots in a single frame were recorded. Due to limited camera field of view, for highly expanded beam setting, *i.e.* low a/W, when the beam spot covered the aperture entirely or almost entirely, the beam spot shape could not be assessed correctly and the beam spot center has been identified as in, or close vicinity to the center of the aperture. Uniform distribution of the intensity in the frame further confirms the reduction of the fluctuations and stabilization of the channel transmittance.

An improved quality of beam spot variance estimation can be achieved by extending the recording time of CCD camera. Furthermore, more precise estimation of the transmittance can be achieved by monitoring the deviation of mean beam spot center from the aperture center (to employ Rice distribution as in Eq. 3.18). For a more general treatment, one can also incorporate the effect of beam distortion, although the link used in the experiment does not exhibit strong enough turbulence for beam distortion to be impactful.

6.2 Main results

In Fig. 6.2 we present the dependency of the key rate on the ratio a/W between the receiving aperture $a = 150mm$ and the beam spot size W. The experimentally obtained values are represented by circles and squares, while theoretical predictions, based on log-negative Weibull distribution, are represented by solid and dashed lines. The latter illustrate the dependency for the protocol with optimized state variance, while experimental results for the same protocol are given by blue squares. We show that small beam expansion can indeed lead to the improvement of the secure key rate of the protocol with fixed modulation. Minor improvement of the key rate can also be observed for the protocol that employ optimized modulation. Further expansion of the beam spot, however, significantly reduces transmittance and consequently the key rate. This confirms the positive effect of the beam expansion in the fading channel on the CV QKD, though the beam spot size should be chosen based on given conditions. The method would certainly be more beneficial in an atmospheric channel that exhibits stronger turbulence, as predicted in Fig. 6.2 (bottom). The latter estimates the key rate under different values of beam-spot fluctuations variance σ_b^2. It is evident from the plot, that our method would allow to restore the security of the optimized protocol at stronger variance $\sigma_b^2 = 0.4$.

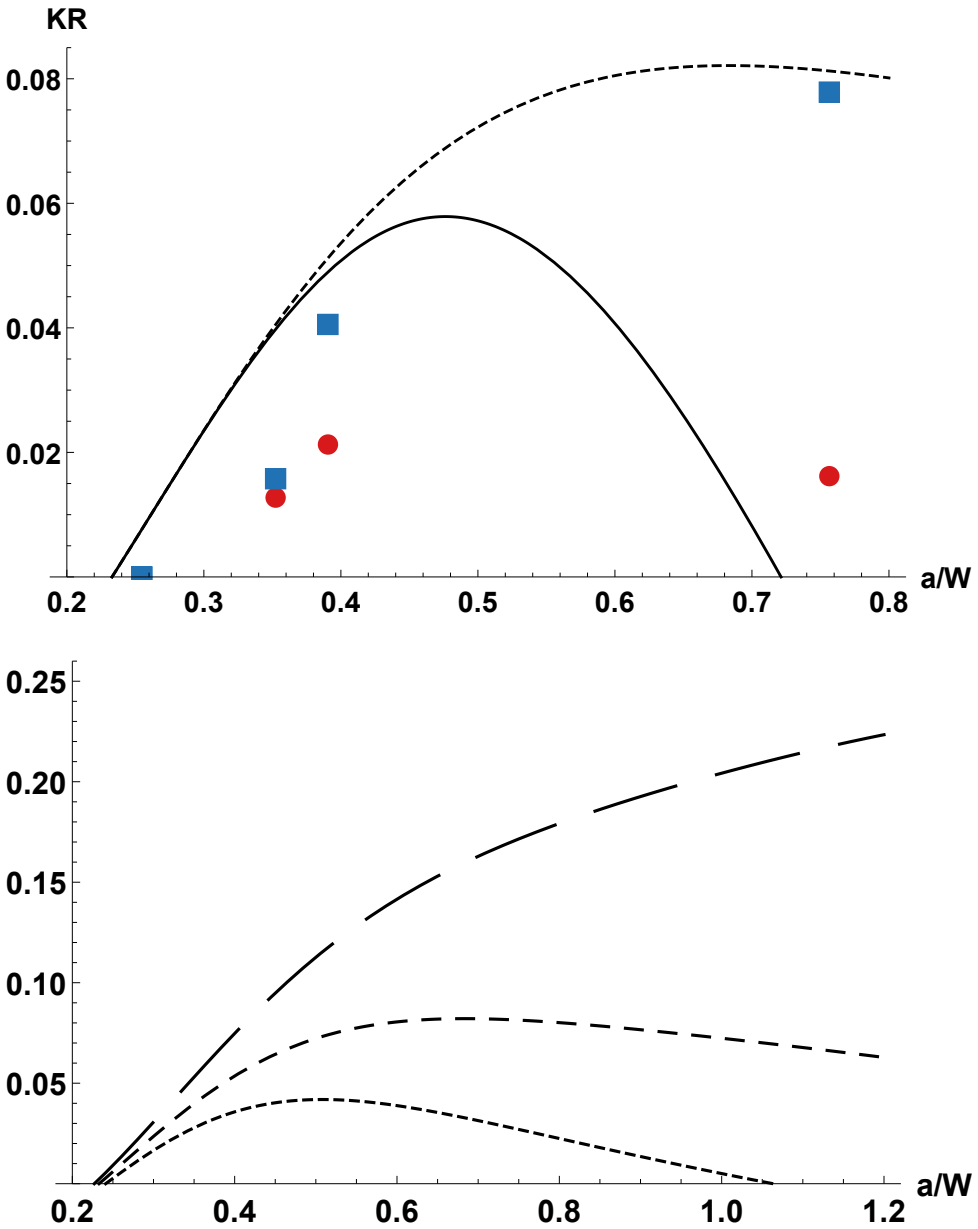


Figure 6.2: Lower bound on the key rate secure against collective attacks in the fading channel versus aperture-to-beam size ratio a/W:
(top) obtained from the analytical fading distribution (lines) along with the experimental results (points) versus aperture-to-beam size ratio, with state variance either 7 SNU (solid black line, red circles) or optimized (dashed black line, blue squares);
(bottom) obtained from the analytical fading distribution at $\sigma_b^2 = 0.2, 0.3, 0.4$ (from top to bottom) upon optimized modulation variance.
Both plots exhibit 1% SNU of channel excess noise, and 97% post-processing efficiency.

Summary

The study shows the viability of real fading channel stabilization by expanding the signal beam. The method allows to suppress the transmittance fluctuations at the cost of increased channel loss. Within the parameters of the studied real channel the such stabilization did not improve the nonclassical resource (entanglement), however it allowed to enhance the key rate of the coherent-state protocol (upon optimal beam expansion).

The suggested method can be successfully used in links exhibiting higher turbulence, although only up to some extent. Applicability greatly depends on the level of transmittance fluctuations in the channel. For channels with very high turbulence (and high loss) the fluctuations are small, and suggested stabilization method will not yield any positive improvements. On the other hand, beam expansion can be beneficial in mid-range terrestrial free-space links with relatively high fluctuations and average transmittance levels.

Importantly, the method is autonomous and does not require adaptive control of the source and detectors based on characterization of beam wandering. Furthermore, it can also be combined with other methods aimed at stabilization of the fluctuations of the free-space atmospheric channels.

7 | Improvement of CV QKD protocols in atmospheric links

This chapter summarizes the main results of the article that explores the applicability, and the extent of optimization of the squeezed-, and coherent-state Gaussian CV QKD protocols that involve propagation via free space atmospheric channels (see [4] or Chapter 8 for a copy of the article).

We start with the security analysis of the Gaussian squeezed-state CV QKD protocol employing homodyne detection (see Ch. 2.2) and established over an untrusted channel that exhibits transmittance fluctuations. Based on the obtained results we suggest an accessible and resource-friendly optimization method of the protocol, and further assert it's effectiveness for the realistic atmospheric turbulent channels simulated using a novel theoretical model.

7.1 Model

Although the generic squeezed-state protocol has already been studied in the fading channels [108, 285], to acquire a better understanding of the advantages of the non-classical carrier states, we require an entanglement-based model that allows trusted preparation side to independently control the available resources. Hence, we adopt the three-mode purification scheme (described in Chapter. 2.3.1) that employs three single-mode squeezers and a homodyne detection. Furthermore, we incorporate the effect of the fading channel according to the formalism described in Chapter 2.1.3. The channel is characterized by mean loss $\langle\eta\rangle$, strength of transmittance fluctuations (fading strength) $Var(\sqrt{\eta})$, and noise ε. We also consider generalized case of composite channel with additional losses $\eta_{1,2}$ and noise $\varepsilon_{1,2}$. The overall scheme is shown in Fig. 7.1.

The analysis is initially performed for the general channel with transmittance fluctuations to identify possible optimization techniques. Further, we asses the applicability of the optimization in realistic atmospheric links. The properties of the link are numerically simulated for various distances and turbulence strengths based on the novel theoretical elliptical-beam model of the transmittance probability distribution (see Sec. 3.2.2 for further details regarding the model).

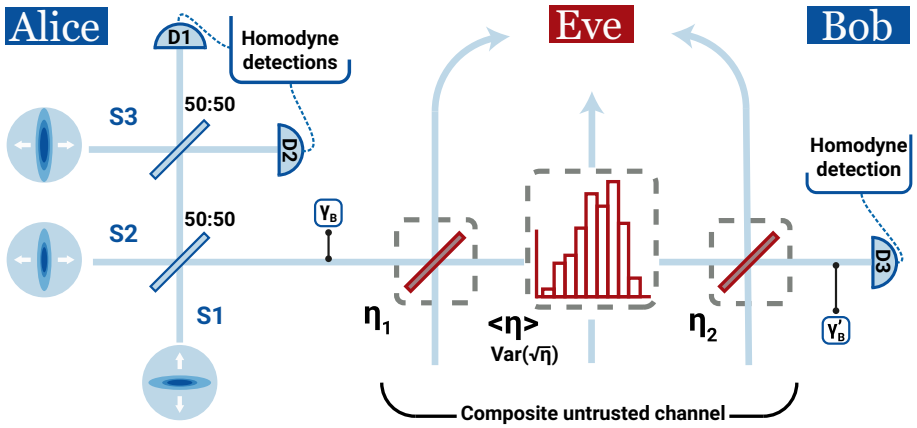


Figure 7.1: An entanglement-based CV QKD scheme used for the security analysis. On trusted preparation side the two oppositely squeezed modes S_1 and S_2 are coupled on a balanced beamsplitter. Alice performs homodyne measurements on the output ports (D1 and D2) of another balanced beamsplitter on which S_1 mode and squeezed vacuum mode S_3 have interacted. The signal is sent to Bob via composite untrusted channel that consists of two fiber channels with fixed losses (η_1 and η_2), and an atmospheric channel defined by the properties of transmittance probability distribution $\tau(\eta_j)$, namely by $\langle\eta\rangle$ and $\mathrm{Var}(\sqrt{\eta})$. Bob conducts homodyne measurement (D3), obtaining correlated string of data with Alice, and they proceed to key sifting, error correction, and privacy amplification.

7.2 Main results

To distinguish the effect of a fading channel on the security of the CV QKD protocols, we focus on RR and collective attacks, but assume perfect conditions, *i.e.* noiseless channel $\varepsilon = 0$, perfect post-processing $\beta = 1$, and absence of additional losses $\eta_{1,2} = 1$. We plot (Fig. 7.2) a dependency of the key rate on the squeezing V_S and modulation variance V_M for various values of transmittance fluctuations $Var(\sqrt{\eta})$ with mean channel losses $\langle\eta\rangle = 1/2$, corresponding to short range link. The color indicates the key rate, that starts from $R_{RR} \in (0, 0.1)$ (brightest colored area) and increases by 0.1 with each color shade, with the darkest shade representing $R_{RR} > 0.5$.

In the absence of transmittance fluctuations $Var(\sqrt{\eta}) = 0$, the addition of squeezing V_s is always advantageous for Alice and Bob, as it improves robustness to losses and excess noise in the channel, and consequently the key rate. Apparently, introduction of even small transmittance fluctuations to the channel immediately imposes limitations on applicable squeezing and modulation, *e.g.* using signal states with strong squeezing $V_s < 0.02$ is not compatible with a secure key distribution. As the fluctuations become stronger, the ranges of values, allowing to maintain the security of the protocol, continue to shrink. Optimization of squeezing and modulation is required to improve or, for certain channel parameters, restore the performance of the protocol. In realistic conditions of noisy channel $\varepsilon \neq 0$, limited post-processing efficiency $\beta < 1$, stronger mean losses $\langle\eta\rangle$ or composite channel $\eta_{1,2} < 1$ the need for squeezing and encoding alphabet size optimization is stressed yet further. Crucially, optimal performance can be reached by a feasible squeezing for a

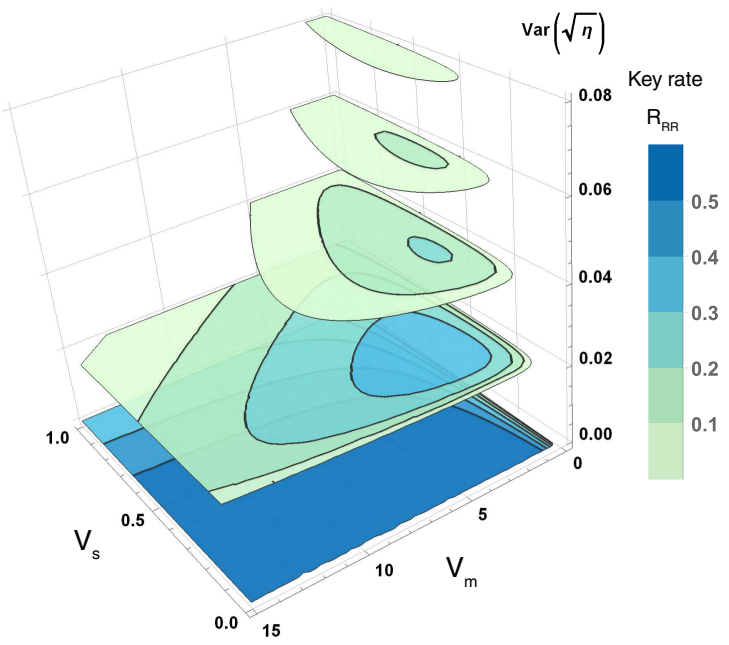


Figure 7.2: Positive key rate (in bits per channel use) for squeezing V_s, modulation variance V_m and fading strength $\mathrm{Var}(\sqrt{\eta})$, $\langle\eta\rangle = 1/2, \epsilon_{atm} = 0$. The key rate values range from $0 < R \leqslant 0.1$ (lightly shaded areas) to $R > 0.5$ (darkest shaded areas) with 0.1 step. In atmospheric channel with weak turbulence once can expect to observe $Var(\sqrt{\eta}) \leq 0.01$, while under strong turbulence at least $Var(\sqrt{\eta}) > 0.04$

nonvanishing $Var(\sqrt{\eta})$.

Optimization of the generic squeezed-state CV QKD protocol, where modulation and squeezing are mutually fixed (and security analysis is based on conventional entanglement-based scheme, (see Ch. 2.2) allows to reach highest key rate for given channel parameters just as well, as the scheme used in our analysis, where the squeezing and modulation can be optimized separately. However, our results can be directly translated to P&M schemes, used in practical implementations, and support more adaptable use of resource. In other words, our results show that one can achieve a key rate equivalent to the obtained using an entanglement-based scheme, but with less squeezing, compensating by applying modulation of higher variance.

An example of optimization advantages in realistic conditions is shown in Fig. 7.3, where the performance of the squeezed- (with feasible maximal squeezing values V_s^{max} =-3, and -10 dB) and the coherent-state protocols in a short atmospheric urban link are compared. The channel parameters have been simulated based on the monitoring data of structure constant of refractive index of air C_n^2, performed in another experiment [286]. The coherent-state protocol (triangles) can be successfully implemented only during suitable atmospheric conditions (around 5am and 5pm). The squeezed-state protocol with limited squeezing $V_s^{max} = -3dB$ and smaller block size can on average be used during the whole day with an exception of possible temporary signal loss around 10am. However, increasing the block size and/or maximal squeezing V_s^{max}, would have allowed to operate over such short atmospheric link continuously throughout the whole monitoring period.

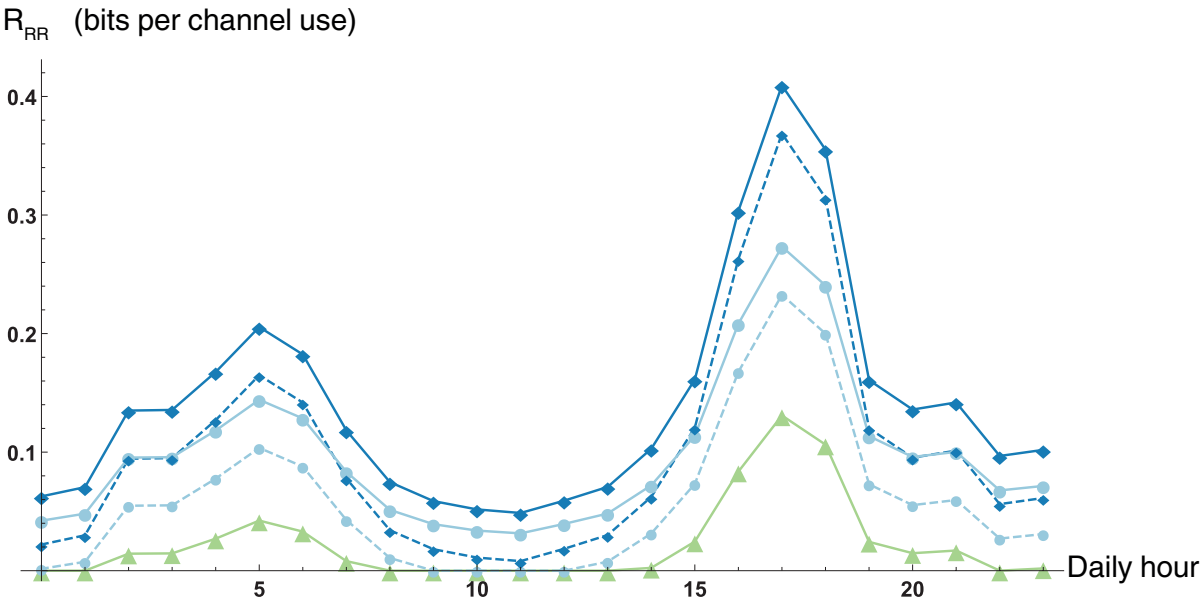


Figure 7.3: Optimized secure key rate of the coherent-state protocol (green triangles), and the squeezed-state protocol (blue circles, and blue squares) in 2.2 km long atmospheric channel. Each point on the plot was obtained for the transmittance distribution simulated using the averaged (over 4 months period) hourly statistics of structure constant of refractive index of air C_n^2. Finite-size effects are considered for block sizes of $n = 10^6$ (dashed lines) and $n = 10^{10}$ (solid lines). The squeezed-state protocol has been optimized over both modulation V_m and squeezing V_s, with the upper limit on the latter $V_s^{max} = -3dB$ (circles), $V_s^{max} = -10dB$ (squares). Excess noise $\epsilon_+ = 1\%$, efficiency $\beta = 95\%$, additional losses (imposed by the composite channel) $\eta_1\eta_2 = -2.2dB$.

The squeezing is also more advantageous in better atmospheric conditions, which is illustrated by the fact that for the protocol, that has higher values of attainable squeezing $V_s^{max} = -10dB$, the difference between global maxima and minima is greater than for any other protocol.

Our research also considers short -distance links exhibiting excess noise (Ch. 3.1.4) in atmospheric channels with different lengths and turbulence strengths. We confirm that both the coherent-, and the squeezed state protocols can be established over short atmospheric links, even in presence of substantial excess noise and untrusted losses. Anti-squeezing noise have been shown to improve the key rate, provided the fading strength $Var(\sqrt{\eta})$ is low, *i.e.* for short communication distances, but can contribute to the eavesdropper at longer distances, or under stronger transmittance fluctuations. The use of feasible levels of squeezing always enhances the performance of the protocol, and supports distribution on longer distances in noisier channels comparing to the coherent-state protocol. While modulation optimization is sensible for all channel conditions, squeezing optimization becomes relevant only at longer distances or stronger turbulence.

Summary

We have analyzed the effect of transmittance fluctuations on the squeezed- and the coherent-state protocols, and have shown that such fluctuations limit maximal applicable values of squeezing and modulation variance. Based on the analysis, we discover an accessible and resource-friendly optimization method. We confirm the viability of the optimization, and show the performance improvement in terms of secure key rate increase, reduction of the downtime of the protocol, and expanding the range of atmospheric conditions, communication distances, and levels of additional losses and noise suitable for generating secure key.

Importantly, the optimization is compatible with other methods for improvement of CV QKD performance in free space, such as beam-tracking [223], adaptive optics [222], post-selection [108, 186, 287], channel multiplexing [195, 198, 288], etc. Next step towards this free-space novel quantum key distribution technique is an experimental verification of the functionality of the free-space squeezed-state protocol which will stimulate further theoretical and experimental developments and practical implementations.

8 | 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.

Preventing side-channel effects in continuous-variable quantum key distribution

Ivan Derkach, Vladyslav C. Usenko, and Radim Filip
Published: *Physical review A* Vol. 93, Issue 24, 032309 (2016)
Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic

Following is an exact copy of the published article.

Preventing side-channel effects in continuous-variable quantum key distribution

Ivan Derkach,* Vladyslav C. Usenko,† and Radim Filip‡
Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic
(Received 1 December 2015; revised manuscript received 11 February 2016; published 8 March 2016)

The role of the side channels in the continuous-variable quantum key distribution is studied. It is shown how the information leakage through a side channel from the trusted sender station increases the vulnerability of the protocols to the eavesdropping in the main quantum communication channel. Moreover, the untrusted noise infusion by an eavesdropper on the trusted receiving side breaks the security even for a purely attenuating main quantum channel. As a method to compensate for the effect of the side-channel leakage on the sender side, we suggest several types of manipulations on the side-channel input. It is shown that by applying the modulated coherent light on the input of the side channel that is optimally correlated to the modulation on the main signal and optionally introducing additional squeezing in the case of the squeezed-state protocol, the negative influence of the lossy side channel on the sender side can be completely removed. For the trusted receiving side, the method of optimal monitoring of the residual noise from the side-channel noise infusion is suggested and shown to be able to completely eliminate the presence of the noisy side channel. We therefore prove that the side-channel effects can be completely removed using feasible operations if the trusted parties access the respective parts of the side channels.

DOI: 10.1103/PhysRevA.93.032309

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a major communication application of quantum information theory aiming at the development of protocols for establishing secure channels protected by the laws of quantum physics. Such channels can then be used to share a secure key for classical symmetrical cryptographic systems. Recently, continuous-variable (CV) [3] protocols of QKD (see [4] for review) were developed and implemented on the basis of squeezed [5–7] or coherent [8–12] states. The security of CV QKD protocols in the case of Gaussian modulation was then shown against collective attacks in the presence of channel noise [13,14], which also implies the security against the most general coherent attacks [15,16].

Continuous-variable QKD protocols, however, suffer from various imperfections. The most threatening are the untrusted (i.e., being under full control of a potential eavesdropper) quantum channels, which are inclined to losses due to the attenuation and can add excess noise in the link. Such noise can also be detection noise indistinguishable from the effect of the channel. In security analysis it is then supposed that all the channel imperfections are due to the presence on an eavesdropper. It was an important step in the development of CV QKD when with the use of reverse reconciliation it was shown possible to establish asymptotically secure key transmission upon any pure channel loss [9], while noise remains limiting to the security of the protocols.

However, the insecure quantum channel is not necessarily the single source of information leakage from a QKD protocol. A potential eavesdropper can use imperfections of the trusted (i.e., fully controlled by the trusted parties) devices such as sources and detectors to gain at least partial information on the signal being sent or to control the measurement being performed at the receiver station. The noise, which is present on the trusted sides, can be fully controlled and calibrated by the trusted parties. Such noise, however, can still be harmful. It was shown in particular that the preparation noise can already break the security in the reverse reconciliation protocol [17], but can be suppressed [18] or tolerated in the direct reconciliation scheme [19,20]. Also, the trusted detection noise limits the key rate, but can be partially helpful to make the protocol more robust against noise in the quantum channel [21,22].

In the less optimistic scenario the noise or loss on the trusted sides can however be under partial control of an eavesdropper, as depicted in Fig. 1(a). This is the case of the side channels, which we define as auxiliary channels that have either input or output controlled by a trusted party but output or input, respectively, controlled by an eavesdropper. From this point of view, the side channels differ from the main channel between the sender and receiver. Supposedly, any additional information can be used by an attacker to increase the knowledge about the transmitted key. Therefore, it is necessary to investigate the influence the side channels can have on security. In the following study we summarize all possible sources of side information and define them together as the side channels on either the sender or the receiver side of the protocol.

One possible way to overcome the negative influence of the side channels is implementing the so-called measurement-device-independent (MDI) QKD protocols [23], which were recently suggested on the basis of CVs [24,25], where the trusted detection stations become shielded from a potential eavesdropper. However, the applicability of the device-independent CV QKD protocols is still very limited, particularly in terms of distance.

In the present paper we study the effect of the side channels in CV QKD protocols with coherent and squeezed states of light. We define the side channels as the imperfections (signal loss and noise) on the trusted sides, which are under partial control of an eavesdropper. In particular, we consider (A) the leakage from the trusted sender station and (B) measurement

*ivan.derkach01@upol.cz
†usenko@optics.upol.cz
‡filip@optics.upol.cz

manipulation by the noise addition in the trusted receiver station. We show the degradation of the key rate and increase of vulnerability to the channel noise in the presence of a side-channel leakage. We also show a security break from the noisy side channel on the detection stage. We suggest methods to compensate for the negative influence of the described side channels. For (A) we consider the possibility to classically apply an additional correlated signal on the side-channel input, which is under control of a trusted sender party. We show the positive effect of such additional modulation and the possibility to optimize the modulation variance for the given parameters of the protocol. Moreover, we show that by applying correlated information encoding and squeezing the input of the side channel, in the case of the squeezed-state protocol, the trusted party is able to completely decouple the side channel from the signal. By decoupling here we mean decorrelation (reducing or turning the correlation to zero) and stopping the leakage of information through the side channel, which completely removes the negative impact of the side channel. For (B) we show the possibility to cancel the infused detection noise by monitoring the output of such a noise-infusing side channel. These are the alternative ways of active compensation of the side channels in the Gaussian CV QKD protocols with the trusted sender and receiver stations, which keep the advantage of usability of such protocols, including the longer channel distances, compared to the device-independent protocols [23–25], and do not involve entanglement or non-Gaussian operations and measurements. If for any reason the input of the sender-side leakage or the output of the receiver-side noise infusion are not available for the manipulations or monitoring, respectively, then the negative impact of the side channels shown in the current paper has to be either taken into account in the security analysis or compensated for by the possible use of the MDI schemes.

The paper is structured as follows. In Sec. II we define the side channels and recapitulate the methods of CV QKD security analysis being used. In Sec. III we demonstrate the negative impact of the side channels on the CV QKD security. In Sec. IV we introduce the methods aimed at compensating for the negative effect of the side channels. We summarize in Sec. V.

II. TYPES OF SIDE CHANNELS

We study the effect of the side channels on the standard and optimized CV QKD protocols [7,26,27] on the basis of the Gaussian modulation of squeezed and coherent states, as depicted in Fig. 1(a). The trusted sending side (Alice) prepares the signal state (squeezed or coherent) with variance V_S (so that $V_S < 1$ or $V_S = 1$, respectively) using the source S. Alice then applies random Gaussian quadrature displacement of variance V_M (also referred to as the modulation variance), so that the overall variance of the modulated states becomes V, using the modulator M. The prepared state travels through the untrusted channel parametrized by transmittance (loss) η and excess noise ϵ both being under *full* control of an eavesdropper (Eve). The signal is then detected by the remote receiving party (Bob) using the homodyne detector H. Further, with no loss of generality, we assume that the quadrature x is measured by Bob. Thus, in the standard Gaussian CV QKD protocol (without the side channels) Alice applies displacement x_M

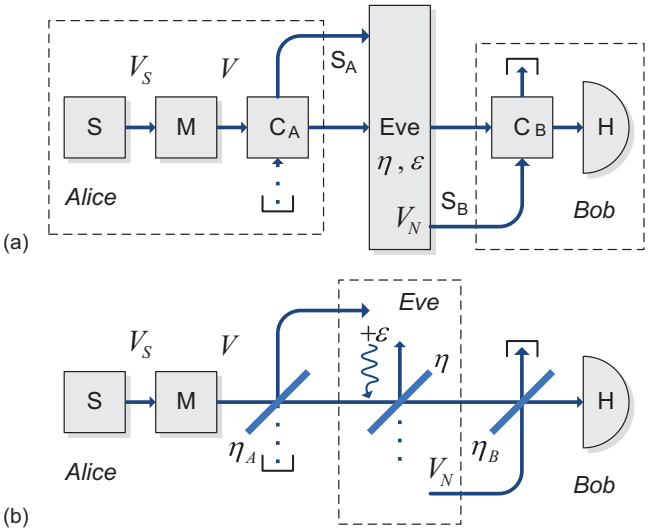


FIG. 1. (a) Scheme of the CV QKD based on signal state preparation in the source S and Gaussian quadrature displacement applied in the modulator M. The untrusted channel is parametrized by transmittance η and excess noise ϵ. The signal is coupled to the lossy side channel S_A with untrusted output on the sender side and to the noisy side channel S_B with untrusted input of variance V_N on the receiving side. The remote trusted party performs measurement with the homodyne detector H. The trusted devices and channels are within the dashed boxes. (b) Scheme of the CV QKD with sender-side leakage modeled as coupling of the signal to a vacuum mode on a beam splitter with transmittance η_A. The receiver-side untrusted noise infusion is modeled as coupling to a noisy mode with variance V_N on a beam splitter with transmittance η_B. The untrusted channels are within the dashed box.

to the signal quadrature x_S and sends the state with the quadrature $x_A = x_S + x_M$ to the channel so that the variances are $\mathrm{Var}(x_A) = V$, $\mathrm{Var}(x_S) = V_S$, and $\mathrm{Var}(x_M) = V_M$ and then $V_S + V_M = V$. In the standard Gaussian CV QKD squeezed-state protocol [26] the signal states are modulated up to the antisqueezing (variance of the quadrature complementary to a squeezed one), so $V_M = 1/V_S - V_S$ holds, i.e., the variance of modulation is fixed by squeezing of the signal states. We will also consider the optimized Gaussian CV QKD protocols [7,27], where modulation V_M is independent of the variance of the signal states and can be freely optimized for a given signal resource and parameters of the setup. The quantum channel transforms the modulated signal such that Bob measures the quadrature $x_B = (x_A + x_N)\sqrt{\eta} + x_0\sqrt{1-\eta}$, where x_0 is the quadrature of the vacuum input of the channel loss and x_N is the quadrature of the channel excess noise with the variances $\mathrm{Var}(x_0) = 1$ and $\mathrm{Var}(x_N) = \epsilon$.

Note that the trusted parties must know the channel parameters to assess the security of the protocols and therefore the channel must be properly estimated. While the issue of the channel estimation was recently studied in the finite-size context [28], in the present paper we focus on the side-channel effects and assume that the channel parameters are already known to the trusted parties. The channel estimation is still possible in the presence of the side channels because the side-channel parameters (losses and noise) can be estimated

independently by the local measurements on the trusted sides. This also allows us to consider the protocols based on the preparation and measurement of a single quadrature (e.g., x), while the channel estimation would require additional modulation and measurement in the complementary one. Moreover, since the methods of the side-channel compensation suggested below do not change the data ensemble size (defined by the signaling and detection rate), the finite-size effects [28,29] would not qualitatively change the results of the paper.

Two types of side channels are considered in our study as shown in Fig. 1(a). The first one (further also referred to as the type-A side channel) is the sender-side side-channel leakage, when a vacuum mode is coupled to the signal and only the output of the coupling C_A is accessible by an eavesdropper. An eavesdropper Eve has no control of the side-channel input and of the strength of the coupling, thus the input state of such a side channel is initially vacuum. Eve however receives the side-channel output similarly to noninvasive passive attacks in classical cryptography [30]. The sender (Alice), on the contrary, has full control of the input of such a side channel before the coupling C_A. The second type of side channel (further also referred to as the type-B side channel) is untrusted noise addition in the receiver station. In this case an untrusted noise with variance V_N is supposedly prepared by Eve and coupled to the signal prior to detection with the output of the coupling being inaccessible to the eavesdropper. The eavesdropper is not able to change the coupling strength. On the contrary, the receiving side (Bob) is able to control (e.g., measure) the output of the coupling C_B. In both the cases we assume that the trusted parties are not able to directly remove the side channels or change the coupling strengths (C_A and C_B, respectively).

These are the two main types of possible semitrusted side channels, while the completely trusted noise is covered by previous research [17,18,21,22] and completely untrusted noise can be attributed to the channel. Moreover, the noise infusion on the sender side (symmetrical to the type-B side channel on the receiver side that is considered in the present paper) is equivalent to the additional noise in the untrusted channel. At the same time the side-channel loss on the receiver side (symmetrical to the type-A side-channel loss on the sender side that is also considered here) is equivalent to the additional loss in the untrusted channel. Thus, our analysis covers the main possible semitrusted side channels based on the two-mode interaction in the prepare-and-measure CV QKD.

We do not consider any specific physical realization of the side channels applying our analysis to the general case of semitrusted side channels based on the linear-optical mode interaction. However, the side channels can be expected in any real implementation of CV QKD in either fiber [7,11] or free-space channels [31,32], where coherent and squeezed states were successfully transferred. The sender-side leakage can take place in particular in the case of imperfect modulation, e.g., when the signal is mixed with a temporal, spectral, polarization, or spatial mode, which then leaves the sender station. The receiver-side noise infusion may, e.g., be caused by imperfect light collection from a free-space channel with a background radiation.

Linear optical crosstalk is well studied in the classical optical communications where it is present in the multiplexed channels and receivers [33], but was also reported in the quantum communications [34]. Linear coupling represented by the beam-splitter transformation is generally used to model the interaction of a quantum-optical system with the environment [35]. Therefore, in our work we use the typical linear optical interaction and model the mode coupling between the signal and the side channels as the beam splitters [see Fig. 1(b)]. The type-A side channel is modeled as coupling to a vacuum mode on a beam splitter with transmittance η_A. On the other side we model the type-B side channel as coupling to a thermal noise mode with variance V_N on a beam splitter with transmittance η_B. In the case of the sender-side leakage (type-A) side channel the quadrature that enters the quantum channel is then changed to $x'_A = x_A\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A}$, where x_{SCA} is the quadrature value of the vacuum state on the input of the beam splitter $\mathrm{Var}(x_{SCA}) = 1$. In the case of the noise-infusing (type-B) side channel the output of the quantum channel is changed as $x'_B = x_B\sqrt{\eta_B} + x_{SCB}\sqrt{1-\eta_B}$, where x_{SCB} is the input noise of the type-B side channel with $\mathrm{Var}(x_{SCB}) = V_N$.

In the analysis of the negative impact of the side channels on CV QKD and the methods to compensate for such impact we mainly study the security against collective attacks, which in the asymptotic limit were shown to be no less effective than the most general coherent attacks [36]. In this case Eve performs the optimal collective measurement on the accessible modes after the process of bases reconciliation is completed, implying that Eve attaches a separate uncorrelated probe to each transmitted state and keeps probes in a quantum memory until she can gather additional information. To obtain simple insight into the conditions for insecurity of the protocols we also study the security against individual attacks, in which case Eve is limited by the individual measurement on the accessible modes. This weaker security analysis allows us to analytically derive the regions of insecurity of the protocols in the presence of side channels since insecurity against individual attacks implies insecurity against the more effective collective attacks.

Following the generalization of the Cziszár-Körner theorem [37] on the quantum measurements performed by Devetak and Winter [38], the protocol is secure if the mutual information between the trusted parties exceeds the information available to Eve on the data on the trusted receiver side (which is the case of reverse reconciliation, which is more stable against channel loss [9]). The security is then described by the positivity of the lower bound on the key rate, which in the case of collective attacks reads

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

where $\beta \in (0,1)$ is the postprocessing efficiency and χ_{BE} is Holevo bound that determines Eve's achievable information limit in the case of collective attacks [13,14]. The efficiency β depends on the effectiveness of the data postprocessing algorithms that are being used in the secure key distillation given the particularly low signal-to-noise ratio. We set β as an independent parameter and do not consider any particular post-processing algorithm. In the following analysis we therefore fix the reconciliation efficiency as $\beta = 0.95$, which is realistic taking into account the recent progress in the error-correcting algorithms for the Gaussian-distributed data [39].

The Holevo bound can be expressed as $\chi_{BE} = S(\gamma_E) - S(\gamma_{E|B})$ through the von Neumann entropy $S(\gamma_E)$ of the generally multimode state (including the side channels), which is available to Eve for the collective measurement described by the respective covariance matrix γ_E, and the von Neumann entropy $S(\gamma_{E|B})$ of the state available to Eve conditioned on the measurement results of the remote trusted party Bob [40] and described by the covariance matrix $\gamma_{E|B}$. Covariance matrices are the matrices of the second moments of quadratures of the form $\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$, where $r_i = (x_i, p_i)^T$ is the quadrature vector of an ith mode. Along with the first moments, the covariance matrices explicitly describe the Gaussian states and are sufficient for the security analysis of the Gaussian protocols [13,14] due to the extremality of the Gaussian states [41]. We analyze the security against the collective attacks using the most general purification method [40], where the equivalent entanglement-based representation of the protocols is used and all the state imperfections corresponding to the side channels and the main channel are attributed to Eve.

In the case of individual attacks the upper bound on the information available to an eavesdropper is given by the Shannon mutual information I_{BE} instead of the Holevo bound and the lower bound on the key rate (in the optimistic case of perfect postprocessing efficiency) reads $K_{ind} = I_{AB} - I_{BE}$. Details of calculations for security analysis in the cases of both individual and collective attacks are given in the Appendix, while here we present the main expressions and results. In the next section we study the negative impact of the side channels on CV QKD.

III. NEGATIVE EFFECT OF SIDE CHANNELS

A. Side-channel loss on the trusted sender side

Let us first consider the type-A side channel. We start by analyzing the region of insecurity of the protocol with respect to the individual attacks and without the untrusted channel noise. The mutual information in this case reads (see the Appendix for details)

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta_A \eta V_M}{\eta_A \eta (V-1)+1}}, \tag{2}$$

while the information available to Eve reads

$$I_{BE} = \frac{1}{2}\log_2 \frac{[\eta_A \eta (V-1)+1][V - \eta_A \eta (V-1)]}{V} \tag{3}$$

and is independent of the signal states (squeezed or coherent). As can be seen, the side channel decreases the mutual information between the trusted parties and increases Eve's information, therefore limiting the key rate already for individual attacks with pure channel losses.

In the optimal (given perfect postprocessing $\beta = 1$) limit of infinite squeezing and modulation ($V \to \infty$) upon pure channel loss ($\epsilon = 0$) the key rate for the standard Gaussian CV QKD protocol can be written as

$$K_{V\to\infty} = \lambda \log_2 \frac{1}{1 - \eta_A \eta}, \tag{4}$$

where $\lambda = 1$ for the squeezed-state protocol and $\lambda = 1/2$ for the coherent-state one. The channel transmittance η is therefore effectively decreased by the side-channel coupling η_A. Thus the presence of the type-A side channel does not break the security, i.e., the key rate remains positive for any nonzero value of η_A, as one would expect, because the channel remains purely lossy.

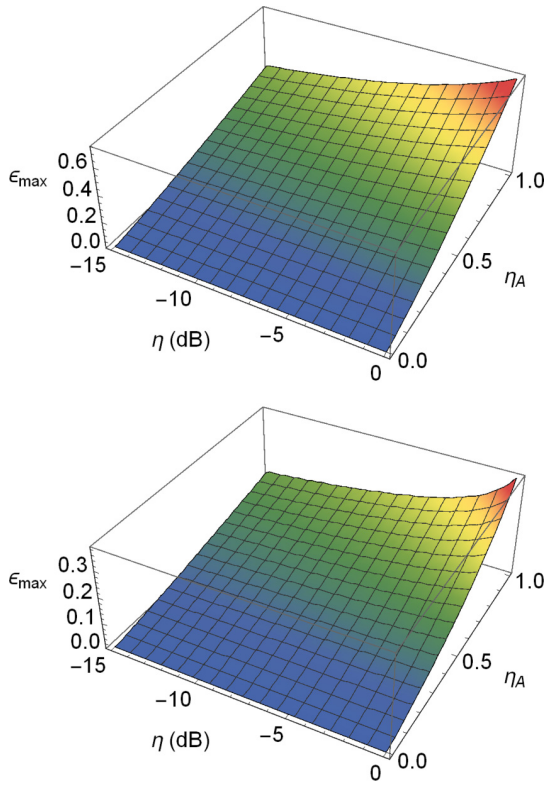


FIG. 2. Maximum tolerable excess noise dependence on the channel losses (on a dB scale) and the type-A side-channel coupling ratio η_A for the standard squeezed-state (top) and coherent-state (bottom) protocols. Here $\beta = 1$ and $V = 10^3$.

If the channel noise is present, then the side-channel loss increases the sensitivity of the protocol to the channel noise already in the case of the individual attacks. In the limit of strong modulation $V \to \infty$ and strong channel loss $\eta \ll 1$, the maximum tolerable channel noise is $\epsilon_{\max} = \eta_A/2$ for the standard coherent-state protocol and $\epsilon_{\max} = \eta_A$ for the standard squeezed-state protocol with arbitrarily strong squeezing.

In the case of collective attacks (see the Appendix for details) the side-channel leakage on the trusted sender side also lowers the key rate and substantially reduces the tolerance to the channel excess noise, which is clearly visible in Fig. 2, where the maximum tolerable channel excess noise $\epsilon_{\max}$ (in shot-noise units, which are the variance of vacuum fluctuations) is plotted versus channel transmittance and side-channel loss for the standard CV QKD protocols with strong modulation.

B. Noise infusion on the trusted receiver side

The performance of the protocols is different in the case of the type-B side channel. In this case the presence of additional noise V_N coupled to a signal can lead to the security break already for the purely attenuating channel (i.e., when $\epsilon = 0$). The mutual information between the trusted parties in this case

is reduced by the noise V_N and reads

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta\eta_B V_M}{\eta_B(\eta V + 1 - \eta) + (1-\eta_B)V_N}}. \quad (5)$$

The security break can be observed already in the case of individual attacks upon pure channel loss. Eve's upper bound on the leaking information depends only on the overall variance V and reads

$$I_{BE} = \frac{1}{2}\log_2 \frac{\eta_B(\eta V + 1 - \eta) + (1-\eta_B)V_N}{\frac{\eta_B V}{\eta + (1-\eta)V} + \frac{1-\eta_B}{V_N}}. \quad (6)$$

In the limit of strong modulation $V \to \infty$ and strong channel loss $\eta \ll 1$ the bound on the side-channel noise for either the squeezed- or coherent-state standard CV QKD protocol reads

$$V_N^{\max}\big|_{\eta \ll 1}^{V \to \infty} = \frac{1}{1 - \eta_B}. \quad (7)$$

In the more general case of collective attacks the side-channel noise V_N not only undermines the tolerance of the protocol to the channel noise ϵ, but also leads to the security break contrary to the type-A side-channel leakage. This can be seen from the profiles of the maximum tolerable channel noise in the case of $V_N = 1.05$, i.e., when the input of the type-B side channel only slightly exceeds the shot-noise variance as shown in Fig. 3. Note that the squeezed-state protocol appears to be more stable against the side-channel noise infusion (its security region is larger in terms of the tolerable channel loss and side-channel coupling at the given V_N). Thus, the presence of the side-channel leakage or noise infusion makes the protocol more sensitive to the channel noise and can even break the security for the purely attenuating channel. In the next section we suggest the methods to compensate for negative effects by manipulations at the trusted sides and without affecting the untrusted quantum channel.

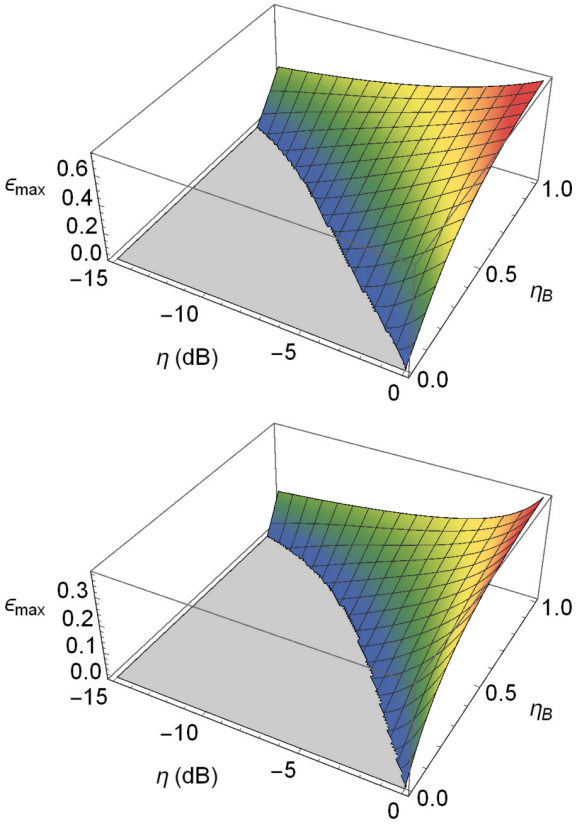


FIG. 3. Maximum tolerable excess noise dependence on the channel losses (on a dB scale) and the type-B side-channel coupling ratio η_B for the standard squeezed-state (top) and coherent-state (bottom) protocols. Here $\beta = 1$, $V = 10^3$, and the side-channel noise variance $V_N = 1.05$.

IV. DECOUPLING OF SIDE CHANNELS

A. Side-channel loss on the trusted sender side

We suggest that the trusted sender (Alice) should look for the input of the type-A side channel in the case it cannot be removed completely and then apply state manipulation on the side-channel input [see Fig. 4(a)]. Three options can be considered depending on the accessibility of the side channel and technical ability of Alice.

First, Alice can infuse Gaussian thermal noise to the side channel by replacing the vacuum input of the side channel with

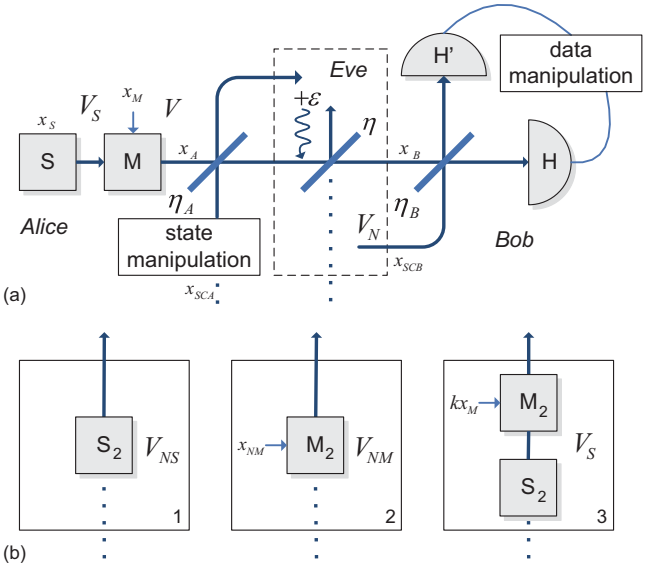


FIG. 4. (a) Methods aimed at compensating for the negative impact of the side channels: state manipulation on the input of the type-A sender-side lossy side channel and monitoring of the output of the type-B receiver-side noise-infusing side channel using the monitoring homodyne detector H′ and subsequent data manipulation involving also the measurement results from the main homodyne detector H. (b) Types of state manipulation on the input of the type-A side channel: 1 (left), noise infusion using the source S_2 producing a thermal state with variance V_{NS}; 2 (middle), controllable uncorrelated modulation on the side-channel input using the modulator M_2; and 3 (right), controllable correlated modulation with displacement kx_M proportional to the modulation of the main signal using the modulator M_2. In the case of the squeezed-state protocol to achieve complete decoupling of the side channel the side-channel input should be replaced by the squeezed state with variances V_S and $1/V_S$ using the source S_2 prior to the modulator M_2. In the case of the coherent-state protocol such preparation is not needed and the source S_2 needs not to be used.

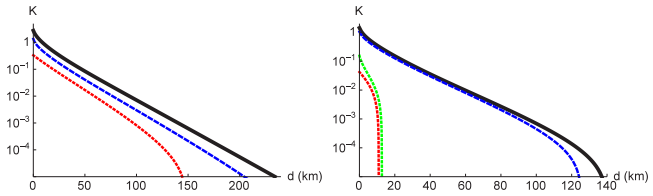


FIG. 5. Key rate secure against collective attacks versus distance in a standard telecom fiber (with an attenuation of -0.2 dB/km) for the squeezed-state protocol with $V_S = 0.1$ (left) and the coherent-state protocol (right) in the presence of the type-A side channel $\eta_A = 0.4$ and no compensating methods (red dotted lines), with optimized unknown noise on the input of the channel (green upper dotted line for the coherent-state protocol), with optimized uncorrelated modulation on the input of the side channel (blue dashed lines), with optimized correlated modulation on the input of the side channel and no additional source S_2 (coincides with the blue dashed line for the squeezed-state protocol), and in the perfect case in the absence of the side channel, i.e., $\eta_A = 1$ (solid black lines). The latter curve overlaps with the ones for the optimized correlated modulation for the coherent-state protocol, for the optimized correlated modulation and squeezing of the side-channel input, and for the optimized uncorrelated modulation and squeezing on the input of the side channel for the squeezed-state protocol. Here $\beta = 0.95, \epsilon = 5\%$, and the modulation variance V_M is optimized for the given parameters.

the source of noise with variance V_{NS} [see Fig. 4(b), left]. The efficiency of such method is however very limited. Indeed, such noise reduces the mutual information

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta_A \eta V_M}{\eta[\eta_A V + (1-\eta_A)V_{NS}]+1-\eta}}. \tag{8}$$

However, it also, to some extent, decreases the Holevo quantity due to a partial decoupling of the side channel from the main channel, but at the same time acts as a preparation noise [18]. Thus, the addition of such unknown noise is of limited helpfulness, when the main channel has low loss, i.e., is short distance. Moreover, for the squeezed-state protocol, where the Holevo bound is effectively minimized by squeezing, the reduction of the mutual information due to the presence of additional noise appears to be more harmful, so mostly the unknown noise on the input of the side channel has either no or a very limited positive effect. This can be seen from the graphs in Fig. 5, where the key rate is plotted versus distance $d = -50\log_{10}\eta$ in a standard telecom fiber with attenuation of -0.2 dB/km (here and in the following we plot the key rate in bits per measurement). The improvement for the coherent-state protocol is small but visible [upper (green) dotted line compared to the lower (red) dotted one], while the improvement for the squeezed-state protocol is negligible (the corresponding curve overlaps with the one with no manipulation on the side-channel input performed, given as the dotted red line).

Second, Alice can use the additional modulator M_2 on her side to control the input of the side channel. Alice's modulation therefore shifts the quadrature of the side-channel input x_{SCA}. Let us assume that the additional modulation (displacement) on the input of the type-A side channel is independent from the main modulation performed on the signal, but is known to Alice and contributes to her data and to the correlation with Bob [see Fig. 4(b), center]. We can write the change of the input of the lossy side channel in terms of the x quadrature (calculations for the case when the p quadrature is modulated and measured will be equivalent) as $\tilde{x}_{SCA} = x_{SCA} + x_{NM}$, where x_{NM} is the shift, known to Alice, with variance $\mathrm{Var}(x_{NM}) = V_{NM}$.

The mutual information between the trusted parties in this case is increased:

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta(\sqrt{\eta_A}V_M + \sqrt{1-\eta_A}V_{NM})^2}{(V_M+V_{NM})\{\eta[\eta_A(V-V_{NM})-\eta_A+\epsilon]+1\}}} \tag{9}$$

due to increased correlations between the trusted parties. However, it simultaneously decorrelates (reduces the correlation with the main signal mode) the output of the side channel and increases the information leakage from the main channel. Therefore, such additional uncorrelated modulation on the input of the side channel V_{NM} can play a positive role mainly when the side channel is strong enough (typically $\eta_A < 0.8$) because otherwise the information leakage from the main channel prevails over the positive role of decoupling. Moreover, the modulation variance V_{NM} must be optimized for the given setup parameters. However, such a method can significantly increase the secure distance of the protocol especially for the coherent-state protocol, as can be seen from Fig. 5, where the corresponding key rate is given as the blue dashed lines.

Third, we suggest the method of correlated modulation on the input of the side channel and optionally additional squeezing of the side-channel input in the case of the squeezed-state protocol. Importantly, the method uses only the classical correlation of the Gaussian quantum states; no entanglement is required. The method as we show below allows (i) complete decoupling of the modulation from the side channel (no fraction of the modulation data appears on the side-channel output) and (ii) complete decorrelation of the side-channel output from the signal mode. These effects allow one to restore the performance of the protocol and thus completely remove the negative influence of the type-A side channel.

Indeed, Alice can apply the weighted correlated displacement on the input of the side channel [see Fig. 4(b), right] with the factor k so that the input of the side channel becomes $\tilde{x}_{SCA} = x_{SCA} + kx_M$. After the coupling between the signal and the modulated side-channel input the quadratures are $x'_A = x_S\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A} + x_M(\sqrt{\eta_A} + k\sqrt{1-\eta_A})$ and $\tilde{x}'_{SCA} = x_{SCA}\sqrt{\eta_A} - x_S\sqrt{1-\eta_A} + x_M(k\sqrt{\eta_A} - \sqrt{1-\eta_A})$. It is easy to see that when $k = \sqrt{(1-\eta_A)/\eta_A} \equiv k_{\mathrm{opt}}$ the outputs of the side-channel coupling become $x'_A = x_S\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A} + x_M/\sqrt{\eta_A}$ and $\tilde{x}'_{SCA} = x_{SCA}\sqrt{\eta_A} - x_S\sqrt{1-\eta_A}$. Therefore, due to the destructive interference effect, the untrusted output of the side channel contains no information on the signal displacement x_M, i.e., the side channel is completely decoupled from the modulation. Then, in the case of the coherent-state protocol, since $\mathrm{Var}(x_{SCA}) = V_S = 1$ the correlation between the outputs of the side channel in the regime of optimal correlated modulation with k_{opt} vanishes, i.e., $\mathrm{Cov}(x'_A, \tilde{x}'_{SCA}) = 0$, and the output of the side channel, containing already no encoded information, becomes in addition completely decorrelated from the signal mode. The eavesdropper therefore cannot

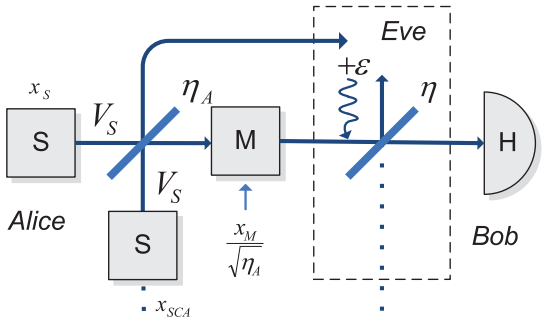


FIG. 6. Equivalent scheme of the method [depicted in Fig. 4(b), right] in the case of the optimal correlated displacement with $k = \sqrt{(1-\eta_A)/\eta_A}$ applied to the input of the side channel. The side channel is effectively moved to the signal state prior to the main modulator M and the displacement on the signal is scaled as $x_M/\sqrt{\eta_A}$. The source S_2 should be present in the squeezed-state protocol to achieve the complete decoupling of the side channel.

profit from such the side channel. Importantly, both conditions above (decoupling the modulation and decorrelating the side channel) are required to fully eliminate the side-channel effect. In the case of the squeezed-state protocol the decorrelation is achieved upon the additional manipulation on the input of the side channel prior to the modulation so that the vacuum state is replaced by the squeezed state with variances $(V_S, 1/V_S)$, equivalent to the signal state. Using this generated squeezing in addition to the optimal correlated modulation, the output of the side channel is completely decorrelated from the signal mode for the squeezed-state protocol as well.

Interestingly, in the regime of the optimal modulation with k_{opt} the scheme becomes equivalent to the side-channel attack on the signal prior to modulation; the latter then becomes scaled by $1/\sqrt{\eta_A}$ as shown in Fig. 6. In other words, the optimal correlated displacement with k_{opt} shifts the side-channel attack from the modulated signal to the signal state before the modulation. This is in fact an additional type of side-channel attack that can also take place independently of any other side-channel attacks. It is easy to see that in the case of the coherent-state protocol such an attack yields no additional information for Eve because the correlation between the output of the side channel and the signal mode after the interaction $C_{AS_A} = \sqrt{\eta_A(1-\eta_A)}[V_S - \text{Var}(x_{SCA})]$, which is proportional to the difference of variances of the incoming modes, becomes exactly zero [similarly to the method of decoupling Eve from the main quantum channel (see [42])]. In the case of the squeezed signal, however, such an attack on the signal states leads to the nonzero correlation between the signal state and the side-channel output and this reduces the security of the squeezed-state protocol, which, nevertheless, remains superior to the coherent-state one in terms of key rate, distance, or tolerable excess noise. Therefore, e.g., for $V_S = 0.1$ the optimally correlated displacement appears to be less effective than the uncorrelated one (Fig. 5). This can be overcome if Alice is able to substitute the vacuum input of the side channel by a squeezed state with the same squeezing as the signal state, i.e., $\text{Var}(x_{SCA}) = V_S$ should hold. In this case the correlations between the squeezed signal states and the side-channel output upon k_{opt} vanish and the type-A side channel can be fully decoupled for the squeezed-state protocol as well. For details of the calculations see the Appendix.

The correlation between Alice and Bob in the regime of optimal modulation with k_{opt} changes to $V_M/\sqrt{\eta_A}$ (prior to the main channel). Thus the key rate for the same V_M in the regime of complete decoupling of the type-A side channel is quantitatively different from the key rate of the protocol with the same modulation and in the absence of the side channel. However, in the regime of imperfect postprocessing, i.e., $\beta < 1$, the modulation variance needs to be optimized. With this optimization performed the protocol with the complete decoupling of the type-A side channel becomes fully equivalent in terms of the maximum key rate, tolerable channel loss (or, equivalently, maximum distance), and tolerable channel excess noise to the protocol without the type-A side channel and with optimized modulation for a given β. This leads in particular to the overlap of the curves for the two protocols in Fig. 5, where optimized key rates for the methods of the noncorrelated modulation and of the unknown noise infusion are also given for comparison. Therefore, by optimal decoupling of the type-A side channel using only the correlated modulation and optionally squeezing on the input of the side channel one can *completely* remove its negative influence with no entanglement between the main channel and side channel being required.

Note that the uncorrelated modulation can be also combined with squeezing on the input of the side channel. This combination in the case of the squeezed-state protocol greatly improves the method of uncorrelated modulation, making it (provided the modulation is optimized) almost as effective as the method of optimized correlated modulation combined with squeezing (on the plots in Fig. 5 the corresponding line in the plotted region of parameters overlaps with the black solid line corresponding to the absence of the side channel and the difference corresponding to the limited performance of the method can only be seen for very low values of the key rate, which are irrelevant due to unavoidable finite-size effects [28,29]).

B. Noise infusion on the trusted receiver side

In the case when Eve couples an additional noise to the signal prior to the detection at Bob's side, the monitoring of the coupling output, which is not accessible to Eve, can be used. Then, by applying the proper manipulation on the data from the main detector and from the monitoring detector, the negative influence of the type-B side channel can also be fully compensated for.

We suggest the method of weighted subtraction of data from the main and the monitoring detector and show that the resulting measurement is free from the influence of the type-B side channel. Indeed, if the main homodyne detector H (see Fig. 4) after the noise-infusing side channel measures the quadrature $x'_B = x_B\sqrt{\eta_B} + x_{SCB}\sqrt{1-\eta_B}$, where x_B is the output of the main quantum channel and x_{SCB} is the noise quadrature of the type-B side channel input with $\text{Var}(x_{SCB}) = V_N$, and the monitoring detector H′ measures the quadrature $x'_{SCB} = -x_B\sqrt{1-\eta_B} + x_{SCB}\sqrt{\eta_B}$, then the weighted difference $\Delta x = g x'_B - g' x'_{SCB}$ (and similarly for the p quadrature) is free from the influence of the side channel

for $g = \sqrt{\eta_B}$ and $g' = \sqrt{1-\eta_B}$. Therefore, the additional optimized monitoring on the output of the noise-infusing side channel resulting in the detection of $\Delta x = x_B$ can completely remove the negative impact of such a side channel. Note that any pair of coefficients satisfying $g/g' = \sqrt{\eta_B/(1-\eta_B)}$ fully restores the performance of the protocol leading to $\Delta x \propto x_B$ and the linear scaling of the latter observable does not affect the lower bound on the secure key rate.

The complete removal of the noise-infusing side channel is possible also with the imperfect detectors. If both the main homodyne detector H and the monitoring detector H′ have efficiency η_D and excess noise, which can be modeled by coupling of the signal to the noise mode with the variance V_D on the coupler η_D (this is the standard model of the imperfect homodyne detector used in the security analysis of CV QKD [40]), then the settings g and g' given above also remove x_{SCB} from the weighted difference Δx and the variance then reads $\mathrm{Var}(\Delta x) = \eta_D \mathrm{Var}(x_B) + (1-\eta)V_D$. That is, the optimal monitoring of the side-channel output then becomes equivalent to the side-channel-free detection of the signal on the same imperfect homodyne detector (the details of the calculations are given in the Appendix), which contains only the trusted noise and thus does not lead to the security break in the reverse-reconciliation scheme [21].

To calculate the security against the collective attacks we consider the scheme using the equivalent interferometric setup, when the residual side channel is coupled to the signal and then detected (see the Appendix for details). This leads to the appropriate transformations of the variances and correlations. The results of calculations are given in Fig. 7 without the side-channel monitoring and with optimal monitoring of the residual side channel.

It is evident that the optimal side-channel monitoring restores the performance of the protocol providing exactly the same key rate as in the absence of the side channel. The noise-infusing side channel can therefore be completely compensated for. Simultaneously, the Gaussian entanglement between the trusted parties is fully restored even if it was previously broken by the effect of noise infused in the side channel. Experimental aspects of noise cancellation by the

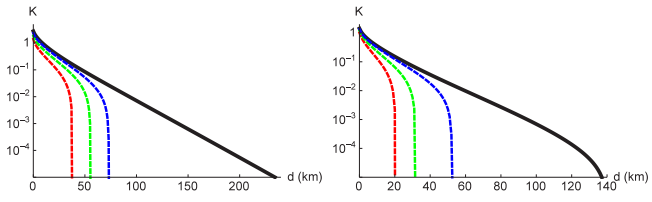


FIG. 7. Key rate secure against collective attacks versus distance in a standard telecom fiber (with an attenuation of -0.2 dB/km) for the squeezed-state protocol with $V_S = 0.1$ (left) and the coherent-state protocol (right) in the presence of the type-B noise-infusing side channel on the receiver side without the side-channel monitoring (dashed lines) and with optimal monitoring, perfectly coinciding with the profile of the key rate without the side channel (solid black lines). The side-channel coupling is $\eta_B = 0.5, 0.7, 0.9$ (from left to right, i.e., red, green, and blue dashed lines, respectively), $\beta = 0.95$, $\epsilon = 5\%$, $V_N = 1.05$, and the modulation variance V_M is optimized for the given parameters.

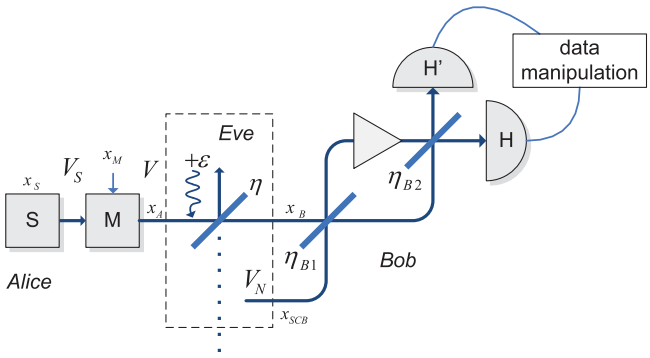


FIG. 8. Scheme of the CV QKD with the generalized interferometric coupling (parametrized by the transmittance values η_{B1} and η_{B2} of the couplers and by the phase shift ϕ) to the noisy side channel with untrusted input of variance V_N on the receiving side and the monitoring of the side-channel output followed by the data manipulation.

measurement have been studied in [43], which demonstrates the feasibility of such a method for CV QKD. Note that the result reported here is obtained under different conditions than the previous analysis of the multimode channels [44,45], where the auxiliary channels received by Bob contain information encoded by Alice, i.e., are parallel to the main quantum channel.

We also consider the side-channel noise infusion based on the generalized interferometric interaction modeled by two couplers with different transmittance values η_{B1} and η_{B2} and a phase shift ϕ in one of the arms between the couplers as shown in Fig. 8.

In this case the monitoring of the side-channel output suggested above can fully restore the performance of the protocol only when the phase shift is absent (i.e., $\phi = 0$; see the Appendix for the details) and the optimal coefficients of the data manipulation read $g = 1$ and $g' = [\sqrt{(1-\eta_{B2})\eta_{B2}} + \sqrt{(1-\eta_{B1})\eta_{B1}}]/(1-\eta_{B1}-\eta_{B2})$. The setting can be obtained by maximizing the mutual information between the trusted parties and therefore does not require the estimation of η_{B1} and η_{B2} independently. However, when the nonzero phase shift is present and the output of the interferometric coupling contains combinations of x and p quadratures of the signal and the noise input, simple side-channel monitoring by the homodyne detection in the x quadrature and the linear data manipulation are not sufficient to completely restore the performance of the protocol. It can can be used to partly compensate for the negative influence of the type-B side channel, as shown in Fig. 9, where the key rate is plotted for the coherent- and squeezed-state protocols with respect to the weighting g' (assuming $g = 1$), which can maximize the mutual information and, respectively, the key rate.

The optimal data manipulation setting in the general case becomes the lengthy function on the parameters of the protocol, including the values of the coupling and the phase shift as well as the signal and modulation variances and the parameters of the channel. In order to improve the decoupling of the side channel an optimal additional phase shift can be applied prior to the control detection (so that the mutual information is maximized) or a more general strategy based

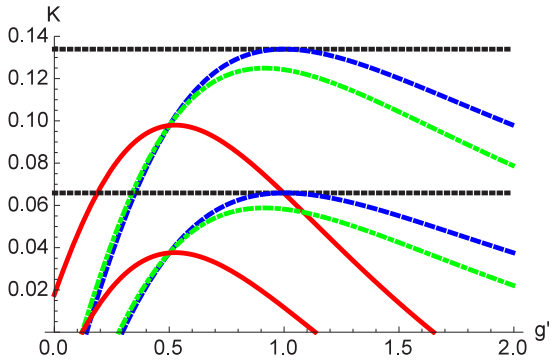


FIG. 9. Key rate secure against collective attacks versus weighting of the data manipulation in the monitoring of the type-B side channel with the generalized interferometric interaction for the squeezed-state protocol with $V_S = 0.1$ (upper lines) and the coherent-state protocol (lower lines) in the absence of the type-B side channel (black horizontal dotted lines), with no phase shift $\phi = 0$ (dashed blue lines), with $\phi = 0.5$ (green dot-dashed lines), and $\phi = 1.5$ (red solid lines). The parameters of the interaction in the presence of the side channel are $\eta_{B1} = 0.9$ and $\eta_{B2} = 0.8$, the modulation variance $V_M = 10$, the channel transmittance is $\eta = 0.1$, and the protocols implementation is otherwise perfect.

on the heterodyne detection and subsequent data manipulation could be used and optimized similarly to the elimination of the cross-talk in the channel [44].

V. CONCLUSION

We have studied the effect of the side-channel leakage and noise infusion on the trusted sides of the continuous-variable quantum key distribution protocols. The negative effect of the side-channel leakage on the trusted sender side leads to the degradation of the key rate and to the increased sensitivity of the protocol to the channel noise. At the same time, the side-channel noise infusion on the trusted receiver side can completely break the security of the protocols even upon pure channel loss. We suggested and examined the method of additional modulation applied to the side-channel input being under the control of a trusted sending party. We show that if the additional modulation is properly correlated with the main modulation on the signal and squeezing applied on the side-channel input in the case of the squeezed-state protocol, the negative impact of the lossy side channel can be completely removed. Alternatively, we show the possibility to compensate for the negative impact of the noisy side channel on the receiver side by introducing the monitoring of the output of the side channel. Since both methods work independently by completely removing the side channels, they can be combined in a single protocol. Moreover, since the optimal settings for the methods are independent of the channel parameters, the methods can be applied by the trusted parties using only the parameters of their local trusted stations and do not themselves rely on the channel estimation. Our result therefore describes effective and feasible methods of compensating for the quantum side channels in a continuous-variable quantum key distribution between the trusted parties, which do not require entanglement or non-Gaussian operations.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the EU FP7 under Grant Agreement No. 308803 (Project BRISQ2), cofinanced by MŠMT ČR (Grant No. 7E13032). I.D. acknowledges Palacký University Project No. IGA_PrF_2014008. I.D. and V.C.U. acknowledge the Project No. P205/12/0694 of the Czech Science Foundation.

APPENDIX: SECURITY ANALYSIS IN DETAIL

Here we provide detailed calculations for the security analysis of the above-described Gaussian continuous-variable quantum key distribution protocols with side channels.

1. Scheme and parametrization

The scheme of the protocols is given in Fig. 1. As mentioned, the channel is parametrized by transmittance (loss) η and excess noise ϵ, while side channels are parametrized by coupling η_A (for the sender-side type-A lossy side channel) and by coupling η_B and excess noise V_N (for the receiver-side type-B noise-infusing side channel). The protocols in the prepare-and-measure (PM) setting are based on the preparation of a signal state (coherent or squeezed) characterized by the quadrature values x_S and p_S, which are Gaussian distributed around zero with variances $\mathrm{Var}(x_S) = V_S$ and $\mathrm{Var}(p_S) = 1/V_S$, where $V_S \leqslant 1$ is generally the squeezed variance, which in the case of coherent states is saturated by $V_S = 1$. Here and in the following, with no loss of generality, we assume that the states are squeezed and measured in the x quadrature. The results for the p-quadrature squeezing and measurement are obtained by replacing $x \to p$ and vice versa. The signal is modulated by applying the displacement x_M or p_M randomly chosen from a Gaussian distribution centered around zero with variance $\mathrm{Var}(x_M) = \mathrm{Var}(p_M) = V_M$ so that the resulting quadrature becomes $x_A = x_S + x_M$. Here and in the following the equivalent expressions apply to the p quadrature since the main quantum channel and the side channels are assumed to be phase insensitive (which is valid for typical optical channels such as optical fiber or free-space links). Now if the channel is present the quadrature values after the channel are given by $x_B = (x_A + x_N)\sqrt{\eta} + x_0\sqrt{1-\eta}$, where x_0 is the quadrature value of the vacuum state coupled to the signal to describe the loss $\mathrm{Var}(x_0) = 1$ and x_N is the quadrature value of the excess noise $\mathrm{Var}(x_N) = \epsilon$.

If the side-channel loss is present at the sender side (type-A side channel), then the signal is coupled to the vacuum input of the side channel, which is modeled by a beam splitter with transmittance η_A, which is the side-channel loss. As mentioned, the quadrature that enters the quantum channel is then changed to $x'_A = x_A\sqrt{\eta_A} + x_{SCA}(\sqrt{1-\eta_A})$, where x_{SCA} is the quadrature value of the vacuum state on the input of the beam splitter $\mathrm{Var}(x_{SCA}) = 1$. If the noise-infusing side channel is present, then, as mentioned in the main text, the output of the quantum channel is further modified to $x'_B = x_B\sqrt{\eta_B} + x_{SCB}\sqrt{1-\eta_B}$, where x_{SCB} is the input noise of the type-B side channel with $\mathrm{Var}(x_{SCB}) = V_N$. Knowing the transformation of the quadrature values, we can obtain the variances and correlations between the quadratures and derive the covariance matrices describing the states shared

between the trusted parties Alice and Bob and available to an eavesdropper Eve, which are then used in the security analysis below.

2. Secure key rate

As mentioned, we estimate the security of the protocols in the presence of the side channels and upon additional manipulations aimed to remove the side channels, as the value and positivity of the lower bound on the key rate, which in the case of collective attacks (when Eve is able to collectively measure her probe states after interaction with the signal) and reverse reconciliation [9] reads $K = \beta I_{AB} - \chi_{BE}$, where $\beta \in (0,1)$ is the postprocessing efficiency that takes into account the amount of data that trusted parties lose due to imperfections of the error correction algorithms, I_{AB} is the mutual information between the trusted parties, and χ_{BE} is the Holevo bound, giving the upper bound on the information that is available to Eve. In the case of individual attacks, when Eve is limited by the individual measurement on her probe states, the Holevo bound is replaced by the classical Shannon information between Eve and Bob I_{BE}.

3. Mutual information and individual attacks

In order to calculate the classical (Shannon) mutual information we use the expression for Shannon entropies in the case of Gaussian continuous distributions [46]

$$I_{XY} = \frac{1}{2}\log_2 \frac{V_X}{V_{X|Y}}, \tag{A1}$$

where X and Y are two zero-mean Gaussian random variables with variances $V_X \equiv \langle X^2\rangle$ and $V_Y \equiv \langle Y^2\rangle$, respectively, and $V_{X|Y} = V_X - C_{XY}^2/V_Y$ is the conditional variance with $C_{XY} \equiv \langle XY\rangle$ the correlation (covariance) between X and Y. Note that (A1) is symmetrical with respect to X and Y. In the case of the Gaussian protocols considered in the paper, the variables are the quadratures displacements being introduced by modulation and the quadrature values measured on the remote side of the channel and by a potential eavesdropper are all Gaussian distributed. This allows us to calculate the mutual information I_{AB} and upper bound the information leakage I_{BE} in the case of individual attacks.

The calculation of the mutual information is straightforward. Following the expression (A1), we can derive the mutual information between Alice and Bob as $I_{AB} = \frac{1}{2}\log_2(V_A/V_{A|B})$, where V_A is the variance of the data imposed by Alice by displacement (typically equivalent to V_M), while conditional variance $V_{A|B} = V_A - C_{AB}^2/V_B$ involves correlation $C_{AB} = \mathrm{Cov}(x_M, x_B)$, i.e., the covariance between the data kept by Alice and the data measured by Bob, and the variance $V_B = \mathrm{Var}(x_B)$ of Bob's measurement results (which is x'_B if the type-B side channel is present).

The calculation of Eve's information I_{BE} in the case of individual attacks is similar. It requires knowing the variances of the modes that are available to Eve for the individual measurements and correlations with the measurement results on the side of Bob; these will be derived in the particular cases below.

4. Collective attacks

In the case of collective attacks, as mentioned, the information, which is available to Eve, is bounded by the Holevo quantity, which is the capacity of a bosonic channel between Eve and Bob. It is calculated as $\chi_{BE} = S(\gamma_E) - S(\gamma_{E|B})$, the difference of the von Neumann (quantum) entropies $S(\gamma_E)$ of the state of the modes, which are available to Eve for a collective measurement described by the covariance matrix γ_E, and $S(\gamma_{E|B})$ of the same state conditioned on the measurement results of Bob.

In the general case, when the excess noise is present in the channel and/or in the type-B side channel, we use the purification method [40], i.e., we assume that an eavesdropper Eve can purify the state shared by the trusted parties, so $S(\gamma_E) = S(\gamma_{AB})$, where AB is generally a multimode initially pure state shared between the trusted parties in which all the impurity is assumed to be caused by Eve's collective attack. After Bob's projective measurement of one of the quadratures a similar equivalence holds for the conditioned states: $S(\gamma_{E|B}) = S(\gamma_{A|B})$. Thus the Holevo bound in Eq. (1) is expressed as $\chi_{BE} = S(\gamma_{AB}) - S(\gamma_{A|B})$.

The entropy $S(\gamma_{AB})$ is determined from the symplectic eigenvalues λ_i of the n-mode covariance matrix γ_{AB} as

$$S = \sum_{i=1}^{n} G\left[\frac{\lambda_i - 1}{2}\right], \tag{A2}$$

where G is the bosonic entropic function [26]

$$G(x) = (x+1)\log_2(x+1) - x\log_2(x). \tag{A3}$$

The subtrahend in the expression for the Holevo bound is the entropy similarly determined by the symplectic eigenvalues of the respective conditional covariance matrix $\gamma_{A|B}$ after Bob's projective measurement (with no loss of generality, we assume measurement of the x quadrature)

$$\gamma_{A|B} = \gamma_A - \sigma_{B|A}[X\gamma_B X]^{\mathrm{MP}}\sigma_{B|A}^T, \tag{A4}$$

where $\sigma_{B|A}$ is the correlation matrix between mode B and the rest of the trusted modes, $X = \mathrm{Diag}(1,0,0,0)$, where Diag denotes a diagonal matrix, and MP is the Moore-Penrose pseudoinverse of the matrix.

The purification [40] is typically based on introducing the entangled [also referred to as Einstein-Podolsky-Rosen (EPR)] sources, which are the two-mode vacuum states described by the covariance matrices of the form

$$\gamma_{\mathrm{EPR}} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{I} \end{pmatrix}, \tag{A5}$$

where V is the variance of each of the two modes, $\mathbb{I}$ is the 2×2 unity matrix, and $\sigma_z = \mathrm{Diag}(1,0,0,-1)$. It is assumed that Alice is performing a homodyne (in the x or p quadrature) or heterodyne (in the x and p quadratures simultaneously using two homodyne detectors on the signal, split on a balanced beam splitter) measurement on one of the modes, which conditionally prepares the squeezed state with variance $1/V$ or coherent state in the other mode, respectively. The unmeasured mode is then being sent through the channel and the side channels. Such a scheme is then equivalent to a PM scheme based on squeezed or coherent states with $V_S = 1/V$ or $V_S = 1$, respectively (depending on the homodyne or heterodyne

measurement applied by Alice) and $V_M = V - V_S$. The mode interactions in the side channels and the main channel based on the liner coupling are taken into account in the covariance matrices using the input-output relations for the quadrature vectors $r_i = (x_i, p_i)^T$ of interacting modes 1 and 2 in the form

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}_{\text{out}} = \begin{pmatrix} \sqrt{T}\mathbb{I} & \sqrt{1-T}\mathbb{I} \\ -\sqrt{1-T}\mathbb{I} & \sqrt{T}\mathbb{I} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}_{\text{in}}, \tag{A6}$$

where T stands for the transmittance of a coupling beam splitter. Such transformations lead to changes of variances and covariances that form the resulting covariance matrices. The lower bound on the key rate secure against collective attacks is then calculated numerically using (A2) and (A3). In the case when modulation V_M is independent of the signal squeezing V_S the more general entanglement-based scheme [27] is used instead of the standard EPR-based purification described above.

The purification method allows us to analyze the security of the protocols in the conditions of untrusted noise by estimating the lower bound on the secure key rate and in particular to study the region of insecurity where the lower bound turns to zero. Further, we describe the theoretical purification schemes used to calculate the Holevo bound in the particular cases. Note that the purification schemes give also the same mutual information I_{AB} as in the PM versions of the protocols. We also cross-check our results using the entangling cloner [47] collective attack being the particular purification of the channel noise by an EPR source possessed by Eve, which is also widely used in CV QKD security analysis as a typical collective attack (see, e.g., [19,20]). The results obtained using the entangling cloner exactly confirm our calculations based on the purification models.

5. Side-channel loss on the sender side

In the case of the type-A side channel, the variance of Alice's data is unchanged and remains V_M and the correlation between Alice and Bob is scaled by the channel and the side channel so that $C_{AB} = \sqrt{\eta_A \eta} V_M$. The variance of the state measured by Bob in the x quadrature after the side channel and the main noisy and lossy channel $V_B = \eta[\eta_A V + \epsilon - \eta_A] + 1$.

We first investigate the influence of the side channel for the case of individual attacks with pure losses ($\epsilon = 0$) to estimate the security region. Taking into account the above-given variances and correlations, the mutual information I_{AB} can be directly obtained as (2). In the case of individual attacks in the purely lossy channel, Eve is able to measure the output mode of the side channel, which we denote by S_A, and the output of the main channel, which we denote by E. Therefore, the mutual information I_{BE} using the symmetry of the mutual information (A1) is to be calculated as

$$I_{BE} = \frac{1}{2} \log_2 \frac{V_B}{V_{B|ES_A}}, \tag{A7}$$

where $V_{B|ES_A}$ is the variance of Bob's measurement conditioned by measurements of Eve on the modes E and S_A. The calculations taking into account the variances of Eve's modes $V_E = (\eta_A V + 1 - \eta_A)(1-\eta) + \eta$ and $V_{S_A} = \eta_A + (1-\eta_A)V$ and correlations $C_{BE} = \eta_A \sqrt{\eta(1-\eta)}(1-V)$ and $C_{BS_A} = \sqrt{\eta_A \eta(1-\eta_A)}(1-V)$ result in the expression

$$V_{B|ES_A} = \frac{V}{\eta_A \eta(1-V) + V} \tag{A8}$$

from which the expression (3) is obtained.

In the case when the channel noise is present we model Eve's individual attack as an optimal entangling cloner [47], i.e., we assume that Eve possesses the two-mode entangled source $E_1 E_2$ with the variance $N = 1 + \frac{\eta\epsilon}{1-\eta}$ so that the mode E_1 interacts with the signal and introduces the loss η and the excess noise ϵ. Eve is then able to measure three modes: the output of the side channel S_A and the modes E_1 and E_2 of the entangling cloner. Therefore, the mutual information I_{BE} between Eve and Bob should read

$$I_{BE} = \frac{1}{2} \log_2 \frac{V_B}{V_{B|S_A E_1 E_2}}, \tag{A9}$$

where $V_{B|S_A E_1 E_2}$ is the variance of Bob's measurement conditioned by measurements of Eve on the modes S_A, E_1, and E_2. The variances of the modes after the side channel and the main channel are $V_B = \eta[\eta_A V + 1 - \eta_A + \epsilon] + 1$ [which also changes the mutual information (3)], $V_{S_A} = \eta_A + (1-\eta_A)V$ is unchanged by the channel noise, $E_1 = \eta N + (1-\eta)(\eta_A V + 1 - \eta_A)$, and $E_2 = N$. The correlations are $C_{BS_A} = \sqrt{\eta_A \eta(1-\eta_A)}(1-V)$, $C_{BE_1} = \sqrt{\eta(1-\eta)}(N - \eta_A V - 1 + \eta_A)$, and $C_{BE_2} = \sqrt{(1-\eta)(N^2-1)}$. From this the conditional variance

$$V_{B|S_A E_1 E_2} = \frac{1 + \eta_A(V-1)}{1 + \eta\epsilon + \eta_A(V-1)[1-\eta(1-\epsilon)]} \tag{A10}$$

can be obtained and used to calculate the key rate secure against the individual attacks in a noisy channel.

In the case of collective attacks in a noisy channel and no additional manipulation on the side-channel input the security is calculated through the 4×4 covariance matrix

$$\gamma_{AB} = \begin{pmatrix} \mathrm{V}\mathbb{I} & \sqrt{\eta_A \eta(V^2-1)}\sigma_z \\ \sqrt{\eta_A \eta(V^2-1)}\sigma_z & [(V-1)\eta_A \eta + \epsilon\eta + 1]\mathbb{I} \end{pmatrix}, \tag{A11}$$

which describes the state shared between the trusted parties in the EPR-based version of the protocols. The conditional matrix after the measurement at Bob in particular contains η_A separately from η and reads

$$\gamma_{A|B} = \begin{pmatrix} V - \frac{\eta_A \eta(V^2-1)}{1+\eta(\eta_A V - \eta_A + \epsilon)} & 0 \\ 0 & V \end{pmatrix}. \tag{A12}$$

From these two matrices the security of the protocol can be analyzed for the case of collective attacks. We do not provide the explicit expressions for the multimode covariance matrices in the further analysis since they are too lengthy; however, they can be directly obtained using the input-output relations (A6) and the details of the purification schemes given below. Further, we present the purification schemes for the different methods of the side-channel decoupling as well as the changes of the variances and correlations of measured data upon the additional manipulations on the side channels.

First, if the uncorrelated noise is added to the input of the side channel, it is modeled as the coupling of one of the modes

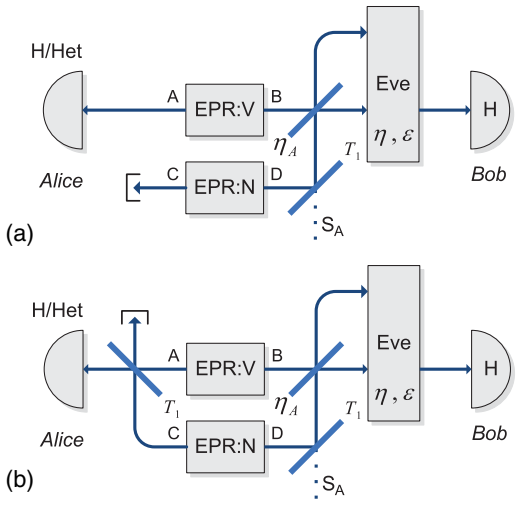


FIG. 10. (a) Theoretical purification of the equivalent PM scheme with the side-channel loss on the sender side and thermal noise applied on the input of the side channel. (b) Purification of the PM scheme with the side-channel loss on the sender side and known modulation applied on the input of the side channel. Homodyne or heterodyne detection is applied at the side of Alice in both cases depending on the protocol.

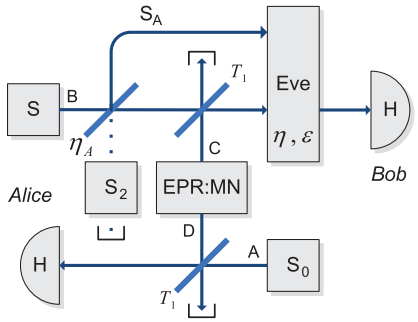


FIG. 11. Theoretical purification of the equivalent PM scheme with the side-channel loss on the sender side and the optimal correlated modulation applied on the input of the side channel precessed by the optional squeezed-state preparation on the source S_2 in the case of the squeezed-state protocol as depicted in Fig. 6. The source S_0 produces an infinitely squeezed state, the entangled source EPR:MN provides the modulation of the signal, and the trusted parties perform homodyne detection on their respective modes A and B.

of the EPR source N [see Fig. 10(a)] to the side-channel input using a strongly unbalanced beam splitter with transmittance (for mode S_A) $T_1 \to 1$. The variance of the source is set to $N = V_{NS}/(1 - T_1)$; this way the noise is added losslessly.

The state of the modes $ABCD$ contains all the purified trusted noise and the Holevo bound for the standard Gaussian protocols is then calculated following the purification method as $\chi_{BE} = S(\gamma_{ABCD}) - S(\gamma_{ACD|B})$. If the known modulation is applied to the side-channel input, then the purification is based on a similar scheme but the second mode of the EPR source N is coupled to the mode A, measured by Alice. This way the displacement that is applied to the input of the side channel is also added to the displacement measured by Alice [see Fig. 10(b)]. Alice's data in this case have the variance $V_A = V_M + V_{NM}$, while the correlation with Bob after the side channel and the main channel is given by $C_{AB} = \sqrt{\eta}(\sqrt{\eta_A}V_M + \sqrt{1-\eta_A}V_{NM})$. Bob's measured variance is $V_B = \eta[\eta_A(V - V_{NM}) - \eta_A + \epsilon] + 1$. From this expression the expression for the mutual information (9) is directly obtained.

The calculations are then similar to the previous case. In both cases, if the generalized scheme in which modulation is independent from the signal states is to be used, then the main source EPR:V is replaced with the respective entanglement-based generalized preparation as described in [27]. The manipulations on the side channel remain purified as described above.

Finally, if the correlated displacement is added and the input of the side channel is additionally squeezed to V_S, then the variance of Alice's data remains V_M, but the correlation with Bob is changed to $C_{AB} = \sqrt{\eta}(\sqrt{\eta_A} + k\sqrt{1-\eta_A})V_M$ and the variance of the state measured at the Bob's side is $V_B = \eta[2kV_M\sqrt{\eta_A(1-\eta_A)} + k^2V_M(1-\eta_A) - \eta_A V_M + V_S + \epsilon - 1] + 1$. From this the expression for the mutual information can be obtained in the general case.

For the optimal $k = \sqrt{(1-\eta_A)/\eta_A}$ and with the side-channel input substituted by the squeezed state with variances V_S and $1/V_S$ (in the case of the squeezed-state protocol) it is easy to see that the main signal mode and the side-channel output described by $x'_A = x_S\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A} + x_M(\sqrt{\eta_A} + k\sqrt{1-\eta_A})$ and $\tilde{x}'_{SCA} = x_{SCA}\sqrt{\eta_A} - x_S\sqrt{1-\eta_A} + x_M(k\sqrt{\eta_A} - \sqrt{1-\eta_A})$, respectively become completely uncorrelated, i.e., $\mathrm{Cov}(x'_A, \tilde{x}'_{SCA}) = 0$. Therefore, the side channel becomes decoupled from the main signal. For the calculations of the Holevo bound the equivalent scheme depicted in Fig. 6 must be purified. This is done by introducing the EPR source MN (see Fig. 11) with variance $V_M/\eta_A(1 - T_1)$. It is coupled to the signal state produced by the source S in the mode B and to the infinitely squeezed state used for simulating the detection, produced by the source S_0 in the mode A on the strongly unbalanced beam splitters with the transmittance for modes A and B being $T_1 \to 1$. The input of the side channel is optionally squeezed using squeezer S_2 in the case of the squeezed-state protocol. The state that is then sent through the channel (mode B) is defined by the single-mode covariance matrix $\gamma_B = \mathrm{Diag}(T_1V_S + V_M/\eta_A, T_1/V_S + V_M/\eta_A)$. In the limit $T_1 \to 1$ this is equivalent to the preparation of a signal state V_S, attacked by the side channel with input V_S (prepared by Alice in the case of the squeezed-state protocol), which leaves the signal state unchanged, and subsequent symmetrical (having the same variance in the both the x and p quadratures) Gaussian modulation with variance V_M/η_A. The correlation between the measurements at Alice and at Bob in the absence of the quantum channel is $C_{AB} = -\sqrt{(V_M/\eta_A)^2 - (1-T_1)^2}$, which is equivalent to the modulation with variance V_M/η_A applied by Alice in the PM setup when $T_1 = 1$. The state that is measured by Alice (mode A) is defined by $\gamma_A = \mathrm{Diag}(T_1V_0 + V_M/\eta_A, T_1/V_0 + V_M/\eta_A)$, where V_0 is the variance of the squeezed state, produced by the source S_2. The first element of matrix γ_A, which is measured by the

x-quadrature homodyne measurement, in the limit of $V_0 \to 0$, corresponds to Alice perfectly knowing the displacements of the modulation V_M/η_A in the PM setup. After the measurement at the Alice's side the state that is conditionally prepared on the channel input is given by $\gamma_{B|A} = \mathrm{Diag}(T_1 V_S + [\eta_A(T_1-1)^2 + T_1 V_0 V_M]/(\eta_A T_1 V_0 + V_M), T_1/V_S + V_M/\eta_A)$, which in the regime of $T_1 = 1$ and $V_0 = 0$ gives $\mathrm{Diag}(V_S, 1/V_S + V_M/\eta_A)$, corresponding to the modulation of the signal state $\mathrm{Diag}(V_S, 1/V_S)$ with variance V_M/η_A in both the quadratures with only one value x being kept. Our purification scheme (see Fig. 11) is therefore equivalent to the PM one (shown in Fig. 6), providing (in the limits $T_1 \to 1$ and $V_0 \to 0$) the same variances and correlations and resulting in the same conditional states. Moreover, the developed scheme allows purification of practically any PM scheme being more adjustable than the standard EPR-based approach [40]. The asymmetrical modulation can be introduced by the general preparation of the state EPR:MN using two different orthogonally squeezed states, however, such an extension was not needed in the tasks of the present paper.

In the purification scheme the state of the modes $ABCD$ is pure, while the channel noise and loss introduce impurity to the state. The mode S_A is not relevant in the scheme since it is uncorrelated from the rest of the setup due to the equality of the variances of modes A and S_A prior to the side-channel coupling η_A (it is shown on the scheme only for explanatory purposes). Then the Holevo bound is calculated as $\chi_{BE} = S(\gamma_{ABCD}) - S(\gamma_{ACD|B})$.

6. Side-channel noise infusion on the receiver side

In the case of the type-B side channel the variance of Alice's data remains V_M and the correlation between Alice and Bob is scaled by the channel and the side channel so that $C_{AB} = \sqrt{\eta\eta_B} V_M$. The variance of the state measured by Bob in the x quadrature after the main noisy and lossy channel and the side channel is $V_B = \eta_B[\eta(V+\epsilon) + 1 - \eta] + (1-\eta_B)V_N$.

Let us first consider the individual attacks in the purely attenuating main channel, i.e., $\epsilon = 0$. Taking into account the above-given variances and correlations, the mutual information I_{AB} can be directly obtained as (5). In the case of individual attacks in the purely lossy channel Eve is able to measure the output mode of the main channel, which we denote by E. Moreover, Eve controls the input of the noisy side channel, which we introduce as an entangling cloner attack, which was shown to be optimal in the case of individual attacks [47]. Therefore, we assume that Eve possesses the two-mode entangled source E_1E_2 with the variance V_N and is able to measure one of the modes E_1, while the other mode E_2 is coupled to the signal on the η_B beam splitter. Therefore, the mutual information I_{BE} using the symmetry of the mutual information (A1) is to be calculated as

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|EE_1}}, \tag{A13}$$

where $V_{B|EE_1}$ is the variance of Bob's measurement conditioned by measurements of Eve on the modes E and E_1. The calculations taking into account the variances of Eve's modes $V_E = V(1-\eta) + \eta$ and $V_{E_1} = V_N$ (since is Eve is measuring the mode of the cloner that did not interact with the signal) and correlations $C_{BE} = \sqrt{\eta\eta_B(1-\eta)}(1-V)$ and $C_{BE_1} = \sqrt{(1-\eta_B)(V_N^2-1)}$ (the latter provided by the correlations within the entangling cloner) result in the expression

$$V_{B|EE_1} = \frac{\eta_B V}{V(1-\eta)+\eta} + \frac{1-\eta_B}{V_N} \tag{A14}$$

from which the expression (6) is obtained.

If the main homodyne detector H and the monitoring detector H′ (see Fig. 4) are both imperfect with loss η_D and noise of the variance V_D, which is coupled to the signal with the ratio η_D [40], then the quadratures measured by the detectors H and H′ will be given by

$$x'_B = \sqrt{\eta_D}(x_B\sqrt{\eta_B} + x_{SCB}\sqrt{1-\eta_B}) + x_1\sqrt{1-\eta_D} \tag{A15}$$

and

$$x'_{SCB} = \sqrt{\eta_D}(-x_B\sqrt{1-\eta_B} + x_{SCB}\sqrt{\eta_B}) + x_2\sqrt{1-\eta_D}, \tag{A16}$$

respectively, where x_1 and x_2 are the quadrature values associated with the detector noise such that $\mathrm{Var}(x_1) = \mathrm{Var}(x_2) \equiv V_D$. The weighted difference $\Delta x = g x'_B - g' x'_{SCB}$ will then be given by

$$\Delta x = x_B\sqrt{\eta_D}(g\sqrt{\eta_B} + g'\sqrt{1-\eta_B}) + x_{SCB}\sqrt{\eta_D}(g\sqrt{1-\eta_B} - g'\sqrt{\eta_B}) + \sqrt{1-\eta_D}(g x_1 - g' x_2). \tag{A17}$$

By setting the weights of the difference to $g = \sqrt{\eta_B}$ and $g' = \sqrt{1-\eta_B}$, the result of the subtraction becomes

$$\Delta x = x_B\sqrt{\eta_D} + \sqrt{1-\eta_D}(x_1\sqrt{\eta_B} - x_2\sqrt{1-\eta_B}), \tag{A18}$$

where the noise of the side channel given by the quadrature value x_{SCB} is completely removed. The variance of the weighted difference then becomes $\mathrm{Var}(\Delta x) = \eta_D V_B + (1-\eta_D)V_D$, i.e., equivalent to the measurement of the signal x_B on the imperfect homodyne detector with loss η_D and noise V_D; the scaling $\sqrt{\eta_D}$ then also applies to the correlation C_{AB}. When the detection is purely lossy, i.e., $V_D = 1$, the expression then further simplifies as $\mathrm{Var}(\Delta x) = \eta_D V_B + 1 - \eta_D$.

In the case of collective attacks in the noisy channel and in the presence of the type-B side channel we use the purification scheme based on the entangled source of modes A and B of variance V with mode A measured on Alice's side with the homodyne or heterodyne detector used. In this case the noisy mode S_B is assumed to be purified by Eve (see Fig. 12). However, it is reflected by the beam splitter with transmittance $T_0 = 0$ fed by the vacuum input and the fully reflected mode C is then coupled on the unbalanced beam splitter T with the signal mode B. Then all the impurity of the state shared between Alice and Bob is attributed to Eve and the following equalities hold: $S(\gamma_E) = S(\gamma_{ABC})$ and $S(\gamma_{E|B}) = S(\gamma_{AC|B})$.

Further, we equivalently represent the type-B side-channel output monitoring and data manipulation by an interferometric scheme, when the outputs of the side-channel coupling η_B (modes B and C in the purification scheme) are coupled again on a beam splitter with transmittance T. The case when the interferometric setup is properly balanced, i.e., $T = \eta_B$, corresponds to the optimized monitoring on the output of the

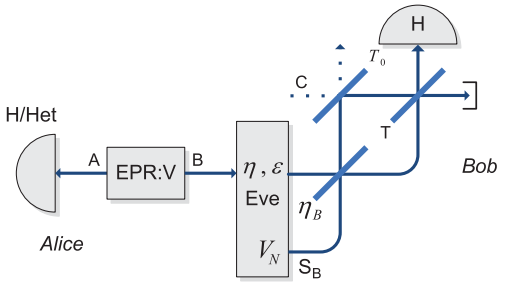


FIG. 12. Theoretical purification of the equivalent PM scheme with the side-channel noise addition on the receiver-side optimal monitoring of the side-channel output, represented by the interferometric scheme applied on the output of the side channel prior to the trusted detection; the homodyne or heterodyne detection is applied at the side of Alice depending on the protocol.

type-B side channel, as described in the main text. Indeed, the quadrature measured on the signal mode B after all the interactions is given by $x'_B = x_B[\sqrt{T\eta_B} + \sqrt{(1-T)(1-\eta_B)}] + x_{SCB}[\sqrt{\eta_B(1-T)} - \sqrt{T(1-\eta_B)}]$, where x_B is the main signal mode before the side-channel interaction and x_{SCB} is the side-channel input prior to interaction. It is easy to see that upon $T = \eta_B$ the resulting quadrature $x'_B = x_B$ of mode B contains no side-channel noise due to the destructive interference and the negative effect of the side channel is removed completely. Note that if the reflection of the mode S_B on the beam splitter T_0 would be absent and the mode B would be directly coupled to the mode S_B on the beam splitter with transmittance T, the equivalent measurement that removes the type-B side channel would be on the mode S_B upon $T = 1 - \eta_B$. The described scheme allows calculations using the purification method simply as $\chi_{BE} = S(\gamma_{ABC}) - S(\gamma_{AC|B})$ since the side-channel output monitoring emulated by the interferometric setup does not change the purity of the states. The performance of the protocol thus becomes equivalent to the one of the protocol without the type-B side channel, which is confirmed in the case of collective attacks in a noisy channel. In the case of the generalized preparation (when modulation is independent of the signal state variance) we apply a similar scheme but replace the EPV:V source with the generalized entangled state preparation as described in [27].

In the case of the interferometric-type interaction between the signal and the type-B side channel, as shown in Fig. 9, the mode transformations during the interactions become more complex and read

$$\begin{aligned} x'_B = {} & x_B[\sqrt{\eta_{B1}\eta_{B2}} - \cos\phi\sqrt{(1-\eta_{B1})(1-\eta_{B2})}] \\ & + x_{SCB}[\sqrt{\eta_{B2}(1-\eta_{B1})} + \cos\phi\sqrt{\eta_{B1}(1-\eta_{B2})}] \\ & - p_B \sin\phi\sqrt{(1-\eta_{B1})(1-\eta_{B2})} \\ & + p_{SCB}\sin\phi\sqrt{\eta_{B1}(1-\eta_{B2})} \end{aligned} \tag{A19}$$

and

$$\begin{aligned} x'_{SCB} = {} & x_B[-\sqrt{\eta_{B1}(1-\eta_{B2})} - \cos\phi\sqrt{\eta_{B2}(1-\eta_{B1})}] \\ & + x_{SCB}[\cos\phi\sqrt{\eta_{B1}\eta_{B2}} - \sqrt{(1-\eta_{B1})(1-\eta_{B2})}] \\ & - p_B\sin\phi\sqrt{\eta_{B2}(1-\eta_{B1})} + p_{SCB}\sin\phi\sqrt{\eta_{B1}\eta_{B2}}, \end{aligned} \tag{A20}$$

now involving the contributions from the p quadratures p_B and p_{SCN} of the signal and side-channel noise modes, respectively, which is caused by the phase shift in the interaction. This prevents the complete decoupling of the type-B side channel by simple manipulation on the homodyne measurement results in the form $gx'_B - g'x'_{SCB}$, as illustrated in Fig. 9 (plotted based on the numerical calculations using the equivalent transmittance T in the purification-based scheme). The complete decoupling in such a case is possible only when $\phi = 0$ and the cross-quadrature terms are absent.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[4] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
[5] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
[6] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[7] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).
[8] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[10] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[11] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[12] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).
[13] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).
[14] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[15] R. Renner, Nat. Phys. **3**, 645 (2007).
[16] M. Mertz, H. Kampermann, S. Bratzik, and D. Bruß, Phys. Rev. A **87**, 012315 (2013).
[17] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[18] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[19] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
[20] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[21] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[22] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).
[23] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[24] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
[25] S. Pirandola *et al.*, Nat. Photon. **9**, 397 (2015).
[26] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[27] V. C. Usenko and R. Filip, New J. Phys. **13**, 113007 (2011).
[28] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).
[29] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[30] F. Standaert, in *Secure Integrated Circuits and Systems* (Springer, Berlin, 2009), pp. 27–44.
[31] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, New J. Phys. **14**, 093048 (2012).
[32] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[33] K.-P. Ho, *Phase-Modulated Optical Communication Systems* (Springer, Berlin, 2005).
[34] N. A. Peters *et al.*, New J. Phys. **11**, 045012 (2009).
[35] S. Haroche, in *Quantum Entanglement and Information Processing*, edited by D. Estéve, J.-M. Raimond, and J. Dalibard, Proceedings of the Les Houches Summer School of Theoretical Physics, LXXIX, 2003 (Elsevier, Amsterdam, 2004), pp. 55–155.
[36] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[37] I. Csiszár and J. Körner, IEEE Trans. Inf. Theor. **24**, 339 (1978).
[38] I. Devetak and A. Winter, Proc. R. Soc. London Ser. A **461**, 207 (2005).
[39] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[40] J. Lodewyck *et al.*, Phys. Rev. A **76**, 042305 (2007).
[41] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[42] C. S. Jacobsen, L. S. Madsen, V. C. Usenko, R. Filip, and U. L. Andersen, arXiv:1408.4566.
[43] M. Lassen, A. Berni, L. S. Madsen, R. Filip, and U. L. Andersen, Phys. Rev. Lett. **111**, 180502 (2013).
[44] R. Filip, L. Mišta, and P. Marek, Phys. Rev. A **71**, 012323 (2005).
[45] V. C. Usenko, L. Ruppert, and R. Filip, Phys. Rev. A **90**, 062326 (2014).
[46] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[47] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

Continuous-variable quantum key distribution with a leakage from state preparation

Ivan Derkach, Vladyslav C. Usenko, and Radim Filip
Published: *Physical review A* Vol. 96, Issue 24, 062309 (2017)
Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic

Following is an exact copy of the published article.

PHYSICAL REVIEW A **96**, 062309 (2017)

Continuous-variable quantum key distribution with a leakage from state preparation

Ivan Derkach,* Vladyslav C. Usenko,† and Radim Filip‡
Department of Optics, Palacky University, 17. listopadu 50, 772 07 Olomouc, Czech Republic
(Received 28 July 2017; published 7 December 2017)

We address side-channel leakage in a trusted preparation station of continuous-variable quantum key distribution with coherent and squeezed states. We consider two different scenarios: multimode Gaussian modulation, directly accessible to an eavesdropper, or side-channel loss of the signal states prior to the modulation stage. We show the negative impact of excessive modulation on both the coherent- and squeezed-state protocols. The impact is more pronounced for squeezed-state protocols and may require optimization of squeezing in the case of noisy quantum channels. Further, we demonstrate that the coherent-state protocol is immune to side-channel signal state leakage prior to modulation, while the squeezed-state protocol is vulnerable to such attacks, becoming more sensitive to the noise in the channel. In the general case of noisy quantum channels the signal squeezing can be optimized to provide best performance of the protocol in the presence of side-channel leakage prior to modulation. Our results demonstrate that leakage from the trusted source in continuous-variable quantum key distribution should not be underestimated and squeezing optimization is needed to overcome coherent state protocols.

DOI: 10.1103/PhysRevA.96.062309

I. INTRODUCTION

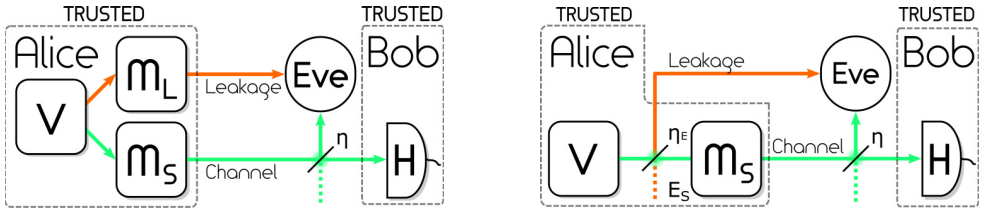
Any practical realization of quantum key distribution (QKD) (see [1] for reviews) deals with imperfections of real physical devices, which may be unaccounted in idealized security proofs. For example, it is well known that QKD systems based on direct photodetection [discrete-variable (DV) protocols] can be compromised by specific response of photodetectors to intense light, called blinding [2]. On the other hand, an eavesdropper can implement so-called Trojan horse attacks in order to get information about the modulator settings from the back-reflected light [3] or use state preparation and encoding flaws in DV QKD protocols [4,5] as well as benefit from information leakage, e.g., from auxiliary degrees of freedom of carrier states [6]. Continuous-variable (CV) QKD protocols (see [7] for reviews), based on the homodyne detection, can be robust against blinding, but are potentially vulnerable to other practical attacks, such as a wavelength attack on the homodyne detector [8] or continuous-variable counterpart of Trojan horse attacks [9].

Most of the practical attacks on the QKD devices can be in principle ruled out using device-independent realization of QKD [10] which, however, is very challenging (as it requires strongly entangled states and almost perfect detectors) and impractical, being limited to channels with high transmittance. There were also measurement-device independent (MDI) QKD protocols suggested and implemented, which rule out detector attacks [11], but keep the source potentially vulnerable, while still being limited mostly to highly transmitting channels in the case of CV QKD [12].

Another method to make QKD more robust against practical imperfections and, at the same time, efficient and stable in conditions of strongly attenuating and noisy channels, is to distinguish between trusted devices (such as source and detector) and untrusted channel (the latter being under full control of an eavesdropper), which can be done by proper set-up characterization. Trusted parties can then identify possible sources of side information available to an eavesdropper, and take them into account in security analysis. In the field of CV QKD this included consideration of already mentioned specific detection attacks [8,13], analysis of source imperfections [14–17], and role of multimode structure of state preparation and detection [18]. Trusted device imperfections may be under partial control of an eavesdropper so that an output of internal loss in a device may contribute to eavesdropper knowledge on the raw key though information leakage (side-channel loss) or so that the noise imposed by trusted device imperfections may be controlled by an eavesdropper to corrupt the data (side-channel noise). Such side channels, based on the basic linear coupling to vacuum or noisy modes, were previously considered on the detection and preparation sides of the protocol, assuming side-channel interaction after the modulation stage [19]. However, loss occurs as well on the stage of state preparation (e.g., it is well known that loss in the source reduces the level of squeezing [20]). On the other hand, modulation can be applied to many modes at once [18] and some of the modes may be directly accessible by an eavesdropper which may result in a zero-error security break similar to a photon-number-splitting attack in DV QKD [21] enabled by multiphoton generation in a signal source. Therefore, in the current paper we analyze side-channel leakage in the trusted station prior to modulation (side-channel attack on the signal states) and also consider multimode modulation such that the auxiliary modes are directly available to an eavesdropper.

In our study we assume basic linear passive coupling with the side channels; we also assume that the trusted parties can be aware of the side channel presence in the trusted source (e.g., by characterizing their devices prior to and during the protocol implementation using local measurements; otherwise the side channel loss would be attributed to the main untrusted channel), but are not able to remove them and stop the potential information leakage. We consider two main classes of CV QKD protocols, namely coherent-state and squeezed-state

*ivan.derkach@upol.cz
†usenko@optics.upol.cz
‡filip@optics.upol.cz



(a) Multimode modulation (b) Premodulation channel

FIG. 1. Prepare-and-measure CV QKD schemes with lossy channels and information leakage from state preparation stations (dashed boxes indicate trusted stations of Alice and Bob). Source V radiates Gaussian states (coherent or squeezed states) in the signal mode (green). States receive amplitude and phase displacements on modulator M_S, and are sent to Bob via quantum channel characterized by losses η. Signal states are measured on the receiver station by a homodyne detector H. (a) In addition to signal mode, the source generates additional leakage mode (orange line) L. States in the latter undergo displacement, correlated to the one of the main signal and characterized by modulation ratio k. An eavesdropper Eve can directly obtain information from an additional mode as well as from the quantum channel. The mode L is present due to the multimode structure of the source and cannot be technically eliminated. Generally an arbitrary amount of modes L_n can be modulated and leak, however, such a case can be reduced to a single effective mode L_{eff}. (b) A side-channel leakage (orange line) is present between state generation and state modulation stages. The initial signal state interacts with another state of mode E_S on a beam splitter with transmittance η_E, and only after that is being encoded with information on the modulator M_S. Eve can obtain information from E_S and quantum channels.

Gaussian protocols. We show that both multimode modulation and side-channel attack on the signal can undermine security of CV QKD protocols. Moreover, such attacks appear to be surprisingly more harmful for the squeezed-state protocol, once the channel noise is low. For more noisy channels and combination of side-channel imperfections the protocol implementation should be optimized to provide security and maximum performance.

The paper is structured as follows. In Sec. II we describe the mechanism of multimode modulation leakage, starting with the CV QKD model description and security analysis (Sec. II A) following with the description of consequences for coherent- and squeezed-state protocols under individual and collective attacks [22–25] and distinction between direct and reverse reconciliation (Sec. II B) [26,27]. In Sec. III we first describe the model and methods used for security analysis of the side-channel attack on the signal states (Sec. III A) and further characterize the impact of such an attack on the security of CV QKD protocols with direct and reverse reconciliation under individual and collective attacks (Sec. III B).

II. LEAKAGE FROM MULTIMODE MODULATOR

A. Security analysis

We examine the effect of the presence and consequent modulation of signal states in additional modes generated by the source on the preparation side of a generic Gaussian CV QKD protocol, illustrated in Fig. 1(a). Following the steps of a common CV QKD protocol [26,28] the trusted sender party prepares either coherent (using a laser source) or squeezed (using, e.g., the optical parametric oscillator) state characterized by the X or P quadrature (with both quadratures being interchangeable) value Q_S with zero mean and variance $V_S = \langle Q_S^2 \rangle - \langle Q_S \rangle^2$ (for the coherent-state protocol $V_S = 1$, while for the squeezed-state protocol signal quadrature variance $V_S < 1$, so that the uncertainty relation is maintained as $V_X V_P \geq 1$). Despite the state generated, Alice then applies both amplitude and phase quadrature modulation according to values Q_M from two independent Gaussian distributions, with variance $V_M = \langle Q_M^2 \rangle - \langle Q_M \rangle^2$, to the output mode of the source so that the state entering the untrusted quantum channel and sent to Bob is characterized by the quadrature value $Q_B = Q_S + Q_M$ and variance $V_B = V_S + V_M$.

The source used by the sender can have a multimodal structure but it is usually presumed that Alice fully controls all the output of the source. In this work we assume that the source in addition to the main mode, characterized by the quadrature value Q_S with variance V_S, can produce additional N leakage modes [Fig. 1(a), orange line], which are characterized by the quadrature values Q_{L_n} with respective variances V_{L_n}, that are not blocked or filtered by trusted parties. This results in amplitude and phase modulation being applied to the leakage modes as well. The signal state noise and modulation are trusted, but the leaking output is fully available to Eve.

Generally additional mode modulation V_{M,L_n} may differ from the modulation V_M applied to the signal mode, therefore we characterize the relation between them by the ratio $V_{M,L_n}/V_M = k$. If the $k = 0$ additional mode is not modulated at all, this results in the state with the initial quadrature value Q_{L_n}, while for $k < 1$ an additional mode receives a fraction of the signal modulation. Alternatively, leakage mode amplitude or phase quadrature displacements can correspond to a Gaussian distribution that has higher variance than that of the signal mode, corresponding to $k > 1$. In other words the encoding alphabet of the secondary mode can be bigger than that of the signal mode, however, excessive letters remain correlated to the signal alphabet. The signal state and the additional modulated state after the modulation are correlated as $C_{SL_n} = kV_M$, while leakage modes are correlated between each other as $C_{L_n L_m} = k^2 V_M$.

After the preparation stage the signal Q_B travels through the untrusted quantum channel (which is generally lossy and noisy, but for simplicity let us first consider the case of noiseless channel), where it is being measured by a homodyne detector. After the untrusted channel, Bob receives the state with quadrature values $Q'_B = (Q_S + Q_M)\sqrt{\eta} + Q_0\sqrt{1-\eta}$ with variance $V'_B = (V_S + V_M - 1)\eta + 1$, where Q_0 is a quadrature value of the vacuum state that is coupled to the

signal state in the channel and has variance $V_0 = \langle Q_0^2 \rangle - \langle Q_0 \rangle^2 = 1$. An eavesdropper, after the signal passes through the untrusted channel, is able to acquire and store mode E with $Q_E = -(Q_S + Q_M)\sqrt{1-\eta} + Q_0\sqrt{\eta}$ and variance $V_E = (V_S + V_M)(1-\eta) + \eta$, and additional source modes L_n ($n \in [1,N]$) with $Q'_{L_n} = Q_{L_n} + kQ_M$ with variance $V'_{L_n} = V_{L_n} + k^2 V_M$. After the signal state is transferred through the untrusted channel, initial correlations with the leakage mode are lowered by channel transmittance as $C'_{SL_n} = kV_M\sqrt{\eta}$.

To get analytical insights into the security of the protocol, and to understand basic limitations, we first study the case of individual attacks in a noiseless channel [as in Fig. 1(a)]. To purely see limitations by the leakage, we consider all data post-processing to be fully efficient. The lower bound on the secure key rate [29] under such attack is

$$R|^{\text{ind}}_{RR(DR)} = I_{AB} - I_{BE(AE)}, \tag{1}$$

where I_{XY} is the mutual information between respective parties, and DR and RR stand for direct reconciliation (when Alice is the reference side of error correction) and reverse reconciliation (when Bob is the reference side [25]), respectively. The state measured by an eavesdropper, can consist of $(N+1)$ modes, including the untrusted quantum channel. Multimode modulation does not change the mutual information between trusted parties, and it corresponds to the one in conventional single-mode prepare-and-measure (P&M) CV QKD protocols (binary logarithm indicates that units of information are bits) [17]:

$$I_{AB} = \frac{1}{2}\log_2\left[\frac{V_M}{V_M - \frac{\eta V_M^2}{\eta(V_S+V_M-1)+1}}\right]. \tag{2}$$

Eve's mutual information with the trusted side depends on the variance of the state of a trusted party conditioned by the measurements of all the modes, available to Eve, $V_{A(B)|E}$ for direct or reverse reconciliation, respectively. For any N leakage modes such a state can be reduced to $V_{A(B)|EL_{\text{eff}}}$, where E is obtained from propagation losses in the quantum channel and L_{eff} is the equivalent effective single-mode leakage. Second moments of the effective leakage mode in the signal quadrature and new effective modulation ratio can be, respectively, written as

$$V_{L_{\text{eff}}} = \frac{N}{\sum_n^N V_{L_n}^{-1}}, \tag{3}$$

$$k_{\text{eff}} = k\sqrt{N}. \tag{4}$$

In order to provide an extensive analysis of CV QKD protocols we examine the possible collective attacks that may be performed by Eve, resulting in the lower bound on the secure key rate given by

$$R|^{\text{col}}_{RR(DR)} = \beta I_{AB} - \chi_{BE(AE)}, \tag{5}$$

where β accounts for limited post-processing efficiency, mutual information I_{AB} remains the same as in Eq. (2), while the information obtainable by the untrusted party is upper limited by the Holevo bound $\chi_{BE(AE)}$ [30] in either reverse or direct reconciliation. In the limit of an infinite block size Eq. (5) also corresponds to the key rate under coherent attacks [31]. Under collective attacks Eq. (3) does not apply, however, second moments of the effective leakage mode can be found numerically. Nevertheless, provided that all L_n have the same initial variance V_L, and multimode modulator [M_L in Fig. 1(a)] outputs N leakage modes $V'_L = V_L + k^2 V_M$, the effective mode will have $V_{L,\text{eff}} = V_L$ with the modulation ratio (4). We will further consider only the case with one additional mode (L) keeping in mind that a more general situation can be reduced to the single-mode one. The equivalent entanglement-based CV QKD scheme, enabling purification-based security analysis in the case of collective attacks [17] corresponding to Fig. 1(a), due to the fact that a fraction of the correlated modulation leaked is unknown to trusted parties, is nontrivial. One way to find the solution is by applying the Bloch-Messiah reduction theorem [32] (for more details on security analysis see Appendix A).

B. Coherent- and squeezed-state protocols

Direct reconciliation. This reconciliation scheme, which is more suitable for short distance channels, being limited by $-3dB$ of loss, is extremely sensitive to the information leakage from the additional source mode. In the limit of ideal state propagation through the quantum channel used by trusted parties $\eta \to 1$, and symmetry of the variances $V = V_L = V_S$, the key rate (1) reads

$$R_{\text{DR}} \approx \frac{1}{2}\left(\frac{[\eta-1]V_M}{V\log[2]}\frac{(2k^2V_M+V)^2}{k^2V_M+V} + \log_2\left[\frac{V_M+V}{k^2V_M+V}\right]\right). \tag{6}$$

It is evident from Eq. (6) that even if the quantum channel is perfect ($\eta = 1$) for arbitrary values of signal modulation the security is lost if the secondary mode receives the same modulation as the signal mode ($k = 1$). In the absence of symmetry of variances $V_L \neq V_S$ excessive modulation can still lead to a security break even if input of the leaking modes are noisy coherent states with $V_L \geqslant 1$.

Reverse reconciliation. Again, assuming that all modes radiated by the source have the same variance $V = V_L = V_S$ in the limit of strong modulation ($V_M \to \infty$) the key rate (1) reads

$$R_{V_M\to\infty}|^{\text{ind}}_{RR} = -\frac{1}{2}\log_2\left[\left(1-\eta+\frac{\eta k^2}{V(1+k^2)}\right)\times(1+\eta[V-1])\right]. \tag{7}$$

If the leakage mode will be completely neglected trusted parties would underestimate Eve's knowledge about the key that will lead to the falsely estimated key rate:

$$R^{(\text{false})}_{V_M\to\infty}|^{\text{ind}}_{RR} = -\tfrac{1}{2}\log_2\{(1-\eta)[1+\eta(V-1)]\}. \tag{8}$$

While mutual information (2) between Alice and Bob remains the same in Eqs. (7) and (8), the cost of underestimation of mutual information $V_{B|E}$ between Bob and Eve is $-1/2\log_2\{(1-\eta)/(1-\eta+k^2\eta/[V(k^2+1)])\}$. Such cost for fixed k is the highest for short distance $\eta \to 1$ and high squeezing $V \to 0$, hence conditions which allow the high false key rate (8) will in fact be security breaking and yield a negative actual key rate (7).

The correlated modulation kV_M that leaks to the untrusted party makes the protocol sensitive not only to losses in the quantum channel η, but also to the initial state squeezing V and the state modulation V_M; security is always limited by the presence of the second source mode for $\eta < 1$. The more the squeezed initial state V is, the smaller the fraction of the modulation V_M is needed to be revealed to an eavesdropper to break the security of the protocol. In the limit of infinite squeezing $V \to 0$ for any nonzero modulation ratio k, the secure protocol cannot be established since the term contributing to Eve's information $k^2/[V(1+k^2)]$ in Eq. (7) approaches infinity, i.e., Eve is able to collect an accurate copy of the signal modulation directly from a leakage channel, without any attack on the main channel.

However, if the coherent-state protocol is used with $V = 1$, one can see from Eq. (7) that the secure key rate remains positive for any arbitrary amounts of correlated modulation leakage. For a long distance with small $\eta \ll 1$, we get always the positive secure key rate $\eta/(\ln 4(1+k^2))$. The key rate drops with longer distance, but never vanishes completely.

Equation (7) also allows one to assess the maximal tolerable $k_{\max}$ ratio for high signal-state modulation:

$$k_{\max}|_{V_M\to\infty} = \sqrt{\frac{V(\eta-2+V-\eta V)}{(\eta-1)(V-1)^2}}, \tag{9}$$

and immediately see that protocols can tolerate excess mode modulation with any ratio k as long as either $\eta = 1$ (quantum channel is perfect) or $V = 1$ (coherent-state protocol is used).

Given that at $V = k^2/(1+k^2)$ the key rate (7) becomes $R = -1/2\log_2[1-\eta+\eta k^2/(1+k^2)]$, and it is the same as when the coherent-state protocol is used ($V = 1$), therefore the amount of squeezing needed to reach improvement over the coherent-state protocol is independent of channel losses η and is bounded as

$$\frac{k^2}{1+k^2} < V < 1, \tag{10}$$

with squeezing that maximizes the key rate (7) being

$$V^{\text{opt}}|_{V_M\to\infty} = \sqrt{\frac{k^2}{1+k^2}}. \tag{11}$$

With the increase of the modulation ratio k it is clear from Eqs. (10) and (11) that the coherent-state protocol is optimal in this regime, however, for low k, the optimized squeezed state protocol can yield significantly higher secure key rates.

One has to address an important aspect of the CV QKD system with multimode modulation—the difference between states in signal and leakage modes. Generally if the effective leaking state is initially more squeezed than the signal ($V_L < V_S$) it is more beneficial for an eavesdropper. An opposite effect is true as well—if the leaking state is initially less squeezed ($V_L > V_S$), the tolerance of protocols to modulation leakage is significantly improved, however, security is still limited by the leakage. For fixed state variance V_L in the secondary source mode, optimal $V_S^{\text{opt}} < V_L$, provided $k < 1$, but $V_S^{\text{opt}} > V_L$ if $k > 1$.

If noise is present in the channel one has to consider an equivalent entanglement-based CV QKD scheme for security analysis [33]. Results obtained for the protocols in realistic conditions (limited post-processing efficiency β and noisy quantum channel, characterized by losses η and noise ε) under collective attacks complement the preceding results for individual attacks. For any nonunity β, the signal modulation V_M must be limited and optimized [34]. Leakage does have an impact on the optimal modulation value, but if the perfect post-processing algorithm ($\beta = 1$) is used, the key rate (5) as a function of the modulation V_M is still monotonically increasing. Despite the states in the signal V_S and leakage V_L modes the excessive modulation is security breaking.

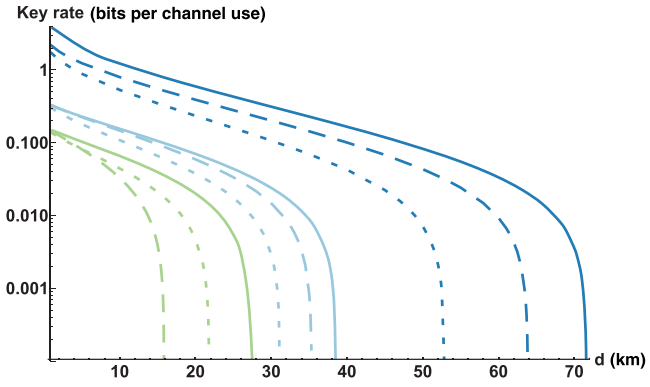


FIG. 2. Key rate (in bits per channel use) versus distance d (in kilometers) in a standard telecom fiber (with attenuation of $-0.2dB/km$) under collective attacks in the case of modulation leakage for different values of ratio between additional and signal state modulation variances $k = 0$ (blue, upper lines), 1 (light blue, middle lines), 1.5 (light green, lower lines) for optimized squeezed-state protocol (solid lines), squeezed-state protocol (dashed lines) with $V_L = V_S = 1/2$, and coherent state protocol with $V_L = V_S = 1$ (dotted lines). Modulation variance V_M is optimized for given parameters, excess noise $\varepsilon = 1\%$, post-processing efficiency $\beta = 97\%$. Evidently the distance is shortened by modulation leakage. Squeezing optimization allows one to achieve overall longer secure distances. Comparing unoptimized squeezing- and coherent-state protocols, the first one prevails under weak leakage $k \leq 1$, the latter under stronger leakage $k > 1$.

Let us look at the case when the source generates identical states into signal and leakage modes $V = V_L = V_S$. In terms of secure distance (Fig. 2), the protocol with broadly accessible squeezing [35] of signal states to $-3dB$ below the shot-noise unit (SNU) is able to prevail over the coherent-state protocol given the limited modulation ratio $k < 1$. On the other hand the coherent-state protocol is less sensitive to leakage and can be used on longer distances if the modulation ratio is higher, $k > 1$ (lower lines in Fig. 2). In fact, in such a regime even the noisy coherent-state protocol [15,36,37] can achieve a higher key rate than the squeezed-state protocol, provided excess noise ε in the channel is low enough.

However, in order to achieve best results under multimode modulation leakage with an arbitrary modulation ratio k, squeezing optimization is suggested. Optimal squeezing [similarly as in Eq. (11)] lowers with leakage increase, and approaches unity $V^{\text{opt}} \to 1$ for high k, e.g., in Fig. 2 optimal squeezing $V^{\text{opt}} < 1/2$ for $k = 0,1$ (upper and middle lines,

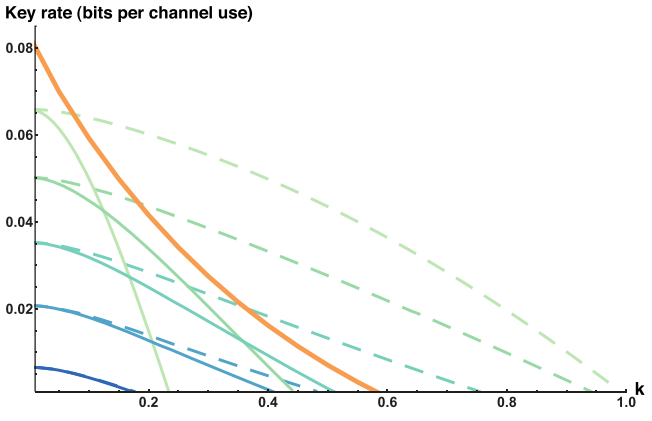


FIG. 3. Performance of the squeezed-state protocol with and leakage from the modulator under collective attacks. The coherent-state protocol, due to combined effects of modulation leakage, excess noise and limited post-processing efficiency, cannot be used for secure key generation at given parameters. Key rate dependency on the leaked modulation ratio k is shown for different values of squeezing (starting from top) V_S=0.1, 0.3, 0.5, 0.7, 0.9 SNU. All solid lines display the key rate with the symmetry of signal and leakage variances ($V_L = V_S$). The thick (orange) line illustrates the key rate of the protocol with both modulation V_M and signal squeezing V_S optimized. Dashed lines display the case when leakage mode input is fixed and independent of the signal ($V_L = 1$). Lowest solid and dashed lines, corresponding to $V_S = 0.9$, very nearly overlap. Signal modulation is optimized for given parameters. Reconciliation efficiency $\beta = 95\%$, channel losses $\eta = 0.1$, and excess noise $\varepsilon = 1\%$. Apparently the squeezed-state protocol is sensitive to leakage, especially for high squeezing. Provided that the source outputs identical states, security is broken when leakage is larger than half of the signal modulation. Robustness to leakage is higher if $V_L > V_S$, but leakage remains a security threat. Squeezing optimization (thick, orange line) heightens robustness and the key rate, but it's not sufficient to maintain security for arbitrary amounts of leakage.

respectively), while for $k = 1.5$ less squeezing is required $1 > V^{\text{opt}} > 1/2$ to achieve longer secure distance.

Squeezed-state protocol susceptibility to leakage is further illustrated in Fig. 3. Highly squeezed states are clearly more sensitive to leakage, but lower squeezing does not necessarily yield higher tolerance to leakage. Contrary to the case of purely lossy channels, where the coherent-state protocol has a nonvanishing key rate for an arbitrary modulation leakage, it may not always be suitable for secure key generation in noisy channels. The squeezed-state protocol remains sensitive even if states in the leakage mode have fixed variance $V_L =$ const and are independent of signal V_S (Fig. 3). Squeezing optimization in such a regime can still be effective, especially under strong leakage $k \gg 1$.

III. PREMODULATION LEAKAGE

A. Security analysis

In this section we will describe and examine another type of threat that may occur on a trusted preparation side of a Gaussian CV QKD system described in the beginning of the previous section (with absence of multimode modulation). Differently from the previous section, we now consider the presence of a channel between the source and modulator, modeled as linear coupling to a vacuum mode, as shown in Fig. 1(b). The signal generated by the source, with the quadrature value Q_S, prior to the modulation stage is linearly coupled to the mode E_S with the coupling ratio η_E. Signal states have zero mean of quadratures and variances $V_S = \langle Q_S^2 \rangle - \langle Q_S \rangle^2$, while states in the premodulation channel E_S are vacuum. During modulation (on modulator M_S) Alice applies displacement Q_M with $\langle Q_M^2 \rangle - \langle Q_M \rangle^2 = V_M$ to both quadratures of the signal states, resulting in a state $Q_B = Q_S\sqrt{\eta_E} + Q_{E_S}\sqrt{1-\eta_E} + Q_M$ with variance $V_B = \eta_E(V_S - 1) + V_M + 1$. Eve can gain information from states $Q'_{E_S} = Q_{E_S}\sqrt{\eta_E} - Q_S\sqrt{1-\eta_E}$ and $Q'_E = Q_E\sqrt{\eta} - (Q_S\sqrt{\eta_E} + Q_{E_S}\sqrt{1-\eta_E} + Q_M)\sqrt{1-\eta}$, obtained, respectively, from quantum and premodulation channels. After the signal passes through the purely lossy untrusted channel and arrives at the trusted receiver side its variance before measurement is

$$V'_B = [\eta_E(V_{X(P),S} - 1) + V_M]\eta + 1, \tag{12}$$

where η characterizes the loss rate in the transmitting channel. General correlations between Eve's states are described as

$$C_{E_S,E_C} = (V_S - V_{E_S})\sqrt{(1-\eta)(1-\eta_E)\eta_E}, \tag{13}$$

while correlations between the signal state and output of the premodulation channel are scaled by the transmittance in the quantum channel,

$$C_{B,E_S} = (V_{E_S} - V_S)\sqrt{\eta(1-\eta_E)\eta_E}. \tag{14}$$

Using the expressions above we can write the mutual information between Alice and Bob as

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_M}{V_M - \frac{V_M^2\eta}{V_M\eta + (V_S-1)\eta_E\eta + 1}}. \tag{15}$$

Similarly we can find the mutual information between Eve and the respective trusted reference side and apply Eq. (1) for analysis of individual attacks. For general analysis we adopt the recently introduced general purification scheme [19] and proceed with an estimation of the CV QKD protocol behavior under collective attacks Eq. (5) in noisy quantum channels.

B. Coherent- and squeezed-state protocols

The main aspect of the premodulation channel is that it provides correlations (14) with the signal to the external party and corrupts the initial carrier states (12). The influence of such a channel can be viewed as a preparation noise [15,17], however, it also provides an eavesdropper with additional correlations with the signal. Furthermore, the premodulation channel can be equivalent to side-channel leakage after the modulation stage, provided Q_M is scaled by $\sqrt{\eta_E}$ [19].

For $V_S = 1$, assuming the initial state in the mode E_S is a vacuum state ($V_{E_S} = 1$) we can immediately conclude that such a lossy channel would not affect the coherent-state protocol, since correlations (13) and (14) will totally vanish, and mutual information between trusted parties (15) will turn to a conventional form (2). In other words, the access to the lossy side channel would not provide the eavesdropper with any additional advantage if the coherent-state protocol is used.

For $V_S < 1$ and $V_{E_S} = 1$ the correlation arises and this case has to be analyzed in detail.

Direct reconciliation. The squeezed-state protocol is affected by the presence of the side channel between the source and modulator, since mutual information (15) diminishes, while information obtained by Eve (expressed in terms of mutual information or Holevo bound for respective attacks) increases. The lower bound on the key rate (1) in a perfectly transmitting channel can be expressed as

$$R|^{\mathrm{ind}}_{DR}|_{\eta\to 1} = \frac{1}{2}\log_2\left[1+\frac{V_M}{1+\eta_E(V_S-1)}\right]. \quad (16)$$

The presence of the premodulation channel lowers the overall key rate, however, secure key distribution is still possible for any side channel coupling ratio η_E.

Reverse reconciliation. Similarly the squeezed-state protocol key rate (1) will decrease due to the existence of the premodulation channel:

$$R|^{\mathrm{ind}}_{RR}|_{V_M\to\infty} = -\tfrac{1}{2}\log_2[(1-\eta)(1+\eta_E(V_S-1)\eta)], \quad (17)$$

though the key rate will still exceed the one for the coherent-state protocol. In the case of individual attacks and in the limit of high modulation ($V_M \to \infty$) the advantage of the squeezed-state over the coherent-state protocol is

$$\left(R|^{\mathrm{sq}}_{RR} - R|^{\mathrm{coh}}_{RR}\right)^{\mathrm{ind}}_{V_M\to\infty} = -\tfrac{1}{2}\log_2[1+\eta_E(V_S-1)\eta]. \quad (18)$$

The premodulation channel grants adversary correlations with the signal and they provide Eve an additional advantage, comparing to the case of preparation noise [15]. Such an advantage diminishes for low transmittance quantum channels and is the highest for $\eta \to 1$:

$$R_{E_S} - R_{\Delta V} = \frac{1}{2}\log_2\left[\frac{1+V_M+\eta_E(V_S-1)}{V_M+V_S/(\eta_E+V_S-\eta_E V_S)}\right]. \quad (19)$$

The correlation advantage $R_{E_S} - R_{\Delta V}$ quickly disappears for the high modulation ($V_M \to \infty$).

Considering the noisy quantum channel and equivalent entanglement-based system under collective attacks (see Appendix B) premodulation channel impact is similar to the previously described case of multimode modulation. The squeezed-state protocol is still superior to the coherent-state one in terms of the secure key rate (5) and tolerance to the channel noise. Squeezing optimization is not required as the key rate (5) linearly increases with an increase of squeezing. While the premodulation channel does not pose a security breaking threat, it can lower the secure distance (Fig. 4) and tolerance to the quantum channel excess noise ε. Even though correlations (14) help an adversary, the worst case scenario for trusted parties is substitution of the initial squeezed state by the coherent states ($V_S = 1$).

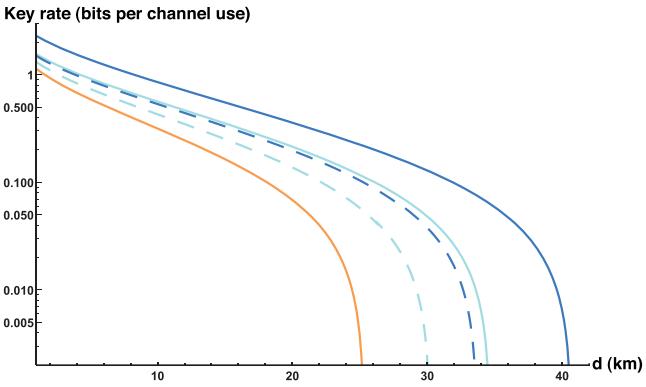


FIG. 4. The key rate (in bits per channel use) versus distance d (in kilometers) in a standard telecom fiber (with attenuation of $-0.2dB/km$) in the case of collective attacks on the coherent-state protocol (orange, lower line) and the squeezed-state protocol with $V_S = 1/10, 1/2$ (upper dark blue and middle light blue, respectively). The premodulation channel coupling ratio $\eta_E = 0.5$ (dashed lines) and 1, i.e., the absence of the channel (solid lines). Modulation variance is optimized for given parameters, $\beta = 97\%$, $\epsilon = 5\%$. Evidently the premodulation channel reduces the secure distance of the squeezed-state protocol. However, even small squeezing allows one to achieve longer distances. Maximal influence of the premodulation channel is set by the performance of the coherent-state protocol.

IV. CONCLUSIONS

We have investigated the negative impact of leakage from the trusted preparation side, namely, the correlated multimode modulation of nonsignal modes of the source and signal loss prior to the modulation stage. We have considered CV QKD coherent- and squeezed-state protocols with direct and reverse reconciliation. We have analyzed prepare-and-measure and equivalent entanglement-based models of leakage for cases of an illustrative individual and more general collective attacks in noisy channels.

Multimode modulation of nonsignal modes of the source limits the performance of both protocols and can lead to a security break even in the case of individual attacks in a purely lossy channel. Surprisingly, the coherent-state protocol can tolerate arbitrary amounts of leakage, though only in the noiseless channel. On the other hand, security of the squeezed-state protocol, with an increase of modulation leakage, quickly becomes compromised without the need for an untrusted party to resort to any additional manipulations onto the trusted side. We show that squeezing, however, can be optimized in order to improve the tolerance against multimode modulation leakage and channel noise. The optimized squeezed protocol then overcomes the coherent state protocol for any parameters.

The leakage from the preparation side prior to the modulation stage introduces noise to the squeezed signal and establishes correlations with an eavesdropper. While the coherent-state protocol is immune to such influence, the squeezed-state protocol suffers from secure key rate deterioration and becomes more sensitive to the excess noise in the channel. Nevertheless performance of the squeezed-state protocol surpasses the one of the coherent-state protocol, without the need for squeezing optimization.

Our results together with previous studies [14,19] describe the effects of the main possible mechanisms of information leakage from the trusted preparation side of continuous-variable quantum key distribution protocols, based on the most common linear passive coupling between optical modes. The results are stimulating for an experimental test of the macroscopically multimode protocols [38–41]. They may also stimulate analysis of side channels in MDI CV QKD protocols, where side-channel attacks on the source are, in principle, possible and therefore relevant similarly to the case of discrete-variable protocols [42].

ACKNOWLEDGMENTS

The authors acknowledge support from Project No. LTC17086 of the INTER-EXCELLENCE program of Czech Ministry of Education. I.D. acknowledges funding from Palacky University Project No. IGA-PrF-2017-008.

APPENDIX A: LEAKAGE FROM MULTIMODE MODULATOR

1. Multimode leakage

Using the initial values of quadrature variances of signal, leakage and untrusted channel modes (described in the main text), and input-output relations [for arbitrary modes 1 and 2 with quadrature vectors $\upsilon_i = (x_i, p_i)^T$],

$$\begin{pmatrix}\upsilon_1\\ \upsilon_2\end{pmatrix}_{\text{out}} = \begin{pmatrix}\sqrt{T}\mathbb{I} & \sqrt{1-T}\mathbb{I}\\ -\sqrt{1-T}\mathbb{I} & \sqrt{T}\mathbb{I}\end{pmatrix}\begin{pmatrix}\upsilon_1\\ \upsilon_2\end{pmatrix}_{\text{in}}, \tag{A1}$$

one can obtain the results of linear interactions in prepare-and-measure (P&M) multimode modulation scheme. Provided the source radiates modes with identical variance ($V_L = V_S$) and the untrusted channel is purely lossy,

$$\sigma_{B,LE} = \begin{pmatrix}\sqrt{\eta}kV_M & 0\\ 0 & -\sqrt{\eta}kV_M\\ -\sqrt{(1-\eta)\eta}(V_M+V_S-1) & 0\\ 0 & \frac{\sqrt{(1-\eta)\eta}(V_S-V_MV_S-1)}{V_S}\end{pmatrix}, \tag{A2}$$

$$\gamma_{LE} = \begin{pmatrix}V_Mk^2+V_S & 0 & -k\sqrt{1-\eta}V_M & 0\\ 0 & V_Mk^2+\frac{1}{V_S} & 0 & k\sqrt{1-\eta}V_M\\ -k\sqrt{1-\eta}V_M & 0 & V_M+V_S-\eta(V_M+V_S-1) & 0\\ 0 & k\sqrt{1-\eta}V_M & 0 & T+(1-\eta)\left(V_M+\frac{1}{V_S}\right)\end{pmatrix}, \tag{A3}$$

where $\sigma_{B,LE}$ (A2) describes correlations of Bob's mode B with channel E and leakage L modes, γ_{LE} is a covariance matrix of channel E and leakage mode L. The conditional covariance matrix can be obtained as

$$\gamma_{X|Y} = \gamma_X - \sigma_{Y,X}[\mathbf{X}\gamma_Y\mathbf{X}]^{\text{MP}}\sigma_{Y,X}^T, \tag{A4}$$

where $\mathbf{X} = \text{Diag}(1,0,0,0)$ and MP stands for Moore-Penrose pseudoinverse of the matrix [43]. Using Eq. (A4) and elements of matrices (A2) and (A3), as well as the matrix describing states received by Bob $\gamma_B = \text{Diag}([\eta(V_S+V_M-1)+1],0,0,[\eta(1/V_S+V_M-1)+1])$, one can find $V_{B|E} = V_{B|LE} = (V_M+k^2V_M+V_S)[\eta(k^2V_MV_S^{-1}+1)+(1-\eta)(V_M+k^2V_M+V_S)]^{-1}$. The latter can be used to assess Eve's mutual information with the trusted receiver side $I_{BE} = 1/2\log_2[V_B/V_{B|LE}]$, and consequently to find the key rate under individual attacks.

2. Purification

While P&M schemes can be used for illustration of modus operandi of protocols and basic security analysis, for an extensive analysis of Gaussian CV QKD protocols one has to consider an entanglement-based scheme [44]. The latter are based on usage of entangled sources that radiate two-mode Gaussian states described, in terms of covariance matrices, as

$$\gamma = \begin{pmatrix}V\mathbb{I} & \sqrt{V^2-1}\sigma_z\\ \sqrt{V^2-1}\sigma_z & V\mathbb{I}\end{pmatrix}, \tag{A5}$$

with V being the variance of each mode, $\mathbb{I}$ is a two-dimensional unity matrix, and σ_z is the Pauli matrix $\sigma_z = \text{Diag}(1,0,0,-1)$. Alice performs a homodyne or heterodyne detection (depending on the protocol intended for use) on one of the modes, thereby conditionally squeezing the other mode, resulting in states with quadrature variances $1/V$ and V or coherent states. The unmeasured and conditioned mode is a signal mode, that is sent through the untrusted quantum channel (characterized by losses η and excess noise ε) to Bob. This technique yields fully equivalent results to P&M schemes that prepare the signal state with the quadrature variance $V_S = 1/V$ (or $V_S = 1$ if Alice performs the heterodyne measurement), and subsequently apply Gaussian modulation of variance V_M.

The entanglement-based scheme with multimode modulation leakage should satisfy following conditions.

(1) Neither states sent by Alice nor states received by Bob nor correlations C_{AB} between them should be dependent on modulation (kQ_M, with variance k^2V_M) applied to states in the leakage mode.

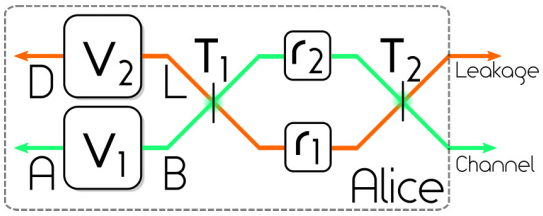


FIG. 5. Purification of modulation leakage ($N = 1$) on the preparation side of the Gaussian CV QKD protocol. Alice's side contains two EPR sources, radiating modes A, B with variance V_1, and modes D, L, with variance V_2. One mode from each source is kept on the preparation side (A,D) while the other two (B,L) interact on the beam splitter with transmittance T_1, undergo single-mode squeezing r_1 and r_2, respectively, and subsequently interact on the beam splitter with transmittance T_2. Signal mode B proceeds through the untrusted channel (η, ε) to Bob, while the L mode is accessible to Eve.

(2) The ratio between the leaking modulation and signal should be $k \geqslant 0$ and its values can exceed 1, since generally the variance of the modulation applied can be greater than that applied to the signal mode.

(3) The ratio k cannot be influenced by a trusted preparation party leaving only two parameters under Alice's control: signal modulation Q_M and amount of squeezing in the state Q_S produced by the source.

(4) The optical configuration should be scalable considering the fact that the trusted source can have an arbitrary multimodal structure.

One of the solutions that can satisfy all required conditions is provided by the Bloch-Messiah decomposition theorem [32], which says that the multimode evolution of an optical system governed by the linear Bogoliubov transformations can be decomposed into a combination of linear and nonlinear optical components (multiport interferometers and single-mode squeezers).

Let us consider the purification of two-mode modulation, i.e., the signal and leakage modes, as in Fig. 5. On the preparation side there are two sources; each generates a pair of entangled modes A,B and L,D, respectively. The states Q_A, Q_B (Q represents X or P quadrature) in modes A,B initially have a variance V_1, while states Q_L, Q_D in modes L,D have variance V_2. One mode from each source, e.g., B and L, interact on a beam splitter with transmittance T_1. The mode interaction effect on the covariance matrix γ_{ABLD} is given by input-output relations (A1).

Further, states in modes B and L are squeezed on individual single-mode squeezers (characterized by the squeezing parameter r_i), resulting in the change of state quadrature variance by e^{-2r_i} or e^{2r_i}. Subsequently modes interact, according to Eq. (A1), on the beam splitter with transmittance T_2. As a result the four-mode covariance matrix γ_{ABLD} after the interaction becomes γ'_{ABLD} and depends on six parameters: T_1,T_2,r_1,r_2,V_1,V_2. The elements of the covariance matrix γ'_{ABLD} can be used to form a set of equations:

$$\begin{aligned} V_{B(X)} &= -2t_1t_2e_-V_- + e^{-2r_1}T_2(T_1V_- + V_2) \\ &\quad + e^{-2r_2}(1-T_2)(V_1 - T_1V_-), \end{aligned}$$

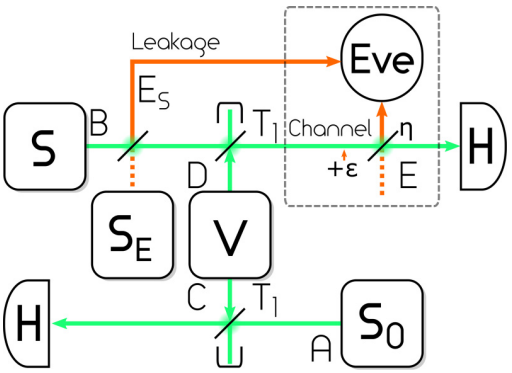


FIG. 6. Purification of the Gaussian CV QKD protocol with the side channel between source and modulation. Source S radiates signal (mode B) that, using entangled source V (modes C,D), receives amplitude and phase modulation, and is sent to Bob, that conducts homodyne detection H. Source S_0 (mode A) generates infinitely squeezed states that are kept on the preparation side. Source S_E (mode E_S) establishes correlations with, and provides Eve with information about signal (B). Losses η and noise ε in the untrusted channel (mode E) are attributed to Eve.

$$\begin{aligned} V_{B(P)} &= 2t_1t_2e_-V_- + e^{-2r_1}(1-T_2)(T_1V_- + V_2) \\ &\quad + e^{-2r_2}T_2(V_1 - T_1V_-), \\ V_{L(X)} &= -2t_1t_2e_+V_- + e^{2r_1}T_2(T_1V_- + V_2) \\ &\quad + e^{2r_2}(1-T_2)(V_1 - T_1V_-), \\ V_{L(P)} &= 2t_1t_2e_+V_- + e^{2r_1}(1-T_2)(T_1V_- + V_2) \\ &\quad + e^{2r_2}T_2(V_1 - T_1V_-), \\ C_{BL(X)} &= t_1(1-2T_2)e_-V_- + t_2(e^{-2r_2}(V_1 - T_1V_-) \\ &\quad - e^{-2r_1}(T_1V_- + V_2)), \\ C_{BL(P)} &= t_1(1-2T_2)e_+V_- + t_2(e^{2r_2}(V_1 - T_1V_-) \\ &\quad - e^{2r_1}(T_1V_- + V_2)),. \end{aligned} \tag{A6}$$

where $V_- = V_1 - V_2$, $t_{1(2)} = \sqrt{(1-T_{1(2)})T_{1(2)}}$, and $e_\pm = e^{\pm(r_1+r_2)}$. To find the solutions of Eq. (A6) one can substitute the left-hand side for the respective variances of states in the signal and leakage modes, and their covariances as follows: $V_{B(X)} \to V_S + V_M$, $V_{B(P)} \to 1/V_S + V_M$, $V_{L(X)} \to V_S + k^2V_M$, $V_{L(P)} \to 1/V_S + k^2V_M$, and $C_{BL(X)} \to kV_M$, $C_{BL(P)} \to -kV_M$. Solving Eq. (A6) for given k, V_S, V_M will yield numerical values of parameters T_1,T_2,r_1,r_2,V_1,V_2 and subsequently a numerical covariance matrix γ'_{ABLD} that can further be used to incorporate the effect of the untrusted quantum channel (η,ε) and analyze the security of the Gaussian coherent- or squeezed-state CV QKD protocol. The same approach can be used to purify cases of N mode leakage, however, N entangled sources are required, increasing the amount of parameters and equations in (A6) to $N(1+N)$.

APPENDIX B: PREMODULATION LEAKAGE

1. Pure losses

Let us now consider the generic CV QKD protocol (without the multimode modulator) and the presence of the channel between the source and the modulator. Results of linear interactions (A1) in the P&M scheme in the purely lossy channel can be described by

$$\sigma_{B,E_S E} = \begin{pmatrix} (1-V_S)\sqrt{\eta_E \eta(1-\eta_E)} & 0 \\ 0 & -\frac{1-V_S}{V_S}\sqrt{\eta_E\eta(1-\eta_E)} \\ (\eta_E - V_M - \eta_E V_S)\sqrt{(1-\eta)\eta} & 0 \\ 0 & (\eta_E - \frac{\eta_E + V_M V_S}{V_S})\sqrt{(1-\eta)\eta} \end{pmatrix}, \tag{B1}$$

$$\sigma_{E_S E} = \begin{pmatrix} (V_S-1)\sqrt{(1-\eta)(1-\eta_E)\eta_E} & 0 \\ 0 & \frac{(1-V_S)}{V_S}\sqrt{(1-\eta)(1-\eta_E)\eta_E} \end{pmatrix}, \tag{B2}$$

$$\gamma_E = \begin{pmatrix} \eta + (1-\eta)(V_M + \eta_E(V_S-1)+1) & 0 \\ 0 & \big(V_M + \eta_E(V_S^{-1}-1)+1\big)(1-\eta)+\eta \end{pmatrix}, \tag{B3}$$

$$\gamma_{E_S} = \begin{pmatrix} V_S + (1-V_S)\eta_E & 0 \\ 0 & \frac{1+\eta_E(V_S-1)}{V_S} \end{pmatrix}, \tag{B4}$$

where $\sigma_{B,E_S E}$ is the matrix describing Eve's correlations to the signal mode after premodulation leakage and losses, $\sigma_{E_S E}$ describes correlations between modes accessible to Eve, and the variances (in X and P quadratures) of the latter are given by γ_E and γ_{E_S}. One can use Eqs. (A4) and (B1)–(B4) to find the variance of Alice and Bob states conditioned by measurements of modes accessible to Eve:

$$V_{A|E} = \frac{V_S[V_M(1+(1-\eta)V_S)+V_S] + \eta_E(1-V_S)[\eta(V_M-V_S)+(1-\eta)V_M V_S]}{V_S[1-\eta+(1-\eta)V_M+\eta] + \eta_E(1-V_S)[(1-\eta)V_M+\eta]}, \tag{B5}$$

$$V_{B|E} = \frac{\eta_E V_M + V_S(V_M(1-\eta_E)+1)}{V_S[1+\eta_E(1-V_S)((1-\eta)V_M+\eta)+(1-\eta)V_M]}. \tag{B6}$$

Eve's mutual information with a trusted party $I_{AE} = 1/2\log_2[V_A/V_{A|E}]$, or $I_{BE} = 1/2\log_2[V_B/V_{B|E}]$ can be calculated using, respectively, Eq. (B5) or (B6) and further used to assess the key rate under individual attacks.

2. Purification

In the case of the side channel present between the source and the modulator, the purification can similarly be done using Bloch-Messiah decomposition (as in Appendix A 2), however, we adopt a general purification scheme as in Fig. 6 [19].

Alice on the preparation side operates an EPR source (A5) that radiates into modes C and D, source S that produces the signal state in mode B and source S_0 that produces the infinitely squeezed state in mode A. Modes produced by the EPR source have variance $V_M/(1-T_1)$ and are, respectively, coupled to modes from the other two sources on strongly unbalanced beam splitters T_1. The leakage is modeled as a signal interaction (A1) with the vacuum mode on a beam splitter with transmittance η_E. The signal further proceeds to the unbalanced beam splitter T_1 where it interacts with mode D that carries information and further is sent to the untrusted channel where it suffers from losses η and noise ε. Mode A carrying the infinitely squeezed state (to simulate the detection on the trusted side) interacts with first entangled mode C on another strongly unbalanced beam splitter characterized by the same value of transmittance T_1.

After the interactions, the state that is kept on the preparation side can be described by the variances as $V_{A(X)} = V_{S_0}T_1 + V_M$, $V_{A(P)} = T_1/(V_{S_0}) + V_M$, and the state that is sent to Bob through the untrusted channel as $V_B = (V_S\eta_E + (1-\eta_E)V_{E_1})T_1 + V_M$, while these two states are correlated as $C_{AB} = -\sqrt{(V_M^2 - (1-T_1)^2)\eta}$. In the limit $T_1 \to 1$ these correspond to the P&M scheme with the premodulation channel—generation of the signal state with variance V_S, the premodulation channel interaction with output accessible to Eve, and further amplitude and/or phase Gaussian modulation of variance V_M. The measurement conducted by Alice conditions Bob's state to $V_{B|A(X)} = T_1((1-\eta_E)V_{E_1} + \eta_E V_S) + \frac{(T_1-1)^2 - V_M^2}{T_1 V_0 + V_M} + V_M$, $V_{B|A(P)} = T_1((1-\eta_E)V_{E_1} + \frac{\eta_E}{V_S}) + \frac{V_0((T_1-1)^2 - V_M^2)}{T_1 + V_0 V_M} + V_M$. In the regime $T_1 = 1$, $V_0 = 1$, and $V_{E_1} = 1$, $\eta_E = 1$ states reduce to $V_{B|A(X)} = V_S$, and $V_{B|A(P)} = 1/V_S + V_M$ that corresponds to modulation with variance V_M applied to both quadratures of the signal state described initially by variances in respective quadratures V_S, $1/V_S$ with only one value (x) being kept. The resulting six-mode covariance matrix (including premodulation E_S and untrusted E channels) $\gamma_{ABCDE_S E}$ allows one to further analyze the security of the Gaussian coherent- or squeezed-state CV QKD protocol.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *ibid.* **81**, 1301 (2009); E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Information **2**, 16025 (2016).

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).

[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006); K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

[4] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004); K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014); F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, *ibid.* **92**, 032305 (2015).

[5] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010); C. Wang, S. Wang, Z.-Q. Yin, W. Chen, H.-W. Li, C.-M. Zhang, Y.-Y. Ding, G.-C. Guo, and Z.-F. Han, Opt. Lett. **41**, 5596 (2016); A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).

[6] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).

[7] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005); C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *ibid.* **84**, 621 (2012); E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).

[8] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 062329 (2013).

[9] B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, E. Diamanti, C. Marquardt, and G. Leuchs, in *2015 Conference on Lasers and Electro-Optics (CLEO)* (IEEE, Piscataway, 2015), pp. 1–2.

[10] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[11] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012); H.-K. Lo, M. Curty, and B. Qi, *ibid.* **108**, 130503 (2012).

[12] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics **9**, 397 (2015).

[13] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **87**, 052309 (2013).

[14] R. Filip, Phys. Rev. A **77**, 022310 (2008).

[15] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).

[16] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).

[17] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).

[18] V. C. Usenko, L. Ruppert, and R. Filip, Phys. Rev. A **90**, 062326 (2014).

[19] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **93**, 032309 (2016).

[20] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Phys. Rev. Lett. **117**, 110801 (2016).

[21] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[22] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).

[23] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[24] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[25] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

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

[27] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[28] N. J. Cerf, M. Lévy, and G. VanAssche, Phys. Rev. A **63**, 052311 (2001); P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photonics **7**, 378 (2013).

[29] I. Devetak and A. Winter, in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, Vol. 461 (The Royal Society, London, 2005), pp. 207–235.

[30] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[31] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).

[32] S. L. Braunstein, Phys. Rev. A **71**, 055801 (2005).

[33] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[34] 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, Phys. Rev. A **76**, 042305 (2007); V. C. Usenko and R. Filip, New J. Phys. **13**, 113007 (2011).

[35] U. L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, Phys. Scr. **91**, 053001 (2016).

[36] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).

[37] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

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

[39] T. Iskhakov, M. V. Chekhova, and G. Leuchs, Phys. Rev. Lett. **102**, 183602 (2009); T. S. Iskhakov, V. C. Usenko, R. Filip, M. V. Chekhova, and G. Leuchs, Phys. Rev. A **93**, 043849 (2016).

[40] A. Christ, C. Lupo, and C. Silberhorn, New J. Phys. **14**, 083007 (2012); G. Harder, C. Silberhorn, J. Rehacek, Z. Hradil, L. Motka, B. Stoklasa, and L. L. Sánchez-Soto, Phys. Rev. A **90**, 042105 (2014).

[41] O. Pinel, P. Jian, R. M. de Araujo, J. Feng, B. Chalopin, C. Fabre, and N. Treps, Phys. Rev. Lett. **108**, 083601 (2012); J. Roslund, R. M. De Araujo, S. Jiang, C. Fabre, and N. Treps, Nature Photonics **8**, 109 (2014).

[42] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Phys. Rev. A **92**, 022304 (2015).

[43] R. Penrose, in *Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 51 (Cambridge University Press, Cambridge, 1955), pp. 406–413.

[44] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).

Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels

Vladyslav C. Usenko[1], Christian Peuntinger[2,3], Bettina Heim[2,3,4], Kevin Günthner[2,3], Ivan Derkach[1], Dominique Elser[2,3], Christoph Marquardt[2,3], Radim Filip[1], and Gerd Leuchs[2,3]

Published: *Optics Express* Vol. 26, Issue 24, pp. 31106-31115 (2018)

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

2) Max-Planck-Institut für die Physik des Lichts, Staudtstr. 2, 91058 Erlangen, Germany

3) Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany

4) Currently at OHB System AG, Manfred-Fuchs-Str. 1, 82234 Oberpfaffenhofen, Germany

---

Following is an exact copy of the published article.

Research Article | Vol. 26, No. 24 | 26 Nov 2018 | OPTICS EXPRESS 31106
Optics EXPRESS

Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels

VLADYSLAV C. USENKO,[1,*] CHRISTIAN PEUNTINGER,[2,3] BETTINA HEIM,[2,3,4] KEVIN GÜNTHNER,[2,3] IVAN DERKACH,[1] DOMINIQUE ELSER,[2,3] CHRISTOPH MARQUARDT,[2,3] RADIM FILIP,[1] AND GERD LEUCHS[2,3]

[1]*Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2]*Max-Planck-Institut für die Physik des Lichts, Staudtstr. 2, 91058 Erlangen, Germany*
[3]*Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*
[4]*Currently at OHB System AG, Manfred-Fuchs-Str. 1, 82234 Oberpfaffenhofen, Germany*
[*]*usenko@optics.upol.cz*

Abstract: Transmittance fluctuations in turbulent atmospheric channels result in quadrature excess noise which limits applicability of continuous-variable quantum communication. Such fluctuations are commonly caused by beam wandering around the receiving aperture. We study the possibility to stabilize the fluctuations by expanding the beam, and test this channel stabilization in regard of continuous-variable entanglement sharing and quantum key distribution. We perform transmittance measurements of a real free-space atmospheric channel for different beam widths and show that the beam expansion reduces the fluctuations of the channel transmittance by the cost of an increased overall loss. We also theoretically study the possibility to share an entangled state or to establish secure quantum key distribution over the turbulent atmospheric channels with varying beam widths. We show the positive effect of channel stabilization by beam expansion on continuous-variable quantum communication as well as the necessity to optimize the method in order to maximize the secret key rate or the amount of shared entanglement. Being autonomous and not requiring adaptive control of the source and detectors based on characterization of beam wandering, the method of beam expansion can be also combined with other methods aiming at stabilizing the fluctuating free-space atmospheric channels.

1. Introduction

The development of experimental quantum optics in the past decades led to the emergence and tremendous progress in the field of quantum information, which studies the possibility to store, transmit and process information encoded into quantum states. Quantum communication, a particular application of quantum information processing, is very naturally suggested by the long coherence time and relatively low coupling to the environment which is typical for optical quantum states. This allows one to use quantum states of light for quantum communication, particularly for sharing a quantum resource (such as entanglement) to connect quantum devices, or for quantum key distribution (QKD), aimed at securely distributing random secret keys between two legitimate parties. The methods of QKD are called protocols and were first suggested on the basis of strongly nonclassical systems such as single photons or entangled photon pairs [1]. Later the natural use of continuous-variable (CV) [2] quantum states of light was suggested [3]. This resulted in the development of CV QKD protocols and methods to produce, characterize and

#341501 https://doi.org/10.1364/OE.26.031106
Journal © 2018 Received 10 Aug 2018; revised 30 Sep 2018; accepted 3 Oct 2018; published 12 Nov 2018

Optics EXPRESS

share CV entanglement.

CV QKD protocols are typically based on the use of Gaussian quadrature-modulated coherent [4,5] or squeezed states [6,7] of light and homodyne detection at the receiving station. Equivalently, quadrature-entangled states and homodyne detection at both the sending and the receiving stations can be used [8]. The security of Gaussian CV QKD protocols [9] was shown against general attacks in the asymptotic regime [10] and against collective attacks in the finite-size regime [11,12] based on the optimality of Gaussian attacks [13–15]. This approach allows to broadly study the security of the protocols using covariance matrices, which explicitly characterize Gaussian states of light [16]. Gaussian CV QKD protocols were well studied and successfully implemented in long-distance fiber links [5, 17, 18], where the transmittance is typically stable and the added channel excess noise is extremely low. On the other hand, atmospheric quantum channels, which are of utmost importance for long-distance satellite communication [19] or free-space terrestrial communication waiving the requirement of necessity of fiber-optical infrastructure, are typically inclined to transmittance fluctuations due to turbulence effects [20–22], also affected by weather conditions [23]. Such transmittance fluctuations (also referred to as channel fading) were analyzed in their impact on applicability of CV quantum communication in the case of atmospheric turbulence [24–27] and uniform transmittance fluctuations [28]. It was shown that channel fading can be destructive to CV QKD protocols and limit the possibility to share CV entangled states. The main reason for this is that the transmittance fluctuations lead to additional excess noise appearing in the variances of the quadrature measurement results [24]. Such fading-related excess noise is proportional to the variance of the transmittance fluctuations and the overall variance of the quadrature distributions in the quantum signal. Therefore in order to allow CV QKD or quantum resource sharing over a fluctuating channel the stabilization of the channel transmittance can be advantageous as a feasible alternative to channel post selection [24] or entanglement distillation [29, 30]. In the case of mid-range atmospheric optical channels, the transmittance fluctuations are typically caused by beam wandering, when the beam spot is randomly traveling around the receiving aperture [31], in addition to such turbulence effects, as, e.g., scintillation, phase degradation of the wave front, and beam spreading. The transmittance fluctuations caused by beam wandering are then governed, in particular, by the ratio between the beam size and the size of the aperture [32]. It was suggested that an increase of this ratio would naturally stabilize the channel and make it more suitable for quantum communication tasks [24], similarly to optimization of the beam spot size for given channel parameters in classical free-space optical communication [33, 34].

In the present paper we discuss the method of beam expansion, aimed at compensating the channel fluctuations caused by beam wandering, in detail for CV quantum communication tasks, where the signal intensity is drastically limited compared to the classical free-space optical communication. We report the experimental test of the method based on the spatial expansion of the beam and the subsequent characterization of the channel transmittance. We show that the fading can be indeed stabilized and the variance of transmittance fluctuations (and, subsequently, quadrature excess noise) can be substantially reduced at the cost of increase of the overall loss of the channel. This leads to the trade-off between channel stabilization and its applicability to entanglement sharing or CV QKD. Therefore the suggested method of channel stabilization should be optimized to reach maximum key rate or secure distance for CV QKD or maximum shared entanglement in practical quantum applications.

2. Fading due to beam wandering in CV quantum communication

The most feasible CV quantum communication and QKD protocols are based on Gaussian states and operations [16]. It is well known that Gaussian states and their properties are explicitly described by the first and the second moments of the field quadrature operators, which can be introduced through the mode's quantum operators as $x = a^\dagger + a$ and $p = i(a^\dagger - a)$, i.e.

Optics EXPRESS

by the mean values $\langle x \rangle$, $\langle p \rangle$ and by the covariance matrix γ of the elements of the form $\gamma_{i,j} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$, where $r_i = \{x_i, p_i\}$ is the quadrature vector of the i-th mode. It was shown that channel fading leads to excess noise in the quadrature variance, which is proportional to the variance of the channel fluctuations and the variance of the state propagating through the channel [30] such that the variance of a quadrature on the output of a purely attenuating fading channel becomes $V'_{r_i} = 1 + \langle \sqrt{\eta} \rangle^2 (V_{r_i} - 1) + \epsilon_{f_i}$. Here $\langle \sqrt{\eta} \rangle$ is the mean channel transmittance and $\epsilon_{f_i} = Var(\sqrt{\eta})(V_{r_i} - 1)$ is the excess noise due to fading, which depends on the variance of the transmittance fluctuations $Var(\sqrt{\eta}) = \langle \eta \rangle - \langle \sqrt{\eta} \rangle^2$ and the r_i-quadrature variance V_{r_i} of the source. Noise due to fading is therefore generally phase-sensitive, but we further, with no loss of generality, assume phase-space symmetry of the considered states, having variance $V_{r_i} = V : \forall i$ in any quadrature, and subsequent phase independence of the noise $\epsilon_f = Var(\sqrt{\eta})(V - 1)$. This noise reduces and possibly destroys the entanglement of a Gaussian state shared over a fading channel and as well decreases the secret key rate of the Gaussian CV QKD. It can lead to loss of security in CV QKD [24], i.e., turning the key rate to zero. The effect is more pronounced for stronger transmittance fluctuations, lower mean channel transmittance and larger initial state variance V.

One of the main causes of transmittance fluctuations in an atmospheric channel is beam wandering [31], when the optical beam moves around the aperture of the receiving detector and becomes clipped. It was studied for transmission of quantum states of light for which the transmittance distribution was shown to be governed by the log-negative Weibull distribution, cut at a certain value of transmittance η_0 [32, 35]. The distribution is then given by the scale and shape parameters, expressed by the beam-center position variance σ_b^2 and the ratio a/W of the aperture radius a and the beam-spot radius W so that the maximum transmittance is defined by $\eta_0^2 = 1 - exp[-2(a/W)^2]$. The beam-spot fluctuations variance σ_b^2 is related to the Rytov parameter [36], defining the turbulence strength, which can be obtained from the atmospheric structure constant of refractive index C_n [37]. The latter, however, was not directly measured in our experiment and further we describe the beam-spot fluctuations by the variance σ_b^2. It was naturally predicted that the expansion of the beam i.e. the decrease of the ratio a/W would result in a stabilization of the channel transmittance at the cost of a decrease of the mean transmittance [24], a technique also used in classical optical communication [33, 34]. In our research we verify and confirm this conjecture and study the effect of beam expansion on the channel properties, the efficiency of sharing quantum entanglement and on the security of CV QKD through a fading channel.

3. Experimental set-up and results

The possibility to stabilize the fading channel by expanding the beam was studied in a real-world scenario in the city of Erlangen. The used point-to-point free-space channel of 1.6 km length connects the building of the Max Planck Institute for the Science of Light with the building of the computer sciences of the Friedrich-Alexander-University Erlangen-Nürnberg. We use a grating stabilized continuous wave diode laser with a wavelength of $\lambda = 809$ nm. The mode of this laser is cleaned using a single mode fiber before the beam is expanded using a telescope (see Fig 1). The beam is then sent through the fading free-space channel to Bob. At Bob we use an achromatic lens with a diameter of $a = 150$ mm and a focal length of 800 mm, which defines our aperture. The beam width of the received beam, i.e. the aperture-to beam size ratio a/W, can be adjusted with the sender telescope. A PIN photodiode detector (bandwidth 150 kHz) is used to measure the fluctuating transmittance of the channel. To estimate the beam width at Bob we use a CCD camera and a screen. No adaptive strategy has been used at Bob's station or between Alice and Bob. The profiles of the transmittance distributions for different beam expansion settings that illustrate the change of the statistics of the channel fading are given in Fig. 2. The transmittance data was analyzed to obtain the mean values of transmittance $\langle \eta \rangle$ and $\langle \sqrt{\eta} \rangle$, and the resulting

Optics EXPRESS

Fig. 1. A schematic view of the experimental set-up. At the sender Alice we use a telescope to expand the beam and adjust its beam width. Subsequently the beam is sent through our 1.6 km free-space link to the receiver Bob. There we use an achromatic lens with a diameter of $a = 150$ mm and measure the fluctuating transmission using a PIN photodiode detector and an analogue-to-digital converter. To estimate the aperture-to-beam size ratio we use a CCD camera and a screen.

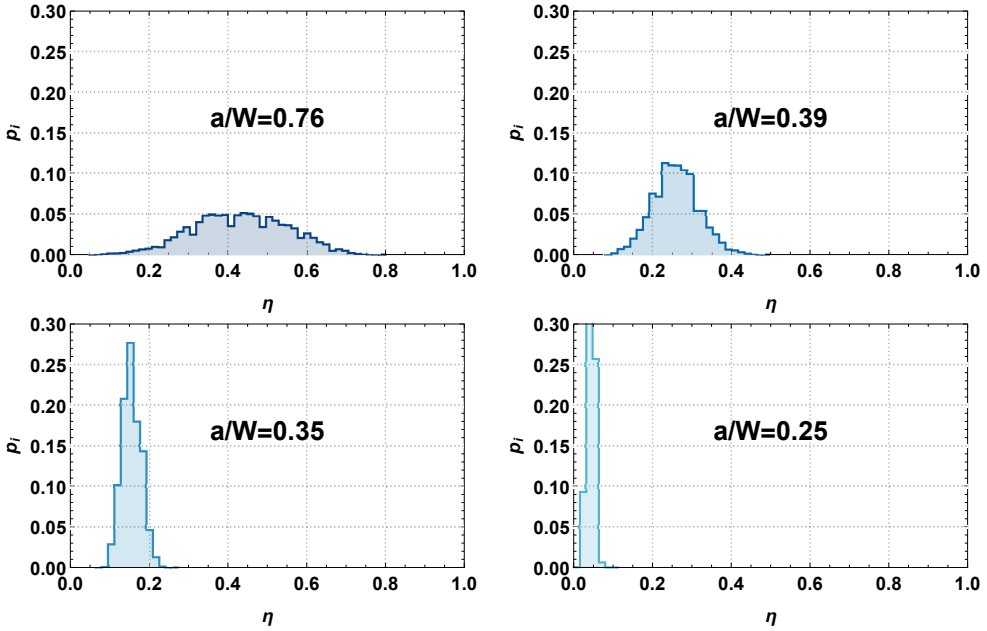


Fig. 2. Transmittance distribution profiles for different aperture-to-beam size ratios as indicated at the plots.

variance $Var(\sqrt{\eta})$, which governs the evolution of a covariance matrix after propagating through the fading channel. The results are given in Fig. 3 along with the values, obtained from the analytical Weibull distribution for the beam-spot fluctuation variance of $\sigma_b^2 = 0.3$, which is set so in all the subsequent calculations except for these, resulting in the plots in Fig. 5. The results of calculations from the experimentally obtained data demonstrate qualitatively the same tendencies with the decrease of the aperture-to-beam size ratio as the theoretical prediction: it is clearly visible from the plots that the expansion of the beam (i.e., decrease of the aperture-to-beam size ratio) reduces the fluctuations of the transmittance and at the same time reduces the average transmittance of the channel. In order to clarify the effect of the channel stabilization by the beam expansion on the quantum communication and quantum resource sharing we apply the

Optics EXPRESS

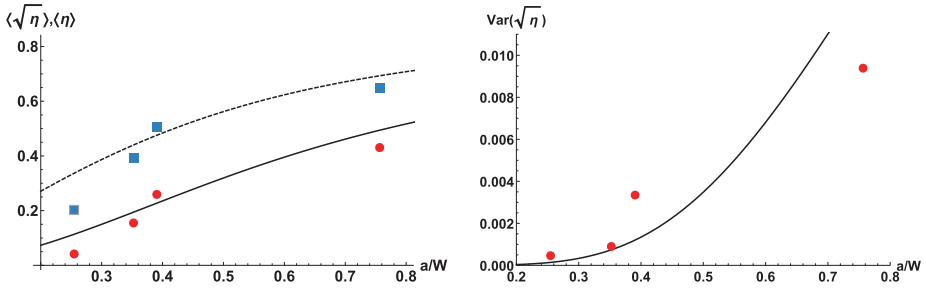


Fig. 3. Characteristics of atmospheric fading channel for larger beam expansion characterized by decreasing aperture-to-beam size ratio a/W. (Left): mean values $\langle\eta\rangle$ (lower solid black line) and $\langle\sqrt{\eta}\rangle$ (upper dashed grey line) estimated from the analytical Weibull distribution along with the experimental results (squares and circles respectively) and (right): variance $Var(\sqrt{\eta})$ of the square root of transmittance from the experimental characterization of the channel (points) and from the analytical estimates (solid line) versus aperture-to-beam size ratio.

obtained characteristics of the channel to these applications in the next section.

4. Effect of beam expansion on entangled resource sharing and CV QKD

Before we analyze the applicability of channel stabilization by beam expansion for CV QKD, we first study the impact of the method on the entanglement of a typical two-mode Gaussian entangled state, namely two-mode squeezed vacuum [16], shared over a fading channel. We characterize the entanglement of the state using the logarithmic negativity [38], defined as

$$LN = \max\{0, -\log_2 \nu\}, \tag{1}$$

where ν is the smallest symplectic eigenvalue of a covariance matrix of a partially transposed state for a pair of modes (see [16] for review on covariance matrix formalism for Gaussian states). We evaluate the logarithmic negativity for a state quadrature variance of $V = 7$ shot-noise units (SNU, being the variance of the vacuum fluctuations), corresponding to approximately -8 dB of conditionally prepared quadrature squeezing after a homodyne detection on one of the beams, which is feasible with current technology [39] and is close to optimum for the given protocol parameters, in the presence of 1% SNU of excess noise (here and further the fixed channel excess noise is related to the channel input). The results of the calculations are given in Fig. 4 (left) obtained from the experimental data and from the analytical fading distribution. It is clear from the graphs that the channel for the non-expanded beam was more suitable for entanglement distribution and that the beam expansion degraded the entanglement due to increase of the overall loss. The reason for such behavior is that in the considered region of parameters Gaussian entanglement is more sensitive to the channel transmittance than to the small amount of excess noise caused by fading. The transmittance fluctuations in the studied channels were relatively low and did not introduce significant noise, which would reduce the Gaussian entanglement of the states, while decreasing the average transmittance due to beam expansion resulting in entanglement degradation.

We also analyze the effect of the beam expansion on the typical CV QKD protocol with coherent states of light and homodyne detection by theoretically estimating the lower bound on the key rate secure against collective attacks [40] in a given channel, which, in the reverse reconciliation scenario (being robust against channel attenuation below -3 dB [5]), is given by

$$KR = \beta I_{AB} - \chi_{BE}, \tag{2}$$

Optics EXPRESS

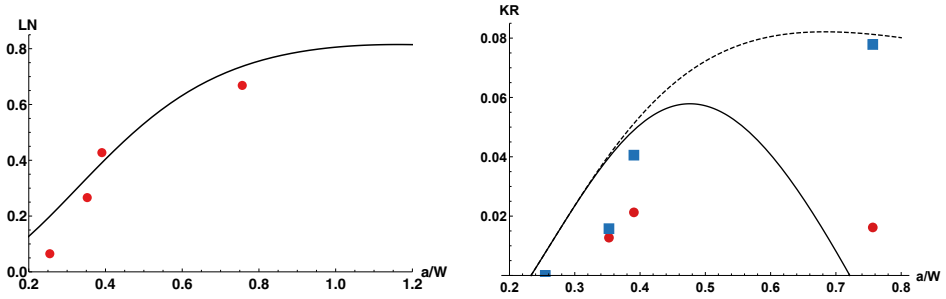


Fig. 4. Entanglement and secure key rate for larger beam expansion characterized by decreasing aperture-to-beam size ratio a/W. (Left): Logarithmic negativity of an entangled state shared over the fading channel and (Right) Lower bound on the key rate secure against collective attacks in the fading channel, obtained from the analytical fading distribution (lines) along with the experimental results (points) versus aperture-to-beam size ratio. State variance is 7 SNU (solid black line, red circles) or optimized (dashed black line, blue squares), channel excess noise is 1% SNU, post-processing efficiency for the Gaussian CV QKD is 97%.

where I_{AB} is the classical (Shannon) mutual information between the trusted parties, χ_{BE} is the Holevo bound on an information on the shared key received by the remote party, which is available to an eavesdropper, $\beta \in (0, 1)$ is the post-processing efficiency, which characterizes how close the trusted parties are able to reach the mutual information I_{AB}. In our analysis we follow the purification-based method (see [41] for the details of security analysis) to calculate the Holevo bound [42] and take into account the realistic post-processing efficiency of 97% [43]. The results of the calculations are given in Fig. 4 (right) and clearly show the improvement of the key rate due to the stabilization of the fading channel with a small beam expansion upon fixed modulation, which, however, becomes disadvantageous upon the further increase of the beam spot. We therefore confirm the positive effect of the beam expansion in the fading channel on the CV QKD, which, however, can be optimized in the particular conditions. For Gaussian entanglement distribution or for the coherent-state CV QKD protocol with optimized modulation the method would have been useful for a stronger channel turbulence. The positive role of fading stabilization for the optimized CV QKD upon stronger turbulence is theoretically predicted in Fig. 5, where the lower bound on the key rate is plotted versus the beam expansion settings at different values of beam-spot fluctuations. It is evident from the plot, that the experimentally tested beam expansion settings would have been advantageous for the optimized protocol at $\sigma_b^2 = 0.4$ (note that in our previous study of the same channel upon stronger turbulence the beam-spot fluctuations variance was estimated as $\sigma_b^2 = 0.36$ [24]).

Despite evident differences in the effect of beam expansion on the considered quantities (namely logarithmic negativity and key rate) as shown in Fig. 4, we theoretically observe a similar behavior of logarithmic negativity at higher values of a/W ratio (out of the experimentally tested and plotted region). Indeed, the logarithmic negativity also has a local maximum at certain ratio a/W (depending on the variance V), similarly to the key rate, and would decrease for higher values of the ratio. The difference is however that the key rate is more sensitive to channel fluctuations due to beam wandering and we therefore observed an improvement of the channel parameters by means of beam expansion for the application of CV QKD. Moreover, entanglement is not vanishing completely at high a/W for moderate initial entanglement corresponding to a variance of $V < 15$. To complete our study, we numerically illustrate the behavior of the logarithmic negativity and the lower bound on the secure key rate with respect to ratio a/W in the given channel for different initial resources in Fig. 6. We characterize the initial resource

Optics EXPRESS

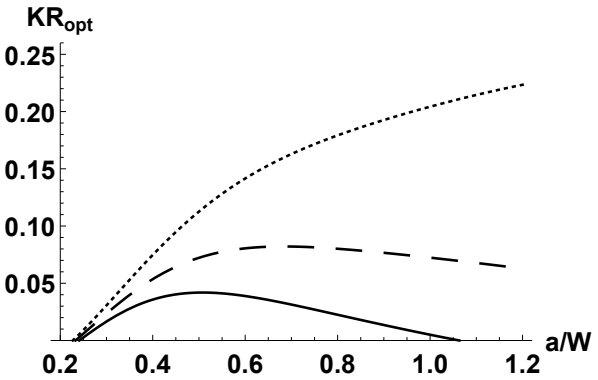


Fig. 5. Lower bound on the key rate secure against collective attacks in the fading channel, obtained from the analytical fading distribution, versus aperture-to-beam size ratio at $\sigma_b^2 = 0.2$ (upper, dotted line),$\sigma_b^2 = 0.3$ (middle, dashed line), $\sigma_b^2 = 0.4$ (lower, solid line) upon optimized modulation variance, channel excess noise is 1% SNU, post-processing efficiency is 97%.

by the state variance V for the key rate plot or, equivalently, by the initial entanglement of the shared state, which reads $LN_0 = (-1/2)\ln(2V^2 - 1 - 2V\sqrt{V^2 - 1})$ for the logarithmic negativity plot, to verify how much of the initial entanglement survives in a fading channel. It is evident from the plots that beam expansion in the considered channel can have positive effect on the key rate practically for any modulation and on the entanglement once the initial entanglement and beam-to-aperture ratio are large. In our study we considered the most feasible coherent-state

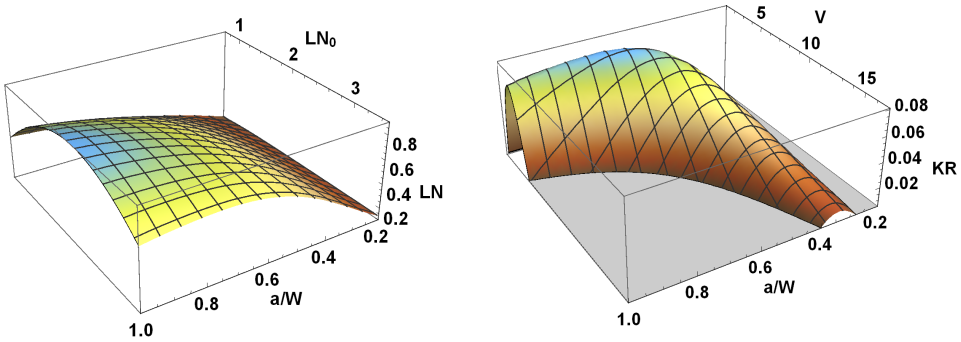


Fig. 6. Entanglement and secure key rate versus aperture-to-beam size ratio a/W at different initial resources. (Left): Logarithmic negativity (LN) of an entangled state shared over a fading channel versus aperture-to-beam size ratio and initial logarithmic negativity LN_0 and (Right) Lower bound on the key rate (KR) secure against collective attacks in the fading channel versus aperture-to-beam size ratio and modulated state variance V. Channel excess noise is 1% SNU, post-processing efficiency for the Gaussian CV QKD is 97%.

CV QKD protocol. While squeezed-state protocol is known to be typically more robust against channel transmittance fluctuations, its performance is still degraded by fading, related to beam wandering [44], so the beam expansion technique can be useful for the squeezed-state protocols as well and should be optimized in the given conditions.

Optics EXPRESS

5. Conclusions

We studied the possibility to stabilize a real fading channel by expanding the beam in order to suppress the transmittance fluctuations concerned with the beam wandering in turbulent atmosphere. We experimentally characterized the change of statistics of the channel transmittance fluctuations and showed that they qualitatively correspond to the theoretical predictions given by the Weibull distribution. We proved the positive effect of the channel stabilization by beam expansion on the distribution of a nonclassical resource (entanglement) and on Gaussian continuous-variable quantum key distribution. We have shown that for the channel used for the experimental results presented here beam expansion could become disadvantageous for Gaussian entanglement of the distributed state, described by the logarithmic negativity, due to weak atmospheric turbulence. On the other hand, channel stabilization by beam expansion can improve the secret key rate of the coherent-state protocol. The improvement requires an optimization of the beam width setting under given conditions. Importantly, the method does not require any adaptive control of the source and detector based on monitoring of the beam wandering. It can be combined with other known methods for fading channel stabilization such as fast steering [45] or concave mirrors [46], channel diversity [47, 48], multiple wavelengths [49], adaptive optics and active tracking systems [50–54]. It should be emphasized that our technique requires a link which allows for a certain margin in the loss tolerance. Especially for satellite links the loss is usually already very high as the aperture-to-beam size is very low, such that our stabilization technique will hardly have any benefit. But our proposed technique can be beneficial in mid-range terrestrial free-space links, what would be the field of application for this stabilization technique. Our result therefore demonstrates a promising and feasible method to stabilize free-space atmospheric channels for the tasks of continuous-variable quantum key distribution and quantum communication, which is best applicable in low or medium loss regime. Future steps will include full implementation of continuous-variable quantum key distribution and entanglement sharing over free-space atmospheric channels aided by channel stabilization methods.

Funding

Czech Ministry of Education (MŠMT) (LTC17086, 7AMB17DE034); EU COST Action (CA15220); Palacký University (IGA-PrF-2018-010); Bavarian Ministry of Economic Affairs, Energy and Technology (STMWI) (LABAY98A).

Acknowledgments

V.C.U. thanks A. A. Semenov for discussions, C.P., B.H. and K.G. thank their colleagues at the FAU computer science building for their kind support and for hosting the receiver.

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513 (2005).
3. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).
4. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
5. 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).
6. N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).
7. 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).
8. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quantum Inf. Comput. **3**, 535–552 (2003).

Optics EXPRESS

9. E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," Entropy **17**, 6072–6092 (2015).
10. 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).
11. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
12. 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).
13. M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
14. R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
15. S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography," Phys. Rev. Lett. **101**, 200504 (2008).
16. 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).
17. 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).
18. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
19. R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Inf. **3**, 30 (2017).
20. G. Berman and A. Chumak, "Photon distribution function for long-distance propagation of partially coherent beams through the turbulent atmosphere," Phys. Rev. A **74**, 013805 (2006).
21. A. A. Semenov and W. Vogel, "Quantum light in the turbulent atmosphere," Phys. Rev. A **80**, 021802 (2009).
22. R. Baskov and O. Chumak, "Laser-beam scintillations for weak and moderate turbulence," Phys. Rev. A **97**, 043817 (2018).
23. D. Vasylyev, A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, "Free-space quantum links under diverse weather conditions," Phys. Rev. A **96**, 043856 (2017).
24. 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).
25. B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, "Atmospheric continuous variable quantum communication," New J. Phys. **16**, 113018 (2014).
26. N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," Phys. Rev. A **91**, 022304 (2015).
27. M. Bohmann, A. A. Semenov, J. Sperling, and W. Vogel, "Gaussian entanglement in the turbulent atmosphere," Phys. Rev. A **94**, 010302 (2016).
28. P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," Phys. Rev. A **97**, 032311 (2018).
29. J. Heersink, C. Marquardt, R. Dong, R. Filip, S. Lorenz, G. Leuchs, and U. L. Andersen, "Distillation of squeezing from non-gaussian quantum states," Phys. Rev. Lett. **96**, 253601 (2006).
30. R. Dong, M. Lassen, J. Heersink, C. Marquardt, R. Filip, G. Leuchs, and U. L. Andersen, "Experimental entanglement distillation of mesoscopic quantum states," Nat. Phys. **4**, 919 (2008).
31. J. H. Churnside and R. J. Lataitis, "Wander of an optical beam in the turbulent atmosphere," Appl. Opt. **29**, 926 (1990).
32. D. Y. Vasylyev, A. Semenov, and W. Vogel, "Toward global quantum communication: beam wandering preserves nonclassicality," Phys. Rev. Lett. **108**, 220501 (2012).
33. H. Guo, B. Luo, Y. Ren, S. Zhao, and A. Dang, "Influence of beam wander on uplink of ground-to-satellite laser communication and optimization for transmitter beam radius," Opt. Lett. **35**, 1977–1979 (2010).
34. Y. Ren, A. Dang, B. Luo, and H. Guo, "Capacities for long-distance free-space optical links under beam wander effects," IEEE Photonics Technol. Lett. **22**, 1069–1071 (2010).
35. D. Vasylyev, A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," Phys. Rev. Lett. **117**, 090501 (2016).
36. D. Vasylyev, W. Vogel, and A. Semenov, "Theory of atmospheric quantum channels based on the law of total probability," Phys. Rev. A **97**, 063852 (2018).
37. L. C. Andrews, R. L. Phillips, and C. Y. Hopen, Laser beam scintillation with applications, vol. 99 (SPIE press, 2001).
38. G. Vidal and R. F. Werner, "Computable measure of entanglement," Phys. Rev. A **65**, 032314 (2002).
39. T. Eberle, V. Händchen, and R. Schnabel, "Stable control of 10 db two-mode squeezed vacuum states of light," Opt. Express **21**, 11546–11553 (2013).
40. 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).
41. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: A threat and a defense," Entropy **18**, 20 (2016).

Optics EXPRESS

42. A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic Gaussian channels," Phys. Rev. A **63**, 032312 (2001).
43. 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).
44. I. Derkach, V. C. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels," arXiv:1809.10167 [quant-ph] (2018).
45. M. R. Suite, H. R. Burris, C. I. Moore, M. J. Vilcheck, R. Mahon, C. Jackson, M. F. Stell, M. A. Davis, W. S. Rabinovich, W. J. Scharpf, A. E. Reed, and G. C. Gilbreath, "Fast steering mirror implementation for reduction of focal-spot wander in a long-distance free-space optical communication link," in *Free-Space Laser Communication and Active Laser Illumination III*, D. G. Voelz and J. C. Ricklin, eds. (SPIE, 2004).
46. M. Hulea, Z. Ghassemlooy, S. Rajbhandari, and X. Tang, "Compensating for optical beam scattering and wandering in fso communications," J. Light. Technol. **32**, 1323–1328 (2014).
47. S. M. Navidpour, M. Uysal, and M. Kavehrad, "Ber performance of free-space optical transmission with spatial diversity," IEEE Trans. Wirel. Commun. **6**, 2813 (2007).
48. E. J. Lee and V. W. Chan, "Part 1: Optical communication over the clear turbulent atmospheric channel using diversity," IEEE J. Sel. Areas Commun. **22**, 1896–1906 (2004).
49. X. Liu, "Free-space optics optimization models for building sway and atmospheric interference using variable wavelength," IEEE Trans. Commun. **57**, 492–498 (2009).
50. G. Baister and P. Gatenby, "Pointing, acquisition and tracking for optical space communications," Electron. & Commun. Eng. J. **6**, 271–280 (1994).
51. B. Epple and H. Henniger, "Discussion on design aspects for free-space optical communication terminals," IEEE Commun. Mag. **45**, 62 (2007).
52. A. ArockiaBazilRaj and U. Darusalam, "Performance improvement of terrestrial free-space optical communications by mitigating the focal-spot wandering," J. Mod. Opt. **63**, 2339–2347 (2016).
53. H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," IEEE Commun. Surv. Tutor. **19**, 57–96 (2017).
54. I. K. Son and S. Mao, "A survey of free space optical networks," Digital Communications and Networks **3**, 67–77 (2017).

Squeezing-enhanced quantum key distribution over atmospheric channels

Ivan Derkach, Vladyslav C. Usenko, and Radim Filip

Published: *New Journal of Physics*. Vol. 22, Issue 5, pp.053006 (2020)

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

Following is the published version of the article.

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
17 December 2019

REVISED
20 February 2020

ACCEPTED FOR PUBLICATION
12 March 2020

PUBLISHED
1 May 2020

PAPER

Squeezing-enhanced quantum key distribution over atmospheric channels

Ivan Derkach[1], Vladyslav C Usenko and Radim Filip

Department of Optics, Palacky University, 17. Listopadu 12, 771 46 Olomouc, Czech Republic
[1] Author to whom any correspondence should be addressed.

E-mail: ivan.derkach@upol.cz, usenko@optics.upol.cz and filip@optics.upol.cz

Keywords: quantum key distribution, Gaussian states, free space communication

Abstract

We propose the Gaussian continuous-variable quantum key distribution using squeezed states in the composite channels including atmospheric propagation with transmittance fluctuations. We show that adjustments of signal modulation and use of optimal feasible squeezing can be sufficient to significantly overcome the coherent-state protocol and drastically improve the performance of quantum key distribution in atmospheric channels, also in the presence of additional attenuating and noisy channels. Furthermore, we consider examples of atmospheric links of different lengths, and show that optimization of both squeezing and modulation is crucial for reduction of protocol downtime and increase of secure atmospheric channel distance. Our results demonstrate unexpected advantage of fragile squeezed states of light in the free-space quantum key distribution applicable in daylight and stable against atmospheric turbulence.

Introduction

Quantum key distribution (QKD) [1–5] is one of the major practical applications of quantum information theory, which provides trusted parties (Alice and Bob) with the methods (protocols) for provably secure distribution of secret cryptographic keys so that security of the key can be verified using fundamental principles of quantum physics. One of the main requirements of QKD is the availability of a dedicated quantum channel capable of transmitting coherent quantum signals between the sending and receiving stations. In the case of fiber-optical channels, being the typical media for QKD implementations, this means a dedicated optical fiber, possibly with co-existing classical or quantum signals. However, the dedicated fiber-optical infrastructure can be unavailable, e.g., in the case of movable stations, necessity of quick channel deployment or in hostile environments. Moreover, the extra-long-distance inter-continental quantum communication over satellites relies on the free-space channels [6]. Therefore, the free-space channels are an important physical medium for QKD implementations.

The main issue faced by the discrete-variable (DV) QKD protocols, based on single-photon states or weak coherent pulses and the direct photon counting, is the sensitivity of the detectors to the background light, which adds noise to the measured data. This renders standard DV QKD protocols practically unusable in the daylight conditions unless spectral filtering is applied, which adds unwanted additional loss and complexity to the set-up. At the same time, applicability and efficiency are crucial for QKD as they directly affect the secret communication, based on the quantum-secure keys. Alternatively, continuous-variable (CV) QKD protocols [7–10], based on the multiphoton coherent [11–15] or squeezed states [16] and homodyne quadrature detection using off-the-shelf equipment, can overcome this limitation. Indeed, a homodyne detector, which matches a signal to a narrow-band local oscillator (LO) beam, being the phase reference for the measurement, can intrinsically filter out the background radiation and make CV QKD protocols directly applicable in the daylight. However, CV QKD protocols are known to be sensitive to transmittance fluctuations, caused by the atmospheric turbulence [17, 18]. Such fluctuations, also referred to as the channel fading, result in the excess noise, which is proportional to the quadrature variance of a signal beam and limits applicability of CV QKD over atmospheric channels [19], which is also valid for the

recently studied fast-fading channels [20]. It was shown that noise due to the channel fading leads to security break of coherent-state CV QKD protocol and requires optimization of modulation and sub-channel post-selection for long-distance implementations over turbulent channels [19]. As a possible alternative solution, the use of squeezed signal states in CV QKD can be considered. Indeed, the squeezed states are known to be more robust against CV QKD imperfections such as inefficient post-processing [21] or strong channel excess noise [22, 23]. However, the foremost choice between DV or CV QKD protocols, aside from background noise resilience, will depend on implementation cost, complexity, distance, and numerous other aspects and conditions. The former are commonly accepted as more suited for long distances, particularly for satellite-based links [24, 25]. The latter, on top of mode selectivity of homodyne detection, which can filter out background ration and enable mode multiplexing, benefit also from high speed and high efficiency of the homodyne detection, and are integrative with existing telecommunication networks [15, 26, 27]. It is therefore not feasible to fairly compare the protocols quantitatively (as there are too many parameters to tune and features to consider) but we instead rely on the qualitative differences between the protocols and consider short- and mid-range free-space links inclined to the atmospheric turbulence as a promising scenario for CV QKD.

In the current paper we suggest squeezed-state protocol for free-space CV QKD with the channel fading and study the applicability and robustness of the protocol to realistic imperfections in comparison to the coherent-state protocol. We confirm the positive effect of signal state squeezing in realistic free-space CV QKD, taking into account channel fluctuations and additional fixed losses as well as other practical imperfections, such as limited post-processing efficiency. We show that squeezing can be helpful in the fluctuating channels, but should be optimized for the given conditions together with modulation used to encode information. We verify the results by considering the fading channel model, based on the beam wander, which is the dominating effect, causing free-space quantum channel fluctuations [28, 29]. Furthermore, we use the open-access turbulence observation results [30] confirm the advantage of squeezed-state protocol using characteristics of the real atmospheric channels and show that the use of squeezed signals allows extending the secure distance of the CV QKD protocols. The advantage is stable against the finite-size effects of limited data ensembles and impurity of the squeezed signal states. Our results therefore pave the way for efficient free-space QKD realization in daylight conditions, robust against atmospheric turbulence effects.

The paper is structured as follows. In section 1 we describe used CV QKD scheme that allows to independently control and manipulate squeezing and displacement in both quadratures of the signal state. Section 2 is devoted to analytical description of the effects of general fading channels on coherent- and squeezed-state protocols. Finally in section 3 we compare the performances of various CV QKD protocols in real and modeled noisy composite untrusted channels.

1. CV QKD protocol

The goal of a QKD protocol is to share a correlated string of data between two trusted parties, usually referred to as Alice and Bob. To do so Alice first prepares a quantum state of light, and encodes key bits into it. In the current work we will operate in the Gaussian regime, meaning the states used are described on phase space by the Gaussian Wigner function [9]. In this case, we can use Gaussian approximation of the states, channel and measurement and use the powerful covariance matrix formalism to simplify analysis to the finite-dimensional case [9]. However, secure key rate is a complex nonlinear functional of the elements of covariance matrix, therefore a usefulness of nonclassical and entangled states has to be analyzed in detail. Hence we suppose that Alice generates coherent or squeezed Gaussian states (using a laser source or e.g. optical parametric oscillator, respectively) and displaces them on a phase space in one or both quadratures (X or/and P) according to two independent Gaussian distributions with zero mean and variance V_{m}. Such a scheme encodes two real numbers from a continuous Gaussian distribution and therefore it has much higher capacity per time interval than a discrete encoding. Due to recent developments in the field of quantum optics, both coherent and displaced squeezed states can be generated with sufficient purity [31, 32]. The signal state prior to modulation can be therefore described by the diagonal covariance matrix $\gamma_{\mathrm{B}} = \mathrm{diag}[V_{\mathrm{s}}, 1/V_{\mathrm{s}}]$, where V_{s} is the variance of the squeezed quadrature, here and further, without loss of generality, it is assumed to be the X quadrature (covariance matrix for a coherent state reduces to a 2×2 unity matrix). Squeezed states are known to be more sensitive to a loss than coherent states, however, still squeezing never vanishes under pure loss. The signal after the modulation is characterized by the covariance matrix $\gamma'_{\mathrm{B}} = \mathrm{diag}[V_{\mathrm{s}} + V_{\mathrm{m}}, 1/V_{\mathrm{s}} + bV_{\mathrm{m}}]$, where for the coherent-state protocol $b = 1$ and it corresponds to modulation in both quadratures, while for the squeezed-state protocol $b = 0$, which indicates that only squeezed quadrature is modulated. We omit optimization over b, because we focus on testing of squeezed state applicability. Displaced signal states together with LO are sent to Bob via untrusted quantum channel

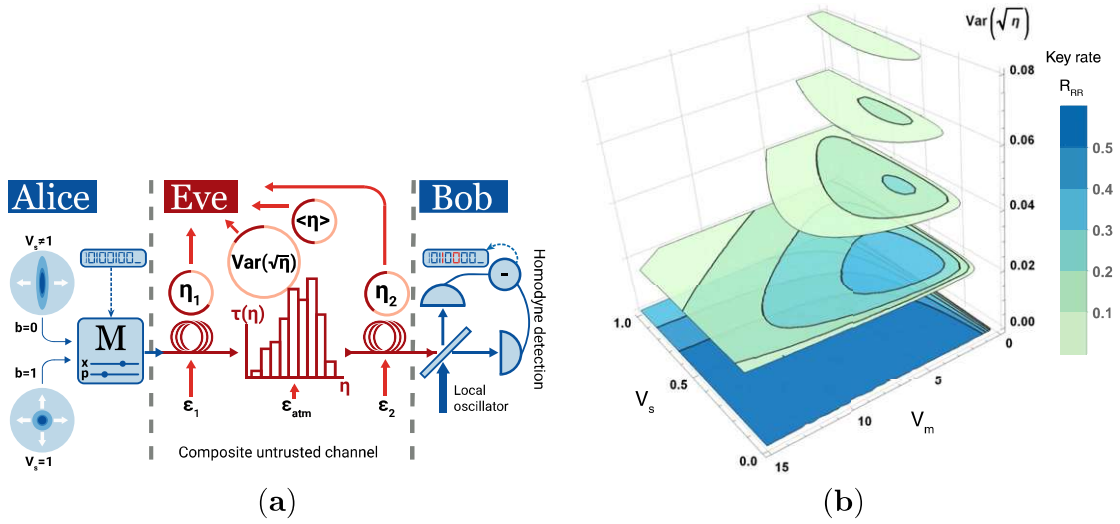


Figure 1. (a) Prepare-and-measure CV QKD scheme. Alice prepares a Gaussian (squeezed $V_s < 1$ or coherent $V_s = 1$) state of light and applies displacement operation in one ($b = 0$) or both ($b = 1$) quadratures. The signal is sent though the untrusted quantum channel to Bob, where the latter conducts homodyne detection. Composite unstrusted channel can consist of noisy fiber channels with fixed losses $\eta_{1,2}$, and excess noise $\epsilon_{1,2}$, respectively, and atmospheric channel $\tau(\eta)$ [characterized by mean losses $\langle\eta\rangle$, and transmittance fluctuations strength $\mathrm{Var}(\sqrt{\eta})$, and excess noise ϵ_{atm}]. Eve can receive information from all the channels, and is considered to perform collective attacks on the protocol. (b) Positive key rate (in bits per channel use) for squeezing V_s, modulation variance V_m and fading strength $\mathrm{Var}(\sqrt{\eta})$, $\langle\eta\rangle = 1/2, \eta_1 = \eta_2 = 1, \epsilon_1 = \epsilon_2 = \epsilon_{\mathrm{atm}} = 0$. The key rate values range from $0 < R \leqslant 0.1$ (lightly shaded areas) to $R > 0.5$ (darkest shaded areas) with 0.1 step. It is evident that the increase in fluctuations strength significantly decreases the key rate, however squeezing and modulation optimization can be conducted in order to improve the performance of the protocol. Importantly, optimal performance can be reached by a feasible squeezing for nonvanishing $\mathrm{Var}(\sqrt{\eta})$.

where the signal suffers from losses and noise (LO can be also reconstructed locally [33–35]). An eavesdropper Eve is presumed to be the cause of both losses and noise within the channel, is able to obtain and store the information about signal states, and is limited in her attacks on the channel only by the laws of physics. Bob on his side conducts a homodyne measurement with an auxiliary LO, and proceeds to key sifting, error correction, and privacy amplification using an authenticated classical channel established beforehand with Alice. As the outcome, Bob produces a sequence of secure bits shared with Alice.

The implementation of the basic coherent- or squeezed-state protocol described above is usually referred to as prepare-and-measure (P & M), and it is depicted on figure 1(a). In a realistic scenario, a short distance P & M free-space QKD will combine fiber-based channels in the buildings before and after the flexible atmospheric channel between the buildings. To predict protocol applicability, the parts of untrusted channel are considered to be either characterized by fixed transmittance (which can correspond to the fiber-optical parts of the entire link) or by fluctuating transmittance, which most commonly correspond to free-space atmospheric links. In the current work we consider a CV QKD protocol realization in a hybrid case, when an untrusted channel may consist of a combination of channels with fixed transmittance $\eta_{1,2}$ (fiber based channels), and a free-space channel with fluctuating transmittance η, governed by a probability distribution $\tau(\eta)$, in the middle. Furthermore both kinds of channels are not restricted to pure losses, but can introduce excess noise, the latter however is assumed to be fixed throughout the duration of all key distribution. Respectively, the excess noise in fiber channels is $\epsilon_{1,2}$, and in free-space channel ϵ_{atm}, while total noise added in the channel and measured by Bob is ϵ_+. Such the excess noise can be small in practice, however, it is important to introduce it in analysis to understand its impact.

Security of a CV QKD protocol is defined in terms of positivity of the lower bound on the rate (in bits per channel use) of the secret key [36, 37] distributed among the trusted parties. Either Alice or Bob must agree to be the reference side of the protocol, which means they will perform direct (DR) or reverse (RR) reconciliation [38, 39], respectively. Even though the efficiency $\beta \in [0, 1]$ of the algorithms for reconciliation is close to unity, it must be accounted for when estimating the key rate of the protocol. We assume pessimistic scenario where Eve is able to purify the state shared between the trusted parties, and conduct collective measurement over her part of the state. The strategy, presumably used by Eve, is called collective attack, and the key rate [40] of the protocol under such attack can be written as:

$$R_{\mathrm{DR}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{AE}}, \quad R_{\mathrm{RR}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{1}$$

where $\chi_{\mathrm{AE(BE)}}$ is the Holevo bound [41]—an upper bound on the information accessible to Eve with respect to the trusted reference side. Quantity I_{AB} in equation (1) is the mutual information between trusted parties. Both contributions to the key rate can be evaluated given the covariance matrix γ_{AB} describing the overall trusted state after channel interaction. The trusted state is presumed to be generated by a modified EPR-based system [21] (for derivation of the respective covariance matrix see also the supplementary information) that supports an independent control of squeezing and modulation.

2. General fading channel influence

Let us first have a look on the sole influence of the channel with transmittance fluctuations on CV QKD protocol. The atmospheric effects present in free-space link will unavoidably affect the transmitted beam, which will experience fading. Hence the transmission coefficient must be described in terms of transmittance probability distribution $\tau(\eta)$, as opposed to a fixed loss in a fiber link. It was shown [42] that such fading channel can be decomposed into a set of sub-channels $\{\eta_j\}$—channels with negligible attenuation fluctuations within them, which occur with probability $\tau(\eta_j)$ so that $\sum_{j=1}^{\infty}\tau(\eta_j)=1$. Now the Gaussian Wigner function of a state after a fading channel is a weighed sum of Winger functions after individual subchannels associated with fixed attenuation η_j [19]. In other words the resulting shared state, described by the covariance matrix γ_{AB}, is a mixture of the states γ_{AB}^{j} after each subchannel, which within the covariance matrix formalism is expressed by averaging over fluctuating transmittance values.

Statistical properties of the transmittance distribution $\tau(\eta)$ that directly affect the covariance matrix of the shared state γ_{AB} and influence the performance of the protocol (1), are the mean value of transmittance $\langle\eta\rangle$, and mean value of square root of transmittance $\langle\sqrt{\eta}\rangle$. They define the fading variance [42] $\mathrm{Var}(\sqrt{\eta})=\langle\eta\rangle-\langle\sqrt{\eta}\rangle^2$. The key rate (1) of the protocol over a fading channel is a function of all parameters of the protocol and the channel $R(V_{\mathrm{s}},V_{\mathrm{m}},\langle\eta\rangle,\mathrm{Var}(\sqrt{\eta}),\epsilon_{\mathrm{atm}})$. Alternatively the overall state after a fading channel can be represented as a state after a channel with fixed attenuation [19] $\langle\sqrt{\eta}\rangle^2$, and additional variance-dependent excess noise $\epsilon_f(\tau(\eta),V_{\mathrm{s}},V_{\mathrm{m}})=\mathrm{Var}(\sqrt{\eta})(V_{\mathrm{s}}+V_{\mathrm{m}}-1)$ (fixed channel excess noise ϵ_{atm} remains the same), so that $R(V_{\mathrm{s}},V_{\mathrm{m}},\langle\sqrt{\eta}\rangle^2,\epsilon_f,\epsilon_{\mathrm{atm}})$. Protocols that use DR or RR have the same dependency on the fading $\mathrm{Var}(\sqrt{\eta})$, with DR being limited to low attenuation channels $\langle\eta\rangle>1/2$, therefore we focus further on the reverse reconciliation since it allows one to analyze a wider range of channels, bearing in mind that the developed methodology is applicable to the protocols with DR as well.

In order to study solely the influence of a fading channel (for $\eta_{1,2}=1$) on the security of the CV QKD protocols, we look at the case of collective attacks conducted in case of noiseless channel ($\epsilon_{\mathrm{atm}}=0$) and perfect post-processing accessible to trusted parties ($\beta=1$, which is a theoretical limit, but recent protocols [27, 37, 43, 44] are very close to it). Figure 1(b) depicts a positive key rate and it is dependency on the squeezing V_{s} and modulation variance V_{m} for various values of transmittance fluctuations $\mathrm{Var}(\sqrt{\eta})$ for $\langle\eta\rangle=1/2$. The brightest colored area includes the key rate values of $R_{\mathrm{RR}}\in(0,0.1)$, and for each consequent darker area the key rate is increased by 0.1, with the darkest area containing values $R_{\mathrm{RR}}>0.5$. Whenever transmittance fluctuations are absent in the channel ($\mathrm{Var}(\sqrt{\eta})=0$), stronger squeezing V_{s} is always more beneficial for Alice and Bob. Strong squeezing allows protocols to achieve high key rate, and tolerate more losses and excess noise in the channel [23]. Typical values of fading in atmospheric channel with weak turbulence are $\mathrm{Var}(\sqrt{\eta})\leqslant 0.01$, while under strong turbulence one can expect at least $\mathrm{Var}(\sqrt{\eta})>0.04$, where the uniformly distributed channel has $\mathrm{Var}(\sqrt{\eta})=0.055$. The values of $\mathrm{Var}(\sqrt{\eta})>0.055$ correspond to a transmittance distribution described by a convex function which in the limit $\mathrm{Var}(\sqrt{\eta})=0.25$ represents the channel with equal probabilities to either perfectly transmit the signal or fail.

The presence of even small fluctuations of transmittance surprisingly limits applicable values of squeezing V_s, e.g. $\mathrm{Var}(\sqrt{\eta})=0.03$ is already sufficient to render the protocol with feasible $V_{\mathrm{s}}=-12$ dB [45] (at -3 dB of mean channel transmittance) insecure. Such sensitivity of strongly squeezed states to transmittance fluctuations is not exhibited in individual attacks, and manifests only for the collective attacks in the Holevo bound χ. It is an example why the collective effects are important to be analyzed. With the increase of transmittance fluctuations $\mathrm{Var}(\sqrt{\eta})$ the optimal values of squeezing are shifted towards lower values, corresponding to stronger squeezing. Therefore, optimization of the squeezing with respect to the channel and information encoding by coherent modulation is required. On the other hand, modulation V_{m} is shown to be bounded as well, and even more so, if one would take into account limited post-processing efficiency β. The need for squeezing optimization is further stressed in the fading channel where mean losses $\langle\eta\rangle$ are increasing, as is visible in the figure 2(a). In this case the modulation V_{m} is already optimized, and the strength of transmittance fluctuations in the fading channel is fixed to a low value $\mathrm{Var}(\sqrt{\eta})=0.01$, however this already alters the performance of the squeezed-state protocols. Even in the presence of such minor transmittance fluctuations the protocol that uses strongly squeezed signal states (as $V_{\mathrm{s}}=0.1$) cannot

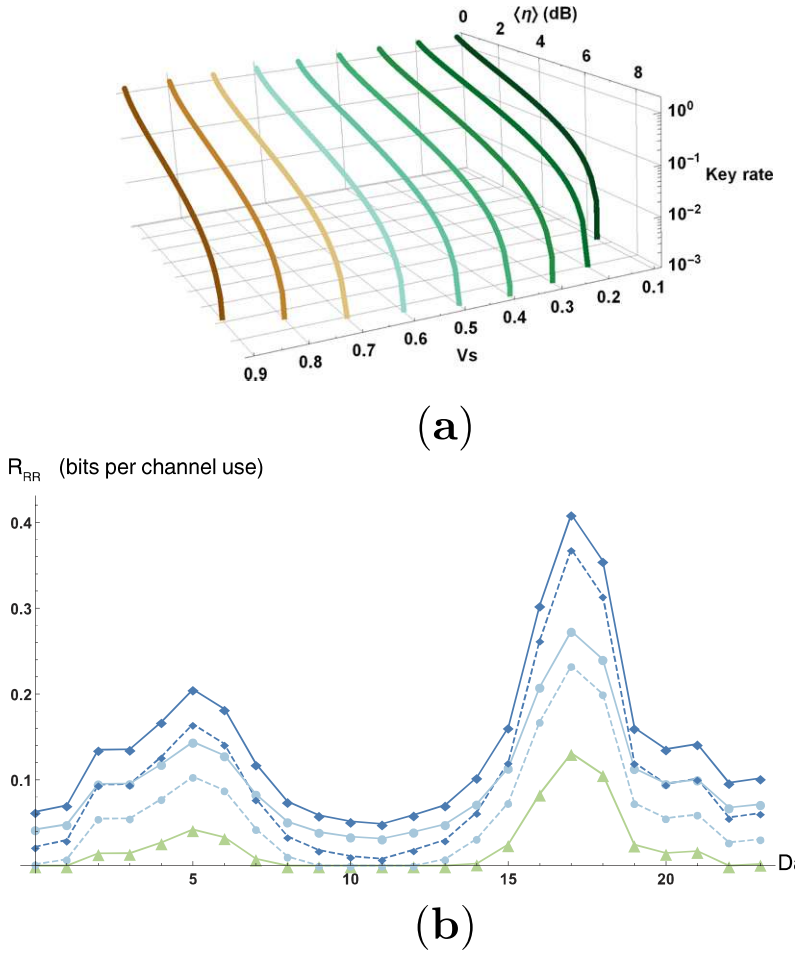


Figure 2. (a) Secure key rate (in bits per channel use) dependency on channel losses $\langle\eta\rangle$ (dB) for various values of squeezing V_s ($\eta_{1,2} = 1$). Transmittance fluctuations are only moderate $\mathrm{Var}(\sqrt{\eta}) = 0.01$, and modulation V_m is optimized. Evidently high squeezing levels of carrier states in CV QKD do not necessarily translate into high tolerance to $\langle\eta\rangle$ with transmittance fluctuations. Squeezing V_s and modulation variance V_m should be optimized in order to sustain the most amount of losses in the untrusted channel. (b) Optimized secure key rate of the coherent-state protocol (green triangles), and the squeezed-state protocol (blue circles, and blue squares) in 2.2 km long atmospheric channel. Each point was obtained for the transmittance distribution simulated using the averaged (over 4 months period) hourly statistics of structure constant of refractive index of air C_n^2. Finite-size effects are considered for block sizes of $n = 10^6$ (dashed lines) and $n = 10^{10}$ (solid lines). The squeezed-state protocol has been optimized over both modulation V_m and squeezing V_s, with the upper limit on the latter $V_s^{\max} = -3$ dB (circles), $V_s^{\max} = -10$ dB (squares). Excess noise $\epsilon_+ = 1\%$, efficiency $\beta = 95\%$, additional losses $\eta_{\mathrm{comb}} = -2.2$ dB. The coherent-state protocol can be successfully implemented only during suitable atmospheric conditions (around 5 am and 5 pm). The squeezed-state protocol with limited squeezing $V_s^{\max} = -3$ dB and smaller block size can on average be used during the whole day with an exception of possible temporary signal loss around 10 am. However increasing the block size and/or maximal squeezing $V_s^{\max}$ would have allowed to operate over such short atmospheric link continuously throughout the period of all 4 months.

tolerate more losses than the one that uses significantly weaker squeezed states (as $V_s = 0.9$). All these results demonstrate that a feasible squeezing is fairly sufficient for multiple increase of the secure key rate over the atmospheric channel.

The main takeaway of the analysis is that for a given fading channel with estimated values of $\langle\eta\rangle$ and $\mathrm{Var}(\sqrt{\eta})$, one should optimize both squeezing V_s and modulation V_m in order to operate in secure regime, in the first place, and subsequently to maximize the secure key rate. In a standard entanglement-based scheme [23, 46, 47] the effective modulation variance V_m of encoding alphabet and conditional squeezing V_s are inherently connected ($V_s = 1/V$ and $V_m = V - 1/V$, respectively). In figure 1(b) the key rate will then occupy a curved plane perpendicular to $V_s - V_m$ plane, and it crosses all regions of the maximal key rate for all values of $\mathrm{Var}(\sqrt{\eta})$. In other words, entanglement-based protocol optimized in terms of key rate will yield roughly same performance as the protocol where squeezing V_s and modulation V_m are optimized separately. However the P & M protocol is simpler for experimental implementation and more flexible, meaning it can achieve the same key rate as entanglement-based protocol, with less squeezing, and compensate by applying modulation with higher variance. On the other hand, the entanglement-based

protocol can be extended to a secure communication network. It is certainly stimulating for further analysis and experimental development.

3. Atmospheric channel fluctuations

Undoubtedly, with increasing distances, and consequently stronger turbulence, squeezing optimization is vital for sustainable operation of the CV QKD protocol. On the other hand, for significantly longer distances, and ultimately, for satellite-based channels, the transmittance fluctuations will have less pronounced effect compared to the overall very strong attenuation mainly due to the fact that the beam wander will be largely compensated for by the natural beam expansion during the beam propagation [48]. In the current work we explore the regime of weak (and weak-to-moderate) turbulence typical for short- and short- to mid-range free-space channels, essential for quick deployment of the link, and independence of existing fiber-optical infrastructure, for which Gaussian CV QKD protocols are a promising solution. In the following section we analyze the performance of both the coherent-state and the squeezed-state protocols established over a composite untrusted channel, as depicted on figure 1(a). We consider limited post-processing $\beta < 1$, additional fixed losses before and after the fading channel $\eta_{1,2} < 1$, as well as thermal excess noise in all channels $\epsilon_{1,2,\mathrm{atm}} > 0$. Finite-size effects [49] were also taken into account as a correction to the key rate (1) $\Delta(n)$ that strongly depends on the total size n of data sets shared by trusted parties.

The covariance matrix describing the state after composite untrusted channel and received by Bob is $\gamma_{\mathrm{B}}' = (\gamma_{\mathrm{B}} - \mathbb{1})\langle\eta\rangle\eta_{\mathrm{comb}} + (1 + \epsilon_+)\mathbb{1}$, where $\eta_{\mathrm{comb}} = \eta_1\eta_2$ is product of all transmittance values of channels with fixed losses, and $\epsilon_+ = \epsilon_2 + \epsilon_{\mathrm{atm}}\eta_2 + \epsilon_1\eta_2\langle\eta\rangle$ is a total excess noise received by Bob. Even though Alice and Bob may not be able to distinguish, and properly attribute losses and noise to each individual channel, they are only required to estimate each time the overall loss $\eta_{\mathrm{comb}}\eta_j$, and total excess noise ϵ_+ imposed on the state that arrives to the Bob's side. Note that estimation of fading or composite channels is more involved comparing to the one of fiber channels, and requires employment of suitable estimation framework [50]. To compensate for imprecise estimation due to low energy states one can either sacrifice larger data blocks or exercise double modulation [51].

3.1. Fading model

To simulate the transmittance in free-space horizontal optical links with dissimilar properties we adopt an atmospheric transmittance probability distribution with an elliptic-beam approximation [29]. The model assumes a Gaussian optical beam propagating through atmospheric horizontal link with isotropic turbulence, where the beam is distorted and suffers from broadening, deformation of beam spot into elliptical shape, as well as beam wander [18, 28]. The model aided the study of nonclassical properties of radiation fields and developing of Gaussian entanglement preservation techniques in turbulent channels [52] and was confirmed experimentally [19, 53]. The model has also been successfully applied in the regimes of weak, weak-to-moderate and strong turbulence, and can incorporate effects of haze and rain [54]. Furthermore, the applied model can be used in conjunction with experimentally employed beam tracking techniques. The probability distribution of the transmittance (PDT) is given as:

$$\tau(\eta, x_0, y_0, W_0, \Theta_1, \Theta_2, \phi) = \frac{2}{\pi}\int_{\mathbb{R}^4} \mathrm{d}^4 v \int_0^{\pi/2} \mathrm{d}\phi \rho_{\mathrm{G}}(v; \mu; \Sigma)\delta[\eta - \eta(v, \phi)]. \tag{2}$$

The probability distribution (2) is determined by $\rho_{\mathrm{G}}(v; \mu; \Sigma)$ Gaussian probability density of four-dimensional vector $v = \left(x_0\, y_0\, \Theta_1\, \Theta_2\right)^T$ with the mean μ and the covariance matrix Σ. The vector v, along with the angle ϕ that accounts for a rotation of an elliptical beam spot, influences the aperture transmittance $\eta(v, \phi)$. The latter is generally obtained by accounting for all turbulent disturbances along the propagation path that affect the intensity of the received light. The model assumes $\eta(v, \phi)$ is mainly impacted by beam wandering, and distortion of the spot shape and size. Depending on the turbulence strength (determined by propagation distance, environmental conditions, operation time, etc) either only the former, or both effects have to be considered. While the transmittance cannot be explicitly evaluated, it can, however, be accurately (provided beam ellipticity is small) approximated by the transmittance of the circular Gaussian beam with an effective spot-radius W_{eff} as:

$$\eta(v, \phi) = \eta_0 \exp\left\{-\left[\frac{r_0/a}{R\left(\frac{2}{W_{\mathrm{eff}}(\phi-\varphi_0)}\right)}\right]^{\lambda\left(\frac{2}{W_{\mathrm{eff}}(\phi-\varphi_0)}\right)}\right\}, \tag{3}$$

where a is the receiving aperture radius, η_0 is transmittance of the beam in the center of the aperture ($x_0 = y_0 = 0$), and $R(\xi)$, $\lambda(\xi)$ are scale and shape functions, respectively. Vector $r_0 = (x_0, y_0, \varphi_0)^T$ is a beam

spot center deviation from the aperture center. In a regime of weak turbulence the distribution (2) reduces to log-negative Rice distribution, and if the beam fluctuates around the aperture center $\langle r_0 \rangle = 0$ to log-negative Weibull distribution [28].

The probability (2) is governed by five real parameters, that are (with an exception of W_0) randomly changed by the atmosphere: current position of beam-spot center x_0, y_0; relation of initial beam-spot radius (W_0) to elliptic beam-spot semiaxes (W_1, W_2) $-$ Θ_1, Θ_2; uniformly distributed angle of semiaxis of elliptical beam-spot relative to x-axis ϕ. The simulation of these parameters relies on analytical description of the first and second moments of the Gaussian vector v, including the correlations between parameters describing beam-centroid position and shape of the arriving beam.

We assume perfect channel estimation and rely on assessment of μ, Σ in regimes of weak, weak-to-moderate and strong turbulence [29] and carry out an atmospheric channel transmittance simulation in respective regimes by Monte Carlo method. The simulation of transmittance (3) in appropriate turbulence regime is ultimately driven by beam wave-number k, propagation distance L and C_n^2 structure constant of the refractive index of the air, as well as initial beam-spot radius W_0. An important description of atmospheric links that incorporates most of aforementioned quantities is the Rytov parameter $\sigma_R^2 = 1.23 C_n^2 k^{\frac{7}{6}} L^{\frac{11}{6}}$. Rytov parameter is defined as the normalized irradiance variance of a plane wave propagating through media with random index of refraction [55]. When the atmospheric turbulence is considered to be weak or weak-to-moderate the dominating effect is the beam wandering, while beam broadening and deformation is minor, the Rytov parameter takes values up to $\sigma_R^2 \lesssim 1$. The regime when both beam wandering and deformation effects are present and non-negligible corresponds to strong turbulence and the Rytov parameter values are $\sigma_R^2 \gg 1$, which corresponds to an increase of either C_n^2 or L, or both.

3.2. Analysis of real channels

The first example we consider is a CV QKD protocol established over an atmospheric channel of fixed length of 2.2 km that is used for an extensive period of time. The transmittance values have been simulated, using the elliptic-beam model (3), based on the data obtained and published by Czech Metrology Institute from atmospheric channel in the urban area of Prague, Czech Republic [30]. The structure constant of refractive index of air C_n^2 has been measured throughout months of May to August, and hourly statistics covering the whole measurement period has been used to simulate transmittance values in given conditions. The atmospheric conditions differ significantly throughout the period of 4 months, however turbulence remains weak $\sigma_R^2 \approx 1$ during the whole duration of channel use. Overall tendencies remain the same—on average the atmosphere is less turbulent during the night, and more during the day: the highest transmittance $\langle \eta \rangle = -1.83$dB, and lowest fading $\mathrm{Var}(\sqrt{\eta}) = 3.25 \times 10^{-3}$ is observed around 5 pm. Depicted on figure 2(b) are the simulation results, that allow to assess whether secure key distribution can be maintained during the whole period of channel use, and how stable can the signal rate be.

We analyze the coherent- and the squeezed-state CV QKD protocols (optimized in terms of signal squeezing V_s for the former, and modulation variance V_m for both) in a composite channel with additional fixed losses $\eta_{\mathrm{comb}} = -4.5$dB, total excess noise $\epsilon_+ = 1\%$, post-processing efficiency $\beta = 95\%$, and finite-size effects were considered for block sizes of $n = 10^6$ (dashed lines) and 10^{10} (solid lines). The optimized coherent-state protocol (bottom line) with a block size of $n = 10^{10}$, on average, most of the operation time cannot reliably distribute signal states between trusted parties and yields secure key only under the best atmospheric conditions, which occur around 5 am and 5 pm. Under consideration of smaller block size $n = 10^6$ security of coherent-state QKD cannot be guaranteed under any atmospheric conditions whatsoever. The squeezed-state protocol on the other hand can be successfully implemented for both considered block sizes. While high squeezed states may be costly to generate, even accessible values of $V_s = -3$dB can significantly improve the performance of the protocol in short atmospheric link with significant additional losses. Provided the finite-size of block to be $n = 10^6$ the security is threatened only during the worst atmospheric conditions (around 11 am) with $\mathrm{Var}(\sqrt{\eta}) = 5.7 \times 10^{-3}$ and $\langle \eta \rangle = -4.17$dB. Increasing the block size n and/or threshold for squeezing optimization $V_s^{\max}$ resolves the issue and completely eliminates downtime of the protocol. Another aspect of the squeezed-state protocol is that stability of the secure key rate decreases if higher values of squeezing V_s are accessible. In other words, squeezing contribution is more significant in better atmospheric conditions, and this is why the difference between global maxima and minima of the key rate on figure 2(b) is greater for the case of $V_s^{\max} = -10$ dB.

Second example we consider is a CV QKD protocol over short atmospheric links of various length and additional losses before and/or after the link. The atmospheric channels of various lengths have been simulated, using the elliptic-beam model (3) assuming signal beam wavelength $\lambda = 1550$nm, aperture size $a = 20$mm, and initial beam-spot radius $W_0 = 40$mm. The Rytov parameter in all channels $\sigma_R^2 < 1$, and corresponds to weak turbulence, for which the dominant atmospheric effect is beam wandering. The results

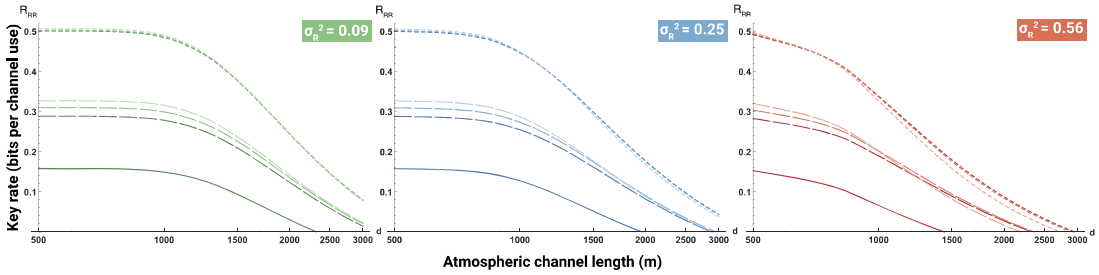


Figure 3. Secure key rate of the squeezed-state (dashed and dotted lines) and the coherent-state (solid lines) CV QKD protocol on the length (in m) of free-space channel in the composite untrusted channel, for various values of Rytov parameter $\sigma_R^2 = 0.09$ (green), 0.25 (blue), and 0.56 (red). Lower values of Rytov parameters yield transmittance distribution $\tau(\eta)$ with smaller variance and higher mean. Reconciliation efficiency $\beta = 95\%$, $\eta_{\rm comb} = -4$dB, total excess noise received by Bob $\epsilon_+ = 2.5\%$, modulation $V_{\rm m}$ is optimized, squeezing is optimized, but limited to experimentally feasible values $V_{\rm s}^{\rm max} = -3$ dB (long dash lines), and $V_{\rm s}^{\rm max} = -10$ dB (short dash lines). Finite-size effects have been accounted for block sizes of $n = 10^6$. Anti-squeezing noise $V_{\rm AN} = 0$ (maximum opacity lines), +3.1dB (medium opacity lines), and +10.3dB (lowest opacity lines). At short distances ($d \leqslant 500$m) atmospheric links, despite the value of Rytov parameter, have narrow transmittance distributions $\tau(\eta)$, with a mean close to unity, and the performance of the CV QKD protocols is governed by losses in fiber channels $\eta_{\rm comb}$ and total excess noise ϵ_+. As atmospheric link length increases, so does the transmittance fluctuations Var($\sqrt{\eta}$), and the need for optimization of the parameters of the CV QKD protocols.

of the calculations for the squeezed-state protocol (dashed and dotted lines), and the coherent-state protocol (solid lines) are depicted on figure 3. All protocols have been optimized in terms of encoding alphabet size $V_{\rm m}$. The squeezed-state protocol was additionally optimized with regard to signal squeezing, which was limited to attainable values $V_{\rm s}^{\rm max} = -10$ dB (short dash lines), and $V_{\rm s}^{\rm max} = -3$ dB (long dash lines). We set post-processing efficiency $\beta = 95\%$, and impose significant additional losses in composite channel $\eta_{\rm comb} = -6$ dB, as well as excess noise $\epsilon_+ = 2.5\%$. Additionally, we account for finite-size effects, assuming block size of $n = 10^6$, and realistic anti-squeezing noise (darkest lines correspond to the protocol with pure states) $V_{\rm AN} = +3.1$ dB (medium opacity lines), and $V_{\rm AN} = +10.3$ dB (minimum opacity lines), so that the signal states are initially characterized by diag$[V_{\rm s}, 1/V_{\rm s} + V_{\rm AN}]$.

In fiber channels with fixed attenuation, noise in anti-squeezed quadrature $V_{\rm AN}$ is usually slightly beneficial for trusted parties, since it does not affect mutual information $I_{\rm AB}$ between them, but at the same time reduces the Holevo bound $\chi_{\rm BE}$. However in fading channels this is not the case, as noise in anti-squeezed quadrature, again does not alter the mutual information $I_{\rm AB}$, but can increase the Holevo bound $\chi_{\rm BE}$. Despite this the squeezed-state protocol can still significantly outperform coherent-state protocol even under substantial anti-squeezing noise. On the other hand modulation in both (X and P) quadratures of coherent-state protocol is a sub-optimal approach if the untrusted channel exhibits significant transmittance fluctuations. It is certainly beneficial for trusted parties to employ either heterodyne detection, or homodyne detection and modulation of only signal quadrature, with the latter being more advantageous in channels with stronger fluctuations. In our example for channels with Rytov parameter $\sigma_R^2 = 0.09$, 0.25, fluctuations of transmittance are low enough so that anti-squeezing noise is actually helpful for the squeezed-state protocol with $V_{\rm s}^{\rm max} = -3$ dB, and does not considerably alter the performance of the protocol with $V_{\rm s}^{\rm max} = -10$ dB. The CV QKD protocols established over the channel with the highest Rytov parameter $\sigma_R^2 = 0.56$ exhibit on short distances the advantages of anti-squeezing noise, and on longer distances, the noise is conversely more harmful for the CV QKD. The anti-squeezing noise presence elevates the need for squeezing optimization.

For very short distances $d \leqslant 500$ m the distinction between channels with different Rytov parameter is insignificant, and secure key rate of the protocols is mainly determined by the excess noise ϵ_+ and additional losses $\eta_{\rm comb}$ in such composite channels. The optimal values of signal state squeezing in such regime are equal to maximally permitted for the protocol $V_{\rm s}^{\rm max}$, while the variance of modulation $V_{\rm m}$ is mainly limited by efficiency of post-processing algorithms β. This is of course due to low values of fluctuations of transmittance Var($\sqrt{\eta}$) in atmospheric channel of such short lengths.

As the length of atmospheric channel increases, so does the variance of transmittance Var($\sqrt{\eta}$), and as consequence the secure key rate starts to drop. However, variance of transmittance Var($\sqrt{\eta}$) reaches maximum at certain distance (determined by the value of the Rytov parameter σ_R^2) and then slowly decreases with the distance. In given example for $\sigma_R^2 = 0.56$ transmittance variance peaks around 1750 m at Var($\sqrt{\eta}$) $= 2.7 \times 10^{-3}$, for $\sigma_R^2 = 0.25$ at around 2000 m with Var($\sqrt{\eta}$) $= 1.2 \times 10^{-3}$, and for $\sigma_R^2 = 0.09$ maximum variance Var($\sqrt{\eta}$) $= 4 \times 10^{-4}$ is for the 2250 m atmospheric channel. Even though the expected fluctuations in simulated channels are low, modulation optimization must be performed to maximize the key rate and reach longer distances for both coherent- and squeezed-state protocols. Squeezing of signal

states yields a clear advantage over coherent states, however squeezing optimization is beneficial only for the channels of length 2000 m and longer, or for atmospheric channels where turbulence is described by higher values of Rytov parameter.

Overall both coherent- and squeezed-state protocols can successfully be implemented over short atmospheric channels even with significant excess noise and additional untrusted losses, but the squeezed states can allow the CV QKD protocol to reach substantially longer secure distances.

4. Summary and conclusions

In the channels with fixed losses the robustness of the CV QKD protocols is unambiguous—the more losses present in the channel, the less noise the signal can tolerate, and vice versa—the more noise present in the channel, the less losses the signal can tolerate. The squeezing of the signal states improves the tolerance against both losses and noise in such channels, and the higher levels of squeezing are more advantageous for the protocol, since it will directly translate into considerable improvement in terms of secure key rate [21, 56, 57]. In fading channels this is not necessarily the case. Surprisingly, the squeezing is still very beneficial for the security of the CV QKD. However, squeezing of the signal states is advantageous for the protocol but should be optimized depending on the properties of transmittance probability distribution. The effect of transmittance fluctuations is analogous to variance- and squeezing-dependent noise, and the more squeezed signal states are used, the more sensitive the resulting protocol can be to transmittance fluctuations in the channel. The presence of fading in the channel limits maximal applicable values of squeezing and modulation variance, and reduces the region of optimal values that allow to maximize the key rate of the protocol.

We have proposed the use and shown an unexpected gain of squeezed-state continuous-variable quantum key distribution protocols in composite untrusted channel, that is the combination of fading atmospheric channel and multiple fiber channels with fixed losses. Our results are compliant with an entanglement-based, as well as prepare-and-measure schemes for the Gaussian states generation, and can be used in all Gaussian CV QKD protocols operated in atmospheric channels. While the coherent-state protocol can only be optimized in terms of displacement of the signal state, it is still a necessary step to reduce the downtime of the protocol. The squeezed-state protocol is sensitive to the fading in untrusted channel, but optimization of squeezing brings considerable benefits, and allows to successfully employ the protocol in greater (comparing to the coherent-state protocol) range of atmospheric conditions, communication distances, and levels of additional losses and noise.

Furthermore, in the case when untrusted additive Gaussian channel noise can be ruled out by trusted device calibration, the trusted parties can group the transmitted data according to estimated stable transmittance windows corresponding to non-fluctuating noiseless channels [50], apply shot-noise-limited modulation of squeezed signal states hence preventing an unauthorized party from gaining any information on the key [58] and improve the resulting key rate by channel multiplexing [59–61]. In the presence of channel noise the protocol optimization along with the post-selection techniques [19, 62] and Gaussian error correction aimed at overcoming low-frequency additive Gaussian noise [63], can significantly improve the performance of Gaussian CV QKD protocols in atmospheric links, enabling efficient and robust free-space quantum key distribution, fully applicable in daylight conditions. Next step towards this free-space novel quantum key distribution technique is an experimental verification of the functionality of the free-space squeezed-state protocol which will stimulate further theoretical and experimental developments and practical implementations.

Acknowledgments

I D and V C U acknowledge the project LTC17086 of the INTER-EXCELLENCE program of the Czech Ministry of Education, V C U acknowledges project 19-23739S of the Czech Science Foundation and project 7AMB17DE034 of the Czech Ministry of Education, I D acknowledges the project PrF-2018-010 of Internal Grant Agency at Palacky University. R.F. acknowledges support by the project CZ.02.1.01/0.0/0.0/16_026/0008460 of the Czech Ministry of Education. The research leading to these results has received funding from the H2020 European Programme under Grant Agreement 820466 CIVIQ.

ORCID iDs

Ivan Derkach https://orcid.org/0000-0001-8014-7202
Vladyslav C Usenko https://orcid.org/0000-0002-8765-8758
Radim Filip https://orcid.org/0000-0003-4114-6068

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[3] Diamanti E, Lo H K, Qi B and Yuan Z 2016 *npj Quantum Inf.* **2** 1–12
[4] Pirandola S *et al* 2019 arxiv:1906.01645v1
[5] Xu F, Zhang X M Q, Lo H K and Pan J W 2019 arxiv:1903.09051
[6] Bedington R, Arrazola J M and Ling A 2017 *npj Quantum Inf.* **3** 1–13
[7] Braunstein S L and Van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[8] Pirandola S, Braunstein S L and Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504
[9] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621–69
[10] Diamanti E and Leverrier A 2015 *Entropy* **17** 6072–92
[11] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[12] Lodewyck J *et al* 2007 *Phys. Rev.* A **76** 42305
[13] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New J. Phys.* **11** 045023
[14] Jouguet P *et al* 2012 *Opt. Express* **20** 14030
[15] Huang D, Huang P, Lin D and Zeng G 2016 *Sci. Rep.* **6** 1–9
[16] Cerf N J, Lévy M and Assche G V 2001 *Phys. Rev.* A **63** 052311
[17] Berman G P and Chumak A A 2006 *Phys. Rev.* A **74** 013805
[18] Semenov A and Vogel W 2009 *Phys. Rev.* A **80** 021802
[19] Usenko V C, Heim B, Peuntinger C, Wittmann C, Marquardt C, Leuchs G and Filip R 2012 *New J. Phys.* **14** 093048
[20] Papanastasiou P, Weedbrook C and Pirandola S 2018 *Phys. Rev.* A **97** 032311
[21] Usenko V C and Filip R 2011 *New J. Phys.* **13** 113007
[22] García-Patrón R and Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
[23] Madsen L S, Usenko V C, Lassen M, Filip R and Andersen U L 2012 *Nat. Commun.* **3** 1083
[24] Dequal D, Vallone G, Bacco D, Gaiarin S, Luceri V, Bianco G and Villoresi P 2016 *Phys. Rev.* A **93** 010301
[25] Yin J *et al* 2017 *Science* **356** 1140–4
[26] Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P and Zeng G 2015 *Opt. Express* **23** 17511–9
[27] Zhang Y C, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 arxiv:2001.02555v1
[28] Vasylyev D Y, Semenov A and Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
[29] Vasylyev D, Semenov A and Vogel W 2016 *Phys. Rev. Lett.* **117** 090501
[30] Grabner M and Kvicera V 2012 *Radioengineering* **21** 455–8
[31] Serikawa T, Yoshikawa J I, Makino K and Frusawa A 2016 *Opt. Express* **24** 28383–91
[32] Vahlbruch H, Mehmet M, Danzmann K and Schnabel R 2016 *Phys. Rev. Lett.* **117** 110801
[33] Qi B, Lougovski P, Pooser R, Grice W and Bobrek M 2015 *Phys. Rev.* X **5** 041009
[34] Soh D B, Brif C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J and Sarovar M 2015 *Phys. Rev.* X **5** 041010
[35] Marie A and Alléaume R 2017 *Phys. Rev.* A **95** 012316
[36] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[37] Gehring T, Händchen V, Duhme J, Furrer F, Franz T, Pacher C, Werner R F and Schnabel R 2015 *Nat. Commun.* **6** 8795
[38] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 *Quantum Inf. Comput.* **3** 535–52
[39] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[40] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.A* **461** 207–35
[41] Holevo A and Werner R 2001 *Phys. Rev.* A **63** 032312
[42] Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2010 *Phys. Rev.* A **82** 012312
[43] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev.* A **77** 042325
[44] Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R, Kasai K, Matsumoto R and Tsurumaru T 2017 *Quantum Science and Technology* **2** 024010
[45] Mehmet M, Ast S, Eberle T, Steinlechner S, Vahlbruch H and Schnabel R 2011 *Opt. Express* **19** 25763–72
[46] Su X, Wang W, Wang Y, Jia X, Xie C and Peng K 2009 *Europhys. Lett.* **87** 20005
[47] Wang N, Du S, Liu W, Wang X, Li Y and Peng K 2018 *Phys. Rev. Appl.* **10** 064028
[48] Usenko V C, Peuntinger C, Heim B, Günthner K, Derkach I, Elser D, Marquardt C, Filip R and Leuchs G 2018 *Opt. Express* **26** 31106
[49] Leverrier A and Grangier P 2010 *Phys. Rev.* A **81** 062314
[50] Ruppert L, Peuntinger C, Heim B, Günthner K, Usenko V C, Elser D, Leuchs G, Filip R and Marquardt C 2019 *New J. Phys.* **21** 123036
[51] Ruppert L, Usenko V C and Filip R 2014 *Phys. Rev.* A **90** 062310
[52] Bohmann M, Semenov A, Sperling J and Vogel W 2016 *Phys. Rev.* A **94** 010302
[53] Bohmann M, Sperling J, Semenov A and Vogel W 2017 *Phys. Rev.* A **95** 012324
[54] Vasylyev D, Semenov A, Vogel W, Günthner K, Thurn A, Bayraktar Ö and Marquardt C 2017 *Phys. Rev.* A **96** 043856
[55] Andrews L C, Phillips R L and Hopen C Y 2001 *Laser Beam Scintillation with Applications* vol 99 (Bellingham, WA: SPIE Press)
[56] Usenko V C and Filip R 2016 *Entropy* **18** 20
[57] Usenko V C and Filip R 2010 *Phys. Rev.* A **81** 022318
[58] Jacobsen C S, Madsen L S, Usenko V C, Filip R and Andersen U L 2018 *npj Quantum Information* **4** 32
[59] Filip R, Mišta L and Marek P 2005 *Phys. Rev.* A **71** 012323
[60] Qi B, Zhu W, Qian L and Lo H K 2010 *New J. Phys.* **12** 103042
[61] Eriksson T A *et al* 2019 *Commun. Phys.* **2** 1–8
[62] Derkach I D, Peuntinger C, Ruppert L, Heim B, Gunthner K, Usenko V C, Elser D, Marquardt C, Filip R and Leuchs G 2016 Proof-of-principle test of coherent-state continuous variable quantum key distribution through turbulent atmosphere (conference presentation) *Quantum Information Science and Technology II* **9996** 999605
[63] Lassen M, Berni A, Madsen L S, Filip R and Andersen U L 2013 *Phys. Rev. Lett.* **111** 180502

9 | Conclusions

This thesis is based on four original publications [1–4] and presents main results of my theoretical research conducted during the course of my PhD studies at the Department of Optics, Palacky University (Olomouc, Czech Republic). My research was supervised by Prof. Radim Filip and co-supervised by Dr. Vladyslav Usenko.

The main idea behind the work is to adopt the practical approach to security analysis of a family of Gaussian CV QKD protocols, and identify possible security threats. We attempt to reduce the gap between theoretical protocol design, and actual implementation of the protocol. While it is unreasonable to expect to account for all possible equipment weaknesses it is paramount to improve the design, making protocols more robust, reliable and efficient with each future iteration.

To identify and solve the issues we use models based on linear-optical interactions and Gaussian formalism. We address semitrusted side channels present at both trusted sides of the protocol, and study the effect of each individual channel in Chapter 4. The work covers the main types of generalized information leakage from, and noise infusion onto the, otherwise presumably shielded, stations of trusted parties. We successfully determine the security bounds, and show the alterations to the protocols performance caused by the mere presence or active usage, by the adversary, of the respective side channel. We also suggest methods for counteracting the limitations imposed by side channels, as well as for complete restoration of the original operation efficiency.

In Chapter 5 we alleviate the assumptions of single-mode state modulation and embrace the possibility of disclosing the information regarding encoded key via auxiliary non-signal modes. Such information leakage is analogous to photon-number splitting attack in discrete variable protocols, and is as threatening for the security of the key distribution based on continuous variables. We explore different regimes of leakage and their effect on protocols under individual and collective attacks. Presuming the auxiliary modes cannot be filtered out completely, we suggest an optimization of squeezing and encoding alphabet size for maximizing the secure distance of the protocol.

In Chapters 6 and 7 we tackle the issue of optimization of CV QKD protocols implementations over free space atmospheric channels. Unlike well studied fiber channels, free space links offer greater deployment speed and convenience, but offer transmission quality that is highly dependent on weather conditions, location and length of the link, and, moreover, varies significantly. We experimentally verify the applicability of beam expansion technique for stabilization of channel transmittance fluctuations, and show the conditions suitable for such technique in Chapter 6. Lastly, we demonstrate the bounds

on applicable levels of squeezing imposed by the turbulence in free space channels. We advocate individual and feasible optimization of resource available at trusted sender side, to securely cover longer distances in atmospheric turbulent links, reduce the downtime of the protocol or recover the ability to establish a secure key.

All developed methods can be combined and are supported by Gaussian CV QKD protocols. Furthermore, they do not require non-Gaussian operations, use of entangled states, unfeasible levels of squeezing, or unrealistic requirements to shielding of the trusted stations, but rather careful analysis of parameters of the trusted equipment. Experimental verification of suggested techniques will certainly stimulate further theoretical and experimental developments of the Gaussian QKD protocol family.

Bibliography

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

[2] 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, 2017.

[3] Vladyslav C. Usenko, Christian Peuntinger, Bettina Heim, Kevin Günthner, Ivan Derkach, Dominique Elser, Christoph Marquardt, Radim Filip, and Gerd Leuchs. Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels. *Optics Express*, 26(24):31106, 2018.

[4] Ivan Derkach, Vladyslav C. Usenko, and Radim Filip. Squeezing-enhanced quantum key distribution over atmospheric channels. *New Journal of Physics*, 22(5):053006, 2020.

[5] M Bohmann, AA Semenov, J Sperling, and W Vogel. Gaussian entanglement in the turbulent atmosphere. *Physical Review A*, 94(1):010302, 2016.

[6] D Vasylyev, AA Semenov, and W Vogel. Atmospheric quantum channels with weak and strong turbulence. *Physical review letters*, 117(9):090501, 2016.

[7] D Vasylyev, AA Semenov, W Vogel, K Günthner, A Thurn, Ö Bayraktar, and Ch Marquardt. Free-space quantum links under diverse weather conditions. *Physical Review A*, 96(4):043856, 2017.

[8] Stephen Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78–88, 1983.

[9] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(P1):7–11, 2014.

[10] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, XLV:295–301, 1926.

[11] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[12] Simon Singh. *The code book: the science of secrecy from ancient Egypt to quantum cryptography*. Anchor, 2000.

[13] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021, 2016.

[14] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[15] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[16] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[17] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557–559, 1992.

[18] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[19] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92(5):057901, 2004.

[20] A Muller, T Herzog, B Huttner, W Tittel, H Zbinden, and N Gisin. "plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, 1997.

[21] Grégoire Ribordy, J-D Gautier, Nicolas Gisin, Olivier Guinnard, and Hugo Zbinden. Automated'plug and play'quantum key distribution. *Electronics letters*, 34(22):2116–2117, 1998.

[22] Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3, 1992.

[23] Paul D Townsend, JG Rarity, and PR Tapster. Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, 29(7):634–635, 1993.

[24] Jacques Breguet, Antoine Muller, and Nicolas Gisin. Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits. *Journal of Modern Optics*, 41(12):2405–2412, 1994.

[25] JD Franson and H Ilves. Quantum cryptography using polarization feedback. *Journal of Modern Optics*, 41(12):2391–2396, 1994.

[26] Antoine Muller, Hugo Zbinden, and Nicolas Gisin. Underwater quantum coding. *Nature*, 378(6556):449, 1995.

[27] Miloslav Dušek, Ondřej Haderka, and Martin Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics communications*, 169(1-6):103–108, 1999.

[28] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330–1333, 2000.

[29] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5), 2003.

[30] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23), 2005.

[31] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23), 2005.

[32] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 207–235. The Royal Society, 2005.

[33] B. Kraus, N. 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(8), 2005.

[34] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[35] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2), 2009.

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

[37] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. 2014.

[38] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1), 2012.

[39] T. C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1), 1999.

[40] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2), 2000.

[41] M. D. Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Physical Review A*, 62(6), 2000.

[42] Ch. Silberhorn, N. Korolkova, and G. Leuchs. Quantum key distribution with bright entangled beams. *Physical Review Letters*, 88(16), 2002.

[43] 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 Journal of Physics*, 11(4):045023, 2009.

[44] Duan Huang, Peng Huang, Dakai Lin, and Guihua Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6(1), 2016.

[45] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1), 2009.

[46] Duan Huang, Peng Huang, Huasheng Li, Tao Wang, Yingming Zhou, and Guihua Zeng. Field demonstration of a continuous-variable quantum key distribution network. *Optics Letters*, 41(15):3511, 2016.

[47] Takuya Hirano, Tsubasa Ichikawa, Takuto Matsubara, Motoharu Ono, Yusuke Oguri, Ryo Namiki, Kenta Kasai, Ryutaroh Matsumoto, and Toyohiro Tsurumaru. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, 2(2):024010, 2017.

[48] Ryo Namiki, Akira Kitagawa, and Takuya Hirano. Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers. *Physical Review A*, 98(4), 2018.

[49] Panagiotis Papanastasiou and Stefano Pirandola. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective gaussian attacks.

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

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

[52] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review Letters*, 89(16), 2002.

[53] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Entanglement purification of gaussian continuous variable quantum states. *Physical Review Letters*, 84(17):4002–4005, 2000.

[54] Jaromír Fiurášek. Gaussian transformations and distillation of entangled gaussian states. *Physical Review Letters*, 89(13), 2002.

[55] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238, 2003.

[56] Tom Richardson, Rüdiger Urbanke, et al. Multi-edge type ldpc codes. In *Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California*, pages 24–25, 2002.

[57] CE Shannon. (1948)," a mathematical theory of communication", bell system technical journal, vol. 27, pp. 379-423 & 623-656, july & october. 1948.

[58] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 73(052316), 2006.

[59] G. Van Assche, J. Cardinal, and N. J. Cerf. Reconciliation of a quantum-distributed gaussian key. *IEEE Transactions on Information Theory*, 50(2):394–400, 2004.

[60] Kim-Chi Nguyen, Gilles Van Assche, and Nicolas J. Cerf. Side-information coding with turbo codes and its application to quantum key distribution. 2004.

[61] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over25kmwith an all-fiber continuous-variable system. *Physical Review A*, 76(4):42305, 2007.

[62] Bing Qi, Lei-Lei Huang, Li Qian, and Hoi-Kwong Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Physical Review A*, 76(5):052323, 2007.

[63] Paul Jouguet, Sébastien Kunz-Jacques, Thierry Debuisschert, Simon Fossier, Eleni Diamanti, Romain Alléaume, Rosa Tualle-Brouri, Philippe Grangier, Anthony Leverrier, Philippe Pache, and Philippe Painchault. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Optics Express*, 20(13):14030, 2012.

[64] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

[65] Yi-Chen 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 fiber. *arXiv preprint arXiv:2001.02555*, 2020.

[66] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the DARPA quantum network. In Eric J. Donkor, Andrew R. Pirich, and Howard E. Brandt, editors, *Quantum Information and Computation III*. SPIE, 2005.

[67] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The SECOQC quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[68] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J. B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden. Long term performance of the swissquantum quantum key distribution network in a field environment.

[69] Abdul Mirza and Francesco Petruccione. Realizing long-term quantum cryptography. *Journal of the Optical Society of America B*, 27(6):A185, 2010.

[70] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo QKD network. *Optics Express*, 19(11):10387, 2011.

[71] Alex Morrow, Don Hayford, and Matthieu Legre. Battelle QKD test bed. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012.

[72] Qantum communication hub. `https://www.quantumcommshub.net`. Accessed: 2019-01-07.

[73] Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Large scale quantum key distribution: challenges and solutions. *Optics express*, 26(18):24260–24273, 2018.

[74] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43, 2017.

[75] Stefano Pirandola, Raul García-Patrón, Samuel L Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Physical review letters*, 102(5):050503, 2009.

[76] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70, 2017.

[77] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[78] Frederic Grosshans and Nicolas J. Cerf. Continuous-variable quantum cryptography is secure against non-gaussian attacks. *Physical review letters*, 92(047905):047905, 2004.

[79] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Physical review letters*, 97(19):190502, 2006.

[80] Raúl García-Patrón and Nicolas J Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical review letters*, 97(19):190503, 2006.

[81] M.M. Wolf, G. Giedke, and J.I. Cirac. Extremality of gaussian quantum states. *Physical Review Letters*, 96(-):080502, 2006.

[82] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Physical Review Letters*, 95(18), 2005.

[83] Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. *Physical Review A*, 76(3), 2007.

[84] Raúl García-Patrón and Nicolas J. Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Physical Review Letters*, 102(13), 2009.

[85] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Physical Review Letters*, 89(3):037902, 2002.

[86] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005.

[87] 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.

[88] 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(6), 2010.

[89] Renato Renner. Security of quantum key distribution. 2005.

[90] Fabian Furrer, Torsten Franz, Mario Berta, Anthony Leverrier, Volkher B. Scholz, Marco Tomamichel, and Reinhard F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical review letters*, 109(100502):100502, 2012.

[91] Fabian Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Physical Review A*, 90(4), 2014.

[92] 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), 2013.

[93] Nathan Walk, Timothy C. Ralph, Thomas Symul, and Ping Koy Lam. Security of continuous-variable quantum cryptography with gaussian postselection. *Physical Review A*, 87(2), 2013.

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

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

[96] Eleni Diamanti and Anthony Leverrier. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy*, 17(9):6072–6092, 2015.

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

[98] 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):621–669, 2012.

[99] 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.

[100] U. Leonhardt and H. Paul. Measuring the quantum state of light. *Progress in Quantum Electronics*, 19(2):89–130, 1995.

[101] Wolfgang P. Schleich. *Quantum Optics in Phase Space*. Wiley-VCH Verlag GmbH & Co. KGaA, 2001.

[102] Radim Filip. Continuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, 77(2), 2008.

[103] Vladyslav C Usenko and Radim Filip. Squeezed-state quantum key distribution upon imperfect reconciliation. *New Journal of Physics*, 13(11):113007, 2011.

[104] Vladyslav C Usenko and Radim Filip. Trusted noise in continuous-variable quantum key distribution: A threat and a defense. *Entropy*, 18(1):20, 2016.

[105] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph. Continuous-variable quantum key distribution using thermal states. *Physical Review A*, 86(2), 2012.

[106] Vladyslav C Usenko and Frédéric Grosshans. Unidimensional continuous-variable quantum key distribution. *Physical Review A*, 92(6):062337, 2015.

[107] Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Single-quadrature continuous-variable quantum key distribution. *Quantum Information & Computation*, 16(13&14):1081–1095, 2016.

[108] Vladyslav C Usenko, Bettina Heim, Christian Peuntinger, Christoffer Wittmann, Christoph Marquardt, Gerd Leuchs, and Radim Filip. Entanglement of gaussian states and the applicability to quantum key distribution over fading channels. *New Journal of Physics*, 14(9):093048, 2012.

[109] Rudiger Urbanke Thomas J. Richardson. *Modern Coding Theory*. Cambridge University Press, 2014.

[110] Charles H Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229, 1988.

[111] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[112] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical review letters*, 77(13):2818, 1996.

[113] Xiangyu Wang, Yichen Zhang, Song Yu, and Hong Guo. High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. *IEEE Photonics Journal*, 10(3):1–9, 2018.

[114] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 5(4), 2015.

[115] Nedasadat Hosseinidehaj, Andrew M Lance, Thomas Symul, Nathan Walk, and Timothy C Ralph. Finite-size effects in continuous-variable quantum key distribution with gaussian postselection. *Physical Review A*, 101(5):052335, 2020.

[116] 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.

[117] Vladyslav C. Usenko and Radim Filip. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, 81(2):022318, 2010.

[118] Frédéric Grosshans, Nicolas J Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Ph Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Information & Computation*, 3(7):535–552, 2003.

[119] Raúl García-Patrón. *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution*. PhD thesis, Université Libre de Bruxelles, 2007.

[120] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23), 2007.

[121] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108(13), 2012.

[122] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Physical Review A*, 86(3), 2012.

[123] Vladyslav C. Usenko, Olena Kovalenko, and Radim Filip. Compensating the crosstalk in two-mode continuous-variable quantum communication. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2018.

[124] 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.

[125] Alastair M. Glass, David J. DiGiovanni, Thomas A. Strasser, Andrew J. Stentz, Richart E. Slusher, Alice E. White, A. Refik Kortan, and Benjamin J. Eggleton. Advances in fiber optics. *Bell Labs Technical Journal*, 5(1):168–187, aug 2002.

[126] Ruifang Dong, Mikael Lassen, Joel Heersink, Christoph Marquardt, Radim Filip, Gerd Leuchs, and Ulrik L Andersen. Continuous-variable entanglement distillation of non-gaussian mixed states. *Physical Review A*, 82(1):012312, 2010.

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

[128] Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard F 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, 2015.

[129] Jérôme Lodewyck and Philippe Grangier. Tight bound on the coherent-state quantum key distribution with heterodyne detection. *Physical Review A*, 76(2):022332, 2007.

[130] 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):–, 2004.

[131] Ryo Namiki, Masato Koashi, and Nobuyuki Imoto. Cloning and optimal gaussian individual attacks for a continuous-variable quantum key distribution using coherent states and reverse reconciliation. *Physical Review A*, 73(3):032302, 2006.

[132] Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Physical Review Letters*, 101(20), 2008.

[133] Nedasadat Hosseinidehaj, Nathan Walk, and Timothy C. Ralph. Optimal realistic attacks in continuous-variable quantum key distribution. 2018.

[134] Cosmo Lupo. Quantum data locking for secure communication against an eavesdropper with time-limited storage. *Entropy*, 17(5):3194–3204, 2015.

[135] Fabian Furrer, Tobias Gehring, Christian Schaffner, Christoph Pacher, Roman Schnabel, and Stephanie Wehner. Continuous-variable protocol for oblivious transfer in the noisy-storage model. *Nature Communications*, 9(1), 2018.

[136] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Physical Review A*, 97(5), 2018.

[137] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 136–145. IEEE, 2001.

[138] N. J. Cerf and C. Adami. Accessible information in quantum measurement. 1996.

[139] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, 2007.

[140] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[141] Xiangyu Wang, Yi-Chen Zhang, Zhengyu Li, Bingjie Xu, Song Yu, and Hong Guo. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *arXiv preprint arXiv:1703.04916*, 2017.

[142] Paul Jouguet. *Security and performance of continuous-variable quantum key distribution systems*. PhD thesis, 2013.

[143] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology*, pages 239–252. Springer, 1989.

[144] A. Holevo and R. Werner. Evaluating capacities of bosonic gaussian channels. *Physical Review A*, 63(3):–, 2001.

[145] R. Simon, S. Chaturvedi, and V. Srinivasan. Congruences and canonical forms for a positive matrix: Application to the schweinler–wigner extremum principle. *Journal of Mathematical Physics*, 40(7):3632–3642, 1999.

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

[147] 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. *Physical Review Letters*, 55(22):2409–2412, 1985.

[148] S Dwyer, L Barsotti, SSY Chua, M Evans, M Factourovich, D Gustafson, T Isogai, K Kawabe, A Khalaidovski, PK Lam, et al. Squeezed quadrature fluctuations in a gravitational wave detector using squeezed light. *Optics express*, 21(16):19047–19060, 2013.

[149] 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. *Physical Review Letters*, 117(11):110801, 2016.

[150] D. E. McCumber. Intensity fluctuations in the output of cw laser oscillators. i. *Physical Review*, 141(1):306–322, 1966.

[151] Hans-Albert Bachor, Timothy C Ralph, St Lucia, and Timothy C Ralph. *A guide to experiments in quantum optics*, volume 1. Wiley Online Library, 2004.

[152] Larry B. Stotts Sherman Karp. *Fundamentals of Electro-Optic Systems Design.* Cambridge University Press, 2018.

[153] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation – the theory of practical implementations. 2017.

[154] Christian S. Jacobsen, Tobias Gehring, and Ulrik L. Andersen. Continuous variable quantum key distribution with a noisy laser. 2015.

[155] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph. Quantum cryptography approaching the classical limit. *Physical Review Letters*, 105(11), 2010.

[156] Richard L Sutherland. *Handbook of nonlinear optics.* CRC press, 2003.

[157] 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.

[158] Thomas Brabec, editor. *Strong Field Laser Physics.* Springer New York, 2009.

[159] R Baumgartner and R Byer. Optical parametric amplification. *IEEE Journal of Quantum Electronics*, 15(6):432–444, 1979.

[160] Richard E Slusher, Ph Grangier, A LaPorta, B Yurke, and MJ Potasek. Pulsed squeezed light. *Physical review letters*, 59(22):2566, 1987.

[161] O. Aytür and P. Kumar. Squeezed-light generation with a mode-locked q-switched laser and detection by using a matched local oscillator. *Optics Letters*, 17:529, 1992.

[162] Chonghoon Kim and Prem Kumar. Quadrature-squeezed light detection using a self-generated matched local oscillator. *Physical review letters*, 73(12):1605, 1994.

[163] Ling-An Wu, H. J. Kimble, J. L. Hall, and Huifa Wu. Generation of squeezed states by parametric down conversion. *Physical Review Letters*, 57(20):2520–2523, 1986.

[164] E. S. Polzik, J. Carri, and H. J. Kimble. Spectroscopy with squeezed light. *Physical Review Letters*, 68(20):3020–3023, 1992.

[165] G Breitenbach, S Schiller, and J Mlynek. Measurement of the quantum states of squeezed light. *Nature*, 387(6632):471–475, 1997.

[166] PK Lam, TC Ralph, BC Buchler, DE McClelland, HA Bachor, and J Gao. Optimization and transfer of vacuum squeezing from an optical parametric oscillator. *Journal of Optics B: Quantum and Semiclassical Optics*, 1(4):469, 1999.

[167] Tobias Eberle, Sebastian Steinlechner, Jöran Bauchrowitz, Vitus Händchen, Henning Vahlbruch, Moritz Mehmet, Helge Müller-Ebhardt, and Roman Schnabel. Quantum enhancement of the zero-area sagnac interferometer topology for gravitational wave detection. *Physical review letters*, 104(25):251102, 2010.

[168] Henning Vahlbruch, Moritz Mehmet, Simon Chelkowski, Boris Hage, Alexander Franzen, Nico Lastzka, Stefan Goßler, Karsten Danzmann, and Roman Schnabel. Observation of squeezed light with 10-db quantum-noise reduction. *Physical review letters*, 100(3):033602, 2008.

[169] Yuishi Takeno, Mitsuyoshi Yukawa, Hidehiro Yonezawa, and Akira Furusawa. Observation of -9 dB quadrature squeezing with improvement of phase stability in homodyne measurement. *Optics Express*, 15(7):4321, 2007.

[170] Gerard J. Milburn D.F. Walls. *Quantum Optics*. Springer Berlin Heidelberg, 2007.

[171] Marlan O. Scully and M. Suhail Zubairy. Quantum optics, 1997.

[172] Timothy C. Ralph Hans-Albert Bachor. *A Guide to Experiments in Quantum Optics*. Wiley VCH Verlag GmbH, 2004.

[173] AI Lvovsky. Squeezed light. *Photonics Volume 1: Fundamentals of Photonics and Physics*, pages 121–164, 2015.

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

[175] Amnon Yariv and Pochi Yeh. Photonics: Optical electronics in modern communications, 2007.

[176] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Physical Review A*, 83(4):042312, 2011.

[177] Roberto Corvaja. Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection. *Physical Review A*, 95(2):022315, 2017.

[178] Wolfram Helwig, Wolfgang Mauerer, and Christine Silberhorn. Multimode states in decoy-based quantum-key-distribution protocols. *Physical Review A*, 80(5), 2009.

[179] T Kouadou, L La Volpe, S De, C Fabre, V Parigi, and N Treps. Single-pass generation of spatial and spectral multimode squeezed states of light. In *Frontiers in Optics*, pages FTh3B–7. Optical Society of America, 2019.

[180] 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*, 27(25):36154–36163, 2019.

[181] Luca La Volpe, Syamsundar De, Tiphaine Kouadou, Dmitri Horoshko, Mikhail Kolobov, Claude Fabre, Valentina Parigi, and Nicolas Treps. Multimode single-pass spatio-temporal squeezing. *arXiv preprint arXiv:2001.03972*, 2020.

[182] Jason Pereira and Stefano Pirandola. Hacking alice's box in continuous-variable quantum key distribution. *Physical Review A*, 98(6), dec 2018.

[183] Yujie Shen, Xiang Peng, Jian Yang, and Hong Guo. Continuous-variable quantum key distribution with gaussian source noise. *Physical Review A*, 83(5), 2011.

[184] Peng Huang, Guang-Qiang He, and Gui-Hua Zeng. Bound on noise of coherent source for secure continuous-variable quantum key distribution. *International Journal of Theoretical Physics*, 52(5):1572–1582, 2013.

[185] Jian Yang, Bingjie Xu, and Hong Guo. Source monitoring for continuous-variable quantum key distribution. *Physical Review A*, 86(4):042314, 2012.

[186] Ivan D Derkach, Christian Peuntinger, László Ruppert, Bettina Heim, Kevin Gunthner, Vladyslav C Usenko, Dominique Elser, Christoph Marquardt, Radim Filip, and Gerd Leuchs. Proof-of-principle test of coherent-state continuous variable quantum key distribution through turbulent atmosphere (conference presentation). In *Quantum Information Science and Technology II*, volume 9996, page 999605. International Society for Optics and Photonics, 2016.

[187] Kazuro Kikuchi. Fundamentals of coherent optical fiber communications. *Journal of Lightwave Technology*, 34(1):157–179, 2015.

[188] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Physical Review A*, 72(5):050303, 2005.

[189] Daniel B. S. Soh, Constantin Brif, Patrick J. Coles, Norbert Lütkenhaus, Ryan M. Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, 5(4), 2015.

[190] Adrien Marie and Romain Alléaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 95(1), 2017.

[191] Rameez Asif and Bill Buchanan. Recent progress in quantum-to-the-home networks. 2018.

[192] Fotini Karinou, Hans H Brunner, Chi-Hang Fred Fung, Lucian C Comandar, Stefano Bettelli, David Hillerkuss, Maxim Kuschnerov, Spiros Mikroulis, Dawei Wang, Changsong Xie, et al. Toward the integration of cv quantum key distribution in deployed optical networks. *IEEE Photonics Technology Letters*, 30(7):650–653, 2018.

[193] Yichen Zhang, Zhengyu Li, Ziyang Chen, Christian Weedbrook, Yijia Zhao, Xiangyu Wang, Yundi Huang, Chunchao Xu, Xiaoxiong Zhang, Zhenya Wang, et al. Continuous-variable qkd over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006, 2019.

[194] Tobias A Eriksson, Takuya Hirano, Motoharu Ono, Mikio Fujiwara, Ryo Namiki, Ken-ichiro Yoshino, Akio Tajima, Masahiro Takeoka, and Masahide Sasaki. Coexistence of continuous variable quantum key distribution and 7× 12.5 gbit/s classical channels. In *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pages 71–72. IEEE, 2018.

[195] Bing Qi, Wen Zhu, Li Qian, and Hoi-Kwong Lo. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, 12(10):103042, oct 2010.

[196] Govind P Agrawal. Nonlinear fiber optics. In *Nonlinear Science at the Dawn of the 21st Century*, pages 195–211. Springer, 2000.

[197] NA Peters, P Toliver, TE Chapuran, RJ Runser, SR McNown, CG Peterson, D Rosenberg, N Dallmann, RJ Hughes, KP McCabe, et al. Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of physics*, 11(4):045012, 2009.

[198] Tobias A. Eriksson, Takuya Hirano, Benjamin J. Puttnam, Georg Rademacher, Ruben S. Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada, and Masahide Sasaki. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. *Communications Physics*, 2(1):1–8, jan 2019.

[199] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[200] Akira Ishimaru. *Wave propagation and scattering in random media*, volume 2. Academic press New York, 1978.

[201] Shiyu Wang, Peng Huang, Tao Wang, and Guihua Zeng. Atmospheric effects on continuous-variable quantum key distribution. *New Journal of Physics*, 20(8):083037, 2018.

[202] Larry C Andrews, Ronald L Phillips, and Cynthia Y Hopen. *Laser beam scintillation with applications*, volume 99. SPIE press, 2001.

[203] Peter W Milonni, John H Carter, Charles G Peterson, and Richard J Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(8):S742, 2004.

[204] D Yu Vasylyev, AA Semenov, and W Vogel. Toward global quantum communication: beam wandering preserves nonclassicality. *Physical review letters*, 108(22):220501, 2012.

[205] Roberto Pierini. Effects of gravity on quantum key distribution. *arXiv preprint arXiv:1807.11855*, 2018.

[206] Ying Guo, Cailang Xie, Peng Huang, Jiawei Li, Ling Zhang, Duan Huang, and Guihua Zeng. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Physical Review A*, 97(5), 2018.

[207] HE Nistazakis, VD Assimakopoulos, and GS Tombras. Performance estimation of free space optical links over negative exponential atmospheric turbulence channels. *Optik*, 122(24):2191–2194, 2011.

[208] Zabih Ghassemlooy, Wasiu Oyewole Popoola, and Erich Leitgeb. Free-space optical communication using subearrier modulation in gamma-gamma atmospheric turbulence. In *2007 9th International Conference on Transparent Optical Networks*, volume 3, pages 156–160. IEEE, 2007.

[209] Ronald L Phillips and Larry C Andrews. Measured statistics of laser-light scattering in atmospheric turbulence. *JOSA*, 71(12):1440–1445, 1981.

[210] David T Wayne, Ronald L Phillips, Larry C Andrews, Troy Leclerc, Paul Sauer, and John Stryjewski. Comparing the log-normal and gamma-gamma model to experimental probability density functions of aperture averaging data. In *Free-Space Laser Communications X*, volume 7814, page 78140K. International Society for Optics and Photonics, 2010.

[211] Ivan Capraro, Andrea Tomaello, Alberto Dall'Arche, Francesca Gerlin, Ruper Ursin, Giuseppe Vallone, and Paolo Villoresi. Impact of turbulence in long range quantum and classical communications. *Physical review letters*, 109(20):200502, 2012.

[212] *Optical Communication*. IntechOpen, 2012.

[213] Matest M Agrest, Michail S Maksimov, Henry Eason Fettis, JW Goresh, and DA Lee. *Theory of incomplete cylindrical functions and their applications*, volume 160. Springer, 1971.

[214] Frank Bowman. *Introduction to Bessel functions*. Courier Corporation, 2012.

[215] Hisashi Kobayashi, Brian L Mark, and William Turin. *Probability, random processes, and statistical analysis: applications to communications, signal processing, queueing theory and mathematical finance*. Cambridge University Press, 2011.

[216] C Erven, B Heim, E Meyer-Scott, JP Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, 2012.

[217] Ying Guo, Cailang Xie, Qin Liao, Wei Zhao, Guihua Zeng, and Duan Huang. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *PRA*, 96:022320, 2017.

[218] Kevin Günthner, Imran Khan, Dominique Elser, Birgit Stiller, Ömer Bayraktar, Christian R Müller, Karen Saucke, Daniel Tröndle, Frank Heine, Stefan Seel, et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica*, 4(6):611–616, 2017.

[219] Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, and Lajos Hanzo. Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook. *IEEE Communications Surveys & Tutorials*, 21(1):881–919, 2018.

[220] Daniele Dequal, Luis Trigo Vidarte, Victor Roman Rodriguez, Giuseppe Vallone, Paolo Villoresi, Anthony Leverrier, and Eleni Diamanti. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *arXiv preprint arXiv:2002.02002*, 2020.

[221] Carlo Liorni, Hermann Kampermann, and Dagmar Bruß. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New Journal of Physics*, 21(9):093055, 2019.

[222] Christopher J Pugh, Jean-Francois Lavigne, Jean-Philippe Bourgoin, Brendon L Higgins, and Thomas Jennewein. Adaptive optics benefit for quantum key distribution uplink from ground to a satellite. *arXiv preprint arXiv:1906.04193*, 2019.

[223] Jean-Philippe Bourgoin, Brendon L Higgins, Nikolay Gigov, Catherine Holloway, Christopher J Pugh, Sarah Kaiser, Miles Cranmer, and Thomas Jennewein. Free-space quantum key distribution to a moving receiver. *Optics express*, 23(26):33437–33447, 2015.

[224] Daniel KL Oi, Alex Ling, Giuseppe Vallone, Paolo Villoresi, Steve Greenland, Emma Kerr, Malcolm Macdonald, Harald Weinfurter, Hans Kuiper, Edoardo Charbon, et al. Cubesat quantum communications mission. *EPJ Quantum Technology*, 4(1):6, 2017.

[225] Cristian Bonato, Andrea Tomaello, Vania Da Deppo, Giampiero Naletto, and Paolo Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[226] Haoyu Qi, Kamil Brádler, Christian Weedbrook, and Saikat Guha. Ultimate limit of quantum beam tracking.

[227] Nedasadat Hosseinidehaj, Andrew M Lance, Thomas Symul, Nathan Walk, and Timothy C Ralph. Finite-size effects in continuous-variable qkd with gaussian post-selection. *arXiv preprint arXiv:1912.09638*, 2019.

[228] Nedasadat Hosseinidehaj, Nathan Walk, and Timothy C Ralph. Composable finite-size effects in free-space cv-qkd systems. *arXiv preprint arXiv:2002.03476*, 2020.

[229] Horace P Yuen and Vincent WS Chan. Noise in homodyne and heterodyne detection. *Optics letters*, 8(3):177–179, 1983.

[230] John R Barry and Edward A Lee. Performance of coherent optical receivers. *Proceedings of the IEEE*, 78(8):1369–1394, 1990.

[231] Susumu Machida and YOSHIHISA Yamamoto. Quantum-limited operation of balanced mixer homodyne and heterodyne receivers. *IEEE journal of quantum electronics*, 22(5):617–624, 1986.

[232] Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, AI Lvovsky, and Liang Tian. A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution. *New Journal of Physics*, 13(1):013003, 2011.

[233] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A*, 87(6):062313, 2013.

[234] Hao Qin, Rupesh Kumar, and Romain Alléaume. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A*, 94(1), 2016.

[235] Hauke Hansen, T Aichele, C Hettich, P Lodahl, AI Lvovsky, J Mlynek, and S Schiller. Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements. *Optics Letters*, 26(21):1714–1716, 2001.

[236] Merlin Cooper, Christoph Söller, and Brian J Smith. High-stability time-domain balanced homodyne detector for ultrafast optical pulse applications. *Journal of Modern Optics*, 60(8):611–616, 2013.

[237] Ranjeet Kumar, Erick Barrios, Andrew MacRae, E Cairns, EH Huntington, and AI Lvovsky. Versatile wideband balanced detector for quantum optical homodyne tomography. *Optics Communications*, 285(24):5259–5267, 2012.

[238] Jürgen Appel, Dallas Hoffman, Eden Figueroa, and AI Lvovsky. Electronic noise in optical homodyne tomography. *Physical Review A*, 75(3):035802, 2007.

[239] 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, 2015.

[240] Weiqi Liu, Jinye Peng, Peng Huang, Duan Huang, and Guihua Zeng. Monitoring of continuous-variable quantum key distribution system in real environment. *Optics express*, 25(16):19429–19443, 2017.

[241] Wilhelmus Jacobus Witteman. *Detection and Signal Processing.* Springer-Verlag GmbH, 2006.

[242] 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. *Physical Review A*, 88(2):022339, 2013.

[243] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, Ming Gui, Yan-Li Zhou, and Lin-Mei Liang. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Physical Review A*, 89(3), 2014.

[244] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Physical Review A*, 87(6), 2013.

[245] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Physical Review A*, 87(5), 2013.

[246] Jing-Zheng Huang, Sébastien Kunz-Jacques, Paul Jouguet, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking on quantum key distribution using homodyne detection. *Physical Review A*, 89(3), 2014.

[247] Hao Qin, Rupesh Kumar, Vadim Makarov, and Romain Alléaume. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Physical Review A*, 98(1), 2018.

[248] 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.

[249] Zhengyu Li, Yi-Chen Zhang, Feihu Xu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 89(5), 2014.

[250] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9(6):397–402, 2015.

[251] Nedasadat Hosseinidehaj and Robert Malaney. Cv-mdi quantum key distribution via satellite. *arXiv preprint arXiv:1605.05445*, 2016.

[252] Hong-Xin Ma, Peng Huang, Dong-Yun Bai, Shi-Yu Wang, Wan-Su Bao, and Gui-Hua Zeng. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. *Physical Review A*, 97(4):042329, 2018.

[253] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[254] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1), 2005.

[255] Gilles Van Assche. *Quantum Cryptography and Secret-Key Distillation*. CAMBRIDGE UNIV PR, 2006.

[256] 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):1301–1350, 2009.

[257] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature photonics*, 3(12):706, 2009.

[258] Khabat Heshami, Duncan G England, Peter C Humphreys, Philip J Bustard, Victor M Acosta, Joshua Nunn, and Benjamin J Sussman. Quantum memories: emerging applications and recent advances. *Journal of modern optics*, 63(20):2005–2028, 2016.

[259] P. Gemmell and N. Naor. Codes for interactive authentication. In *Advances in Cryptology — CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, page 355–367, 1993.

[260] C. Pacher, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger, and J.-Å. Larsson. Attacks on quantum key distribution protocols that employ non-ITS authentication. *Quantum Information Processing*, 15(1):327–362, 2015.

[261] Douglas R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994.

[262] R. Renner and S. Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In *Advances in Cryptology — CRYPTO '03*, Lecture Notes in Computer Science, page 78–95, 2003.

[263] R. Renner and S. Wolf. The exact price for unconditionally secure asymmetric cryptography. In *Advances in Cryptology —EUROCRYPT '04*, Lecture Notes in Computer Science, page 109–125, 2004.

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

[265] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Physical Review Letters*, 120(22), 2018.

[266] Claude E Shannon. Analogue of the vernam system for continuous time series. *Memorandum MM*, pages 43–110, 1943.

[267] Paul Jouguet and Sébastien Kunz-Jacques. High performance error correction for quantum key distribution using polar codes. *Quantum Information and Computation*, 14(3&4), 2013.

[268] Robert G. Gallager. Low-density parity-check codes, 1963.

[269] Rudiger Urbanke Thomas J. Richardson. *Modern Coding Theory*. CAMBRIDGE UNIV PR, 2008.

[270] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for continuous-variable quantum key distribution. *Physical Review A*, 77(042325), 2008.

[271] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, 84(6), 2011.

[272] J.Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[273] Masahito Hayashi and Toyohiro Tsurumaru. More efficient privacy amplification with less random seeds via dual universal hash function. *IEEE Transactions on Information Theory*, 62(4):2213–2232, 2016.

[274] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Physical Review Letters*, 89(13), 2002.

[275] Akira Kitagawa, Masahiro Takeoka, Masahide Sasaki, and Anthony Chefles. Entanglement evaluation of non-gaussian states generated by photon subtraction from squeezed states. *Physical Review A*, 73(4), 2006.

[276] Hiroki Takahashi, Jonas S. Neergaard-Nielsen, Makoto Takeuchi, Masahiro Takeoka, Kazuhiro Hayasaka, Akira Furusawa, and Masahide Sasaki. Entanglement distillation from gaussian input states. *Nature Photonics*, 4(3):178–181, 2010.

[277] Christian S Jacobsen, Lars S Madsen, Vladyslav C Usenko, Radim Filip, and Ulrik L Andersen. Complete elimination of information leakage in continuous-variable quantum communication channels. *npj Quantum Information*, 4(1):32, 2018.

[278] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20), 2008.

[279] Raymond Y Q Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024, 2009.

[280] Xueying Zhang, Yichen Zhang, Yijia Zhao, Xiangyu Wang, Song Yu, and Hong Guo. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 96(4):042334, 2017.

[281] Metin Sabuncu, Radim Filip, Gerd Leuchs, and Ulrik L Andersen. Environment-assisted quantum-information correction for continuous variables. *Physical Review a*, 81(1):012325, 2010.

[282] Radim Filip. Security of coherent-state key distribution through an amplifying channel. *Physical Review A*, 77(3):032347, 2008.

[283] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863–1869, 1995.

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

[285] Nedasadat Hosseinidehaj and Robert Malaney. CV-QKD with gaussian and non-gaussian entangled states over satellite-based channels. In *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016.

[286] Martin Grabner and Vaclav Kvicera. Measurement of the structure constant of refractivity at optical wavelengths using a scintillometer. *Radioengineering*, 21(1):455–458, 2012.

[287] Laszlo Ruppert, Christian Peuntinger, Bettina Heim, KEvin Günthner, Vladyslav C Usenko, Dominique Elser, Gerd Leuchs, Radim Filip, and Christoph Marquardt. Fading channel estimation for free-space continuous-variable secure quantum communication. *New Journal of Physics*, 21(12):123036, dec 2019.

[288] Radim Filip, Ladislav Mišta, and Petr Marek. Elimination of mode coupling in multimode continuous-variable key distribution. *Physical Review A*, 71(1):012323, jan 2005.