

Continuous-variable quantum communication

Vladyslav C. Usenko*

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

Antonio Acín

ICFO-Institut de Ciències Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain and

ICREA - Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

Romain Alléaume

Télécom Paris-LTCl, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

Ulrik L. Andersen

Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800, Kongens Lyngby, Denmark

Eleni Diamanti

Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005, Paris, France

Tobias Gehring

Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800, Kongens Lyngby, Denmark

Adnan A.E. Hajomer

Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800, Kongens Lyngby, Denmark

Florian Kanitschar

Vienna Center for Quantum Science and Technology (VCQ), Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria and

AIT Austrian Institute of Technology, Center for Digital Safety&Security, Giefinggasse 4, 1210 Vienna, Austria

Christoph Pacher

AIT Austrian Institute of Technology, Center for Digital Safety&Security, Giefinggasse 4, 1210 Vienna, Austria and fragmentIX Storage Solutions GmbH, Wohllebengasse 10/7, 1040 Vienna, Austria

Stefano Pirandola

Department of Computer Science, University of York, York YO10 5GH, United Kingdom

Valerio Pruneri

ICFO-Institut de Ciències Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain and

ICREA - Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

(Dated: December 11, 2025)

Tremendous progress in experimental quantum optics during the past decades enabled the advent of quantum technologies, one of which is quantum communication. Aimed at novel methods for more secure or efficient information transfer, quantum communication has developed into an active field of research and proceeds toward full-scale implementations and industrialization. Continuous-variable methods of multi-photon quantum state preparation, manipulation, and coherent detection, as well as the respective theoretical tools of phase-space quantum optics, offer the possibility to make quantum communication efficient, applicable and accessible, thus boosting the development of the field. We review the methodology, techniques and protocols of continuous-variable quantum communication, from the first theoretical ideas, through milestone implementations, to the recent developments, covering quantum key distribution as well as other quantum communication schemes, suggested on the basis of continuous-variable states and measurements.

Keywords: Quantum communication, Quantum information processing with continuous variables, Quantum channels, Quantum cryptography, Homodyne & heterodyne detection

Contents

I. Introduction	2
II. Preliminaries	3
A. Quantum key distribution	3
B. Quantum communication beyond QKD	5
C. Continuous-variable quantum systems	7
1. Gaussian quantum states	7
2. Gaussian operations	8
3. Gaussian channels	9
4. Coherent detection	9
D. Continuous-variable quantum information theory	10
III. Continuous-variable quantum key distribution	11
A. CV-QKD protocols	12
1. Coherent-state protocols	13
2. Squeezed-state protocols	14
3. Entanglement-based protocols	14
4. Two-way protocols	14
5. Measurement-device independent protocols	14
6. Thermal-state protocols	14
B. Theoretical security	15
1. Notions of composable security	15
2. Individual attacks and channel models	17
3. Asymptotic security via Gaussian extremality	18
4. Asymptotic security without Gaussian extremality	20
5. Finite-size security	21
6. Limits of CV-QKD	25
C. Practical implementation of CV-QKD	26
1. Quadrature modulation	27
2. Coherent detection	28
3. Digital signal processing	29
4. Squeezed signal states	30
5. Measurement-device independent protocols	32
6. Fiber and free-space channels	33
D. Implementation security	34
1. Source and detection imperfections	34
2. Security side channels and loopholes	35
3. Security certification	37
E. Post-processing	38
1. Post-processing performance	38
2. Sifting	39
3. Post-selection	39
4. Parameter estimation	40
5. Information Reconciliation/Error Correction	40
6. Privacy amplification	41
7. Message Authentication	42
F. Advances in CV-QKD	42
1. Quantum amplifiers and repeaters	43
2. Post-selection	44
3. Photonic integration	44
4. Channel multiplexing and co-existence	45
IV. CV quantum communication beyond QKD	46
A. Quantum secure direct communication	46
B. Quantum dense coding	47
C. Quantum digital signatures	48
D. Quantum authentication	48
E. Quantum oblivious transfer	49
F. Quantum teleportation	50

G. GKP encoding	52
-----------------	----

V. Summary and outlook	52
-------------------------------	----

Acknowledgments	54
------------------------	----

References	54
-------------------	----

I. INTRODUCTION

Quantum communication (Gisin and Thew, 2007) is the research field at the intersection of quantum physics and information science that studies and develops methods for distribution of quantum states and for information exchange using those states. While mostly associated with quantum-based information security, enabled by quantum cryptography (Pirandola *et al.*, 2020), quantum communication also provides the basis for other communication tasks, which rely on the principles of quantum physics. Naturally based on the quantum states of light due to their relatively low coupling to the environment and long coherence times, quantum communication was boosted by immense advancements in experimental quantum optics, achieved in the past decades. Being an integral part of the second quantum revolution (Dowling and Milburn, 2003), quantum communication became a quantum technology, which revolutionized the communication itself by enabling essentially new principles and properties of information exchange.

In the current review, we present the field of quantum communication based on continuous variables of light, which can be effectively manipulated using practical quantum-optical techniques and measured by means of highly efficient coherent detection. Contrary to discrete-variable (DV) quantum communication, which typically relies on direct photodetection and which is largely based on the corpuscular treatment of light, ideally using single-photon states, continuous-variable (CV) can be seen as utilizing wave-type properties of light through manipulation and coherent detection of generally multi-photon quantum states (see illustration in Fig. 1). Being complementary to the DV approach, CV quantum communication can offer certain advantages, both quantitative and qualitative, particularly concerning efficiency, cost or scalability. During more than two decades of its existence, CV quantum communication has developed from basic ideas to practical realizations and even industrial implementations. Yet it remains an active field of research, aimed at making CV quantum communication more efficient, mature, useful and cost-effective. In the current review we therefore discuss principles, applications, practical aspects, limitations and perspectives of CV quantum communication, providing an overview of this modern and dynamic field of research.

*Electronic address: usenko@optics.upol.cz

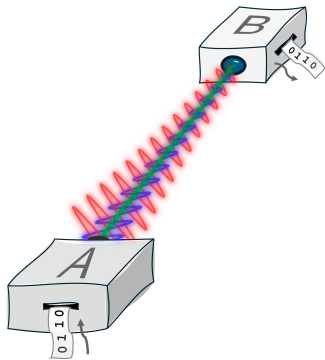


FIG. 1 CV quantum communication uses wave properties of generally multi-photon light to transmit information by encoding it into conjugate observables of electromagnetic field in the transmitter *A* and obtaining it from the results of coherent detection in the receiver *B*, enabling, e.g., stronger information security than in classical communication and with potentially higher efficiency compared to single-photon DV quantum communication.

The review is structured as follows: in Sec. II we recapitulate the methods of quantum communication, historically developed on the basis of DV states, starting from quantum key distribution (QKD) protocols, then describing protocols beyond QKD, and we also provide a brief overview of CV systems, covering CV states, including the broadly used Gaussian ones, respective Gaussian operations, and coherent detection methods; in Sec. III we review CV-QKD, which is the most advanced and developed branch of CV quantum communication, covering its protocols, theoretical security proofs, tools for its practical implementation and security aspects of the implementation, post-processing algorithms used in CV-QKD, and the recent advancements in the field; in Sec. IV we discuss the methods of CV quantum communication beyond QKD, which are less advanced, but are promising for further development; and we conclude the review with a summary and future outlook. Our review is the first one, to the best of our knowledge, covering all major methods of CV quantum communication, presenting principles, modern trends and recent developments in CV-QKD as well as CV protocols beyond QKD. Several review articles, related to CV quantum communication, were published earlier. Quantum cryptography using DV states and measurements was discussed in (Gisin *et al.*, 2002), introducing basic principles and concepts, also used in CV-QKD. Practical security of QKD was reviewed in (Scarani *et al.*, 2009), which was largely focused on DV-QKD, but also briefly discussed CV protocols. A CV quantum information review (Braunstein and Van Loock, 2005) covered the underlining principles and methods behind CV quantum communication, such as CV quantum entanglement, described several quantum communication methods, including QKD, dense coding, and quantum teleportation, as well as other applications of CV information, e.g., quantum computation.

The Gaussian quantum information review (Weedbrook *et al.*, 2012a) described tools of quantum information processing using Gaussian states, such as covariance matrix formalism, which largely remain relevant for the field of CV quantum communication, and covered many of the ongoing developments in the field, such as finite-size security analysis or discretely-modulated protocols, while also describing quantum computation with Gaussian states. The review on CV quantum information (Adesso *et al.*, 2014) presented mathematical structures behind Gaussian quantum information and quantification of CV correlations. Security of CV-QKD and its state-of-the-art experimental implementations were covered in the review (Diamanti and Leverrier, 2015). The review on QKD with practical devices (Xu *et al.*, 2020) reported relevant topics for QKD security, e.g., quantum side channels or quantum hacking, while briefly discussing how they apply to CV-QKD. The review on advances in quantum cryptography (Pirandola *et al.*, 2020) described modern trends in the field of QKD with much attention to CV-QKD protocols, their security analysis and practical implementation. The recent review on CV-QKD (Zhang *et al.*, 2024a) contains practical details of CV-QKD implementations. For convenience, in Table I we present the list of abbreviations, used in the review.

II. PRELIMINARIES

As historically most of the quantum communication methods were first developed on the basis of DV techniques, we start our review with an introduction to DV quantum communication.

A. Quantum key distribution

QKD (Gisin *et al.*, 2002; Pirandola *et al.*, 2020; Scarani *et al.*, 2009) is one of the most mature and important directions within quantum communication, having its goal in the development of protocols for provably secure distribution of secret cryptographic keys. Together with classical encryption algorithms, it provides legitimate users with the methods of secure communication. Such methods are then based on the principles of quantum physics and generally do not rely on mathematical complexity assumptions, which can be overturned either by development of quantum computing or progress in classical computations.

QKD was first suggested as BB84 protocol (named so after its authors, Bennett and Brassard) in (Bennett and Brassard, 1984) using polarization states of single photons as *qubits* (quantum bit states, generally being in superpositions of the two basis states). By using non-orthogonal states and relying on the no-cloning theorem, which forbids perfect copying of unknown quantum states (Wootters and Zurek, 1982), the protocol enables the trusted (honest) parties to ensure the security of

Abbreviation	Meaning
1sDI	One-sided device-independent
AEP	Asymptotic equipartition property
BB84	Bennett-Brassard-1984
CV	Continuous-variable
CW	Continuous-wave
DI	Device-independent
DM	Discrete modulation
DR	Direct reconciliation
DSP	Digital signal processing
DV	Discrete-variable
E91	Ekert-1991
EAL	Evaluation assurance level
EAT	Entropy accumulation theorem
EB	Entanglement-based
EOM	Electro-optical modulator
EPR	Einstein-Podolsky-Rosen
FER	Frame error rate
FFT	Fast Fourier transform
GG02	Grosshans-Grangier-2002
GKP	Gottesman-Kitaev-Preskill
GM	Gaussian modulation
i.i.d.	Independent and identically distributed
InP	Indium phosphide
IQ	In-phase and quadrature
KTP	Potassium titanyl phosphate
LDPC	Low-density parity-check
LHL	Leftover hashing lemma
LLO	“Local” local oscillator
LO	Local oscillator
MD	Multi-dimensional
MDI	Measurement-device independent
NLA	Noiseless linear amplifier
OPA	Optical parametric amplifier
OPO	Optical parametric oscillator
P&M	Prepare-and-measure
PDC	Parametric down-conversion
PIA	Phase-insensitive amplifier
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PP	Protection profile
PQC	Post-quantum cryptographic
PSA	Phase-sensitive amplifier
QA	Quantum authentication
QAM	Quadrature amplitude modulation
QBER	Quantum bit error rate
QDC	Quantum dense coding
QDS	Quantum digital signatures
QKD	Quantum key distribution
QOT	Quantum oblivious transfer
QPSK	Quadrature phase-shift keying
QSDC	Quantum secure direct communication
QT	Quantum teleportation
RCI	Reverse coherent information
RF	Radio-frequency
RR	Reverse reconciliation
SDP	Semi-definite programming
SNR	Signal-to-noise ratio
SNU	Shot-noise unit
TMSV	Two-mode squeezed vacuum
UD	Uni-dimensional
WDM	Wavelength division multiplexing

TABLE I Abbreviations used in the review.

the key, obtained from polarization encoding and measurements, and processed over an authenticated classical channel. By randomly switching the preparation and measurement bases, the trusted parties accumulate the so-called raw key, which is then sifted during the bases reconciliation stage and is further classically processed to obtain the secret key.

The *entanglement-based* (EB) E91 QKD protocol was suggested in (Ekert, 1991) almost a decade later and uses entangled-photon pairs (hence, entangled qubits) so that each of the photons is measured by one of the trusted parties. By randomly switching between three bases settings, the trusted parties can either verify the violation of Bell inequalities (in the incompatible bases) (Aspect *et al.*, 1982) or obtain already the sifted key, once the bases coincide. The security of the scheme relies on the fact that an eavesdropper attempting to intercept the key would break the nonlocal correlations and stop the Bell inequality violation. This reasoning was later extended to the notion of device-independent security, discussed further in this subsection. It was later shown in (Bennett *et al.*, 1992c) that entangled photon pairs can be equivalently used to implement the BB84 protocol without the need for Bell inequality violation, hence randomly switching between two detection bases. This equivalence between prepare-and-measure (P&M) version of the protocol, when Alice prepares the states, and Bob performs their measurement, and EB version became an important feature of QKD protocols, enabling their formal information-theoretical security analysis.

The first experimental test of QKD using the BB84 protocol was reported in (Bennett *et al.*, 1992a) using weak coherent pulses for emulating single-photon states. However, it was pointed out that such realization is vulnerable to photon-number splitting attack (also known as beam splitting attack) allowing an eavesdropper to exploit multi-photon pulses for error-free interception of key bits. It was later shown (Brassard *et al.*, 2000) that such an attack in combination with limited detection efficiency and dark counts (when a photo-detector, working in the Geiger mode, produces a fake click in the absence of an incoming photon), strongly limits the practical applicability of QKD. To overcome the limitation, modified QKD protocols were proposed, such as SARG (Scarani *et al.*, 2004), in which every key bit is encoded into a pair of non-orthogonal states, hence reducing the efficiency of photon-number splitting attack for an eavesdropper, or the decoy-state protocol (Hwang, 2003), using additional multi-photon states to detect the splitting. These developments enabled numerous experimental realizations of QKD in long-distance fibers (Korzh *et al.*, 2015) and in free-space (Ursin *et al.*, 2007) or intercontinental satellite-based channels (Liao *et al.*, 2018).

The security analysis of QKD protocols is largely defined by the set of assumptions on the protocol implementation and on the capabilities of a malicious eavesdropper. One major assumption and necessity to achieve a secure QKD protocol is that the classical communi-

cation of the QKD protocol is transmitted through an authenticated channel to prevent an eavesdropper from performing a man-in-the-middle attack on either the classical channel or jointly on the classical and the quantum channel. An authenticated classical channel can be established from a non-authenticated one by using message authentication codes that in turn consume short keys.

The analysis of attacks on the quantum channel alone is typically based on evaluating the Devetak-Winter rate (Devetak and Winter, 2005) for the achievable secret key, which characterizes the information advantage of the trusted parties over an eavesdropper, capable of storing probe quantum states in a quantum memory. While not generally relying on particular attack models, this approach has to be extended towards the finite-size regime, when statistical aspects of limited data sets have to be taken into account (Tomamichel *et al.*, 2012). The security of a QKD protocol can then be quantified in the context of composable security (Portmann and Renner, 2022), allowing us to evaluate the security of a whole cryptographic system, which contains the given protocol.

However, gaps between theoretical security and practical implementations are always possible and can be exploited by an eavesdropper as, for example, in the blinding attack on the single-photon detectors (Lydersen *et al.*, 2010). To rule out such *quantum hacking* attacks the assumptions on the devices used for QKD can be waived in the device-independent approach.

An important feature of the E91 protocol was the reliance of its security on the violation of Bell inequalities. While this effect is not required for the EB implementation of BB84 and similar QKD protocols, it can be used to waive the assumption on the trusted nature of the devices, namely source and detectors. The resulting *device-independent* (DI) protocol (Acín *et al.*, 2007; Vazirani and Vidick, 2014) can in principle be secure without making assumptions on the internal working of the devices. In practice this means that the trusted parties do not need to fully characterize and calibrate the devices, relying solely on the loophole-free violation of Bell inequality (typically its CHSH version (Clauser *et al.*, 1969)) from the measurement statistics, which can be seen as a part of the more general device self-checking approach (Mayers and Yao, 1998). However, implementation of DI QKD protocols remains demanding in terms of highly pure entanglement, required for their security, and high sensitivity to practical imperfections, which particularly limits the distances at which DI QKD can be implemented.

It is also possible to remove only the trust assumption on the measurement devices, which can rule out quantum hacking attacks on the detectors. Such attacks are more likely to happen since the detectors are susceptible to incoming light, potentially manipulated by an attacker. In this intermediate approach, called *measurement-device independent* (MDI) QKD, the trusted parties only send their modulated states to a middle station, which then performs a Bell-type measurement and announces the

outcomes, allowing the trusted parties to establish correlations on their data, sufficient for distilling a secret key (Braunstein and Pirandola, 2012; Lo *et al.*, 2012). The detection can then be assumed to be under the full control of an eavesdropper because tampering with the detection outcomes can be revealed by the trusted parties. While managing to rule out the attacks on the measurement devices, the MDI protocols also generally offer higher robustness and better performance compared to DI QKD.

Another intermediate scenario is possible, when only one of the trusted parties trusts their measurement apparatus, which is the case of *one-sided device-independent* protocols (1sDI) (Branciard *et al.*, 2012)

B. Quantum communication beyond QKD

While QKD is the most commonly developed application of quantum communication, the field offers several more directions, in which quantum effects bring enhancements (particularly, physics-based security instead of the computational one) to communication methods (mainly cryptographic primitives), and we further give a brief overview on the major ones, which are also being developed within CV quantum communication.

The goal of *quantum secure direct communication* (QSDC) is the family of the protocols, aimed to ensure the security of the directly transmitted information so that its acceptably small part is gained by an eavesdropper, while not relying on QKD. This allows trusted users to directly and deterministically share their secret messages while making the protocols more technically demanding compared to QKD (see (Pan *et al.*, 2024) for the recent review on QSDC). The first QSDC protocol was proposed in (Long and Liu, 2002) as the deterministic QKD of a pre-generated key with no information leakage. The deterministic secure quantum communication was proposed in (Beige *et al.*, 2002) using single-photon states to simultaneously encode two qubits in different bases, accompanied by a classically shared secret key. Another deterministic secure direct communication protocol was proposed on the basis of entangled pairs and a quantum memory on the sender side (Boström and Felbinger, 2002). A protocol for directly sharing a secret key encoded in the sequences of single-photon states, sent back and forth between the trusted parties and stored in quantum memories, was suggested in (Deng and Long, 2004). It was later extended to EB realization (Deng *et al.*, 2003) with reportedly higher performance. QSDC was then experimentally tested using single-photon (Hu *et al.*, 2016) or entangled states (Zhang *et al.*, 2017) with atomic quantum memories.

Quantum dense coding (QDC, also referred to as quantum super-dense coding) allows communicating parties to share more classical bits of information with fewer shared qubits. QDC was first theoretically proposed in (Bennett and Wiesner, 1992), based on an entangled pair,

distributed between two parties, so that after an operation on one particle, its transfer and joint measurement on the other side of the channel, two classical bits (encoded into one of four possible qubit operations) become known to both the parties. QDC was further combined with QSDC in (Wang *et al.*, 2005) and experimentally tested using atomic qubit states (Schaetz *et al.*, 2004) or photonic qubits distributed over optical fibers (Williams *et al.*, 2017).

Quantum digital signature (QDS) protocols are the quantum counterpart of the classical digital signature methods, which are used to verify the authenticity of communicated messages. Similarly to the classical protocols, the quantum digital signature supposes the use of private and public secret keys. The keys are related through a quantum analog of the classical one-way functions. The QDS principles were first described in (Gottesman and Chuang, 2001), showing that multiple remote receivers can validate the signature of a message sender. This is achieved by each of the receivers having a copy of the sender's public quantum key (also referred to as a quantum signature), created, using a quantum one-way function, from a classical private key. The QDS protocol with a sender and two receivers was experimentally demonstrated in (Clarke *et al.*, 2012) using phase-encoded coherent states of light. The signed messages were shown secure against forging and repudiation by considering typical attack scenarios. The receiver however requires a long-term quantum memory for storing the public quantum key. The signed message is then verified by interfering the stored key with a set of states created according to the classical description of the sender's private key, sent along with the message. This requirement was waived in (Dunjko *et al.*, 2014) by allowing the remote receiver to measure the public quantum key instead of storing it in the quantum memory. The classical measurement outcomes are then used to verify the messages, which is however probabilistic. The protocol was realized experimentally (Collins *et al.*, 2014) using only linear-optical components and photodetectors, enabling a more efficient measurement technique with higher probabilities of success.

Quantum authentication (QA) is a family of quantum protocols for verification of the identity of a message sender and/or the integrity of the message. In this regard, it is closely related to QDS, which can be seen as multi-user authentication, and to QKD, which requires authentication in the key post-processing stage but can also provide authentication once the secret key is distributed. Furthermore, QA schemes can vary depending on whether a message is classical or quantum (i.e. if it is a sequence of classical data or quantum states). The possibility of using quantum resources for message authentication was first discussed in (Crépeau and Salvail, 1995), where two trusted parties were shown to be able to verify their mutual knowledge of a classical data string, without revealing the data itself (this way the QA scheme is related to the oblivious transfer protocols discussed in the

next subsection). Quantum protocols for the identification of classical messages, combining classical identification and QKD, were proposed and experimentally tested in (Dušek *et al.*, 1999), depending on whether the public channel between the trusted parties is fully controlled by an eavesdropper or not. Quantum enhancement of classical message authentication was shown in (Curty and Santos, 2001) with one-qubit key reportedly being a sufficient resource for proving the integrity of a classical bit. Furthermore, the efficiency of QA of classical messages was improved to two bits by one qubit (Hong *et al.*, 2017). Authentication of quantum messages by their encryption was addressed in (Barnum *et al.*, 2002), where an asymptotically optimal protocol for authenticating one qubit with two classical bits was presented along with the proof of impossibility to digitally sign quantum states.

Quantum oblivious transfer (QOT) is the quantum version of a communication scheme, in which a sending party transfers one or more of many possible messages to a receiver, while not knowing which (and if any) messages were sent. This essential cryptographic primitive was shown to provide security of multiparty computation (Kilian, 1988). Typically the so-called $1 - \text{out} - \text{of} - 2$ scheme is studied, when one message is communicated out of two, with possible generalizations to the schemes, when k out of n messages are communicated. The $1 - \text{out} - \text{of} - n$ case is commonly referred to as the private database query. Development of QOT protocols was first largely based on reduction to quantum bit commitment (Bennett *et al.*, 1992b) until the latter was shown insecure against quantum attacks (Lo and Chau, 1997; Mayers, 1997). Furthermore, it was shown that unconditionally secure QOT is also impossible (Lo, 1997). The QOT protocols are therefore developed either imposing limitations on the eavesdropping, e.g., noisy storage model, when qubits, stored by a dishonest receiver, undergo decoherence (Wehner *et al.*, 2008), or allowing partial information leakage to an eavesdropper (Chailloux *et al.*, 2010). More recently, a so-called simulation-based security framework was also introduced for QOT, showing that it is possible to construct a practical protocol for QOT only with minimal assumptions, in particular one-way functions (Diamanti *et al.*, 2024).

In the schemes described above, classical information is communicated using quantum states. Differently to that, *quantum teleportation* (QT) offers a possibility to communicate a quantum state (hence, quantum information, e.g., a qubit) between remote parties (Bennett *et al.*, 1993), assisted by classical communication. This is achieved by pre-sharing a quantum resource (an entangled state), performing joint *Bell measurement* on the input state and the local part of the entangled state (projective measurement in the Bell basis) at the side of one of the parties, and classically communicating the outcomes to another party, which performs respective operation on the other part of the entangled state to obtain ideally an exact copy of the teleported quantum state. The quantum state is then transferred without directly

sending the physical system that realizes it, while the original quantum state is destroyed by the measurement, hence not violating the no-cloning theorem. Since the sending and receiving parties generally do not know the teleported state, QT is closely related to QKD and can be seen as a quantum encryption (Gisin *et al.*, 2002). In practice, when entangled resource and device performance are not perfect, the receiver obtains an imperfect copy of the teleported state and the quality of QT is characterized by fidelity (overlap) F between the states. Successful (true) QT then should demonstrate fidelity higher than what can be achieved by the best classical strategy, e.g., by quantum state measurement and reconstruction, in the qubit case limited by $F = 2/3$. QT was first tested using polarization photon states (Boschi *et al.*, 1998; Bouwmeester *et al.*, 1997) and later extensively developed and advanced (see (Hu *et al.*, 2023; Pirandola *et al.*, 2015a) for recent reviews), also toward CV realizations, which can offer unconditional teleportation, as we discuss in Sec. IV.

There are many more protocols and cryptographic primitives, reportedly enabled or enhanced by quantum effects compared to their classical counterparts. The interplay between some of the protocols is yet to be fully clarified in the ongoing development of quantum communication. The above-given introduction nevertheless provides a basis for discussion of the major CV quantum communication schemes in the next sections. Before we proceed, we first recapitulate the basic notions from CV quantum information along with the major properties of the CV quantum states that are useful for quantum communication protocols.

C. Continuous-variable quantum systems

CV quantum systems are defined on infinite-dimensional Hilbert spaces, and described by observables with continuous eigenspectra (see (Braunstein and Van Loock, 2005) and (Weedbrook *et al.*, 2012a) for reviews). A radiation mode k of the quantized electromagnetic field is represented by a harmonic oscillator with frequency ω_k and the Hamiltonian $\hat{H}_k = \hbar\omega_k(\hat{a}_k^\dagger\hat{a}_k + 1/2)$, where $\hat{a}_k^\dagger$ and $\hat{a}_k$ are the creation and annihilation operators of the mode k . Setting $\hbar = 2$, we define the dimensionless *quadrature operators* $\hat{x}_k$ and $\hat{p}_k$ of the field in the mode k as the real and imaginary parts of the creation and annihilation operators, $\hat{a}_k = (\hat{x}_k + i\hat{p}_k)/2$ and $\hat{a}_k^\dagger = (\hat{x}_k - i\hat{p}_k)/2$, from which follows $\hat{x}_k = \hat{a}_k^\dagger + \hat{a}_k$ and $\hat{p}_k = i(\hat{a}_k^\dagger - \hat{a}_k)$. Following the commutation relations for the bosonic operators, $[\hat{a}_l^\dagger, \hat{a}_m] = \delta_{lm}$, we obtain $[\hat{x}_l, \hat{p}_m] = 2i\delta_{lm}$. The conjugate quadrature operators $\hat{x}_k, \hat{p}_k$ of mode k then have the meaning of position and momentum of the harmonic oscillator associated with this mode.

By introducing the variance of an operator $\hat{A}$ as $V(\hat{A}) = \langle(\Delta\hat{A})^2\rangle = \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2$, where $\Delta\hat{A} = \hat{A} - \langle\hat{A}\rangle$

is deviation from the mean, we obtain the Heisenberg uncertainty principle for quadrature operators in mode k as $V(\hat{x}_k)V(\hat{p}_k) \geq 1$. In our notations the quadrature variance of a vacuum state is equal to 1, which defines the shot-noise unit (SNU).

For an N -mode state we can arrange the quadrature operators into a column vector $\hat{\mathbf{r}} = \{\hat{x}_1, \hat{p}_1, \dots, \hat{x}_N, \hat{p}_N\}^T$. The commutation relations can be then expressed as $[\hat{r}_i, \hat{r}_j] = 2i\Omega_{ij}$ through the elements of the symplectic form

$$\Omega = \oplus_{k=1}^N \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (1)$$

A CV quantum state with a density matrix $\hat{\rho}$ can be represented in phase space by means of the Wigner function, which is the (quasi-)probability distribution for the dimensionless quadrature observables introduced earlier and can be written through the eigenstates of the quadrature operators as

$$W(x, p) = \frac{1}{(2\pi)^N} \int_{\mathbb{R}^N} \langle x - y | \hat{\rho} | x + y \rangle e^{ipy} d^N y \quad (2)$$

for $x, p \in \mathbb{R}^N$. The first statistical moments (mean values) of quadratures define the displacement vector $\bar{\mathbf{r}} = \langle\hat{\mathbf{r}}\rangle = \text{Tr}[\hat{\rho}\hat{\mathbf{r}}]$. The second moments form the *covariance matrix* γ with elements

$$\gamma_{i,j} = \frac{1}{2} \langle\{\Delta\hat{r}_i \Delta\hat{r}_j\}\rangle, \quad (3)$$

where $\{\cdot\}$ is the anti-commutator. The diagonal elements of the covariance matrix then give the quadrature variances of a particular mode i as $\gamma_{i,i} = \langle\hat{r}_i^2\rangle - \langle\hat{r}_i\rangle^2$, while the off-diagonal elements represent the quadrature correlations between the modes. The uncertainty principle can be generalized in terms of the covariance matrix as $\gamma + i\Omega \geq 0$, which can be seen as a condition on the physicality of a state represented by a covariance matrix γ .

Alternatively, to the phase-space representation, the CV states can be represented in the Fock (number) basis, composed by the eigenstates of the photon-number operator, $\hat{n} = \hat{a}^\dagger\hat{a}$, such that $\hat{n}|n\rangle = n|n\rangle$. The number basis $\{|n\rangle\}_0^\infty$ then spans the infinite-dimensional Hilbert space of a given mode.

1. Gaussian quantum states

An important class of CV states are the states for which the Wigner function is Gaussian (see (Weedbrook *et al.*, 2012a) for a review on Gaussian quantum information) and can be then represented through the displacement vector $\bar{\mathbf{r}}$ and the covariance matrix γ as

$$W(\mathbf{r}) = \frac{1}{(2\pi)^N \sqrt{\det\gamma}} e^{-\frac{1}{2}(\mathbf{r}-\bar{\mathbf{r}})^T \gamma^{-1} (\mathbf{r}-\bar{\mathbf{r}})} \quad (4)$$

for $\mathbf{r} \in \mathbb{R}^{2N}$ and where $\det$ stands for determinant of a matrix. Importantly, Gaussian states are then explicitly described by the first (displacement vector) and second (covariance matrix) moments of quadratures, which largely simplifies the analysis of those infinite-dimensional states.

The typical example of a Gaussian state, commonly used in CV quantum information, is the *coherent state*, which is an eigenstate of the annihilation operator, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, with a generally complex eigenvalue α . In the Fock basis, a coherent state is then represented as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (5)$$

Coherent states are characterized by the quadrature mean values $\bar{\mathbf{r}}_{\text{coh}} = \{2\text{Re}(\alpha), 2\text{Im}(\alpha)\}$ and the 2×2 diagonal covariance matrix $\gamma_{\text{coh}} = \text{diag}(1, 1)$. The vacuum state can be then seen as the zero-mean coherent state with $\bar{\mathbf{r}}_{\text{coh}} = \{0, 0\}$ yet the same covariance matrix $\gamma_{\text{vac}} = \text{diag}(1, 1)$, containing variances of 1 SNU for either of the quadratures. Note, that a coherent state is a minimum-uncertainty state, saturating equality in the Heisenberg principle, $V(\hat{x}_k)V(\hat{p}_k) = 1$. The mean photon number of a coherent state, obtained as the mean of the photon-number operator $\hat{n} \equiv \hat{a}^\dagger \hat{a}$, is $\langle \hat{n} \rangle_{\text{coh}} = |\alpha|^2$.

A Gaussian (quadrature-)squeezed state is also a minimum-uncertainty state, but with different quadrature variances, which is reflected in the covariance matrix $\gamma_{\text{sq}} = \text{diag}(e^{-2r}, e^{2r})$. Assuming $r > 0$ so that the $\hat{x}$ quadrature is squeezed and denoting the squeezed quadrature variance $V_S \equiv e^{-r}$, $V_S < 1$, we obtain the covariance matrix $\gamma_{\text{sq}} = \text{diag}(V_S, 1/V_S)$, where the $\hat{p}$ quadrature with variance $V_S > 1$ is anti-squeezed (the opposite situation with $\hat{p}$ quadrature squeezing is obtained at $r < 0$). The displacement of squeezed states can be zero (squeezed vacuum states) or non-zero (squeezed coherent states).

A *thermal state* is a Gaussian state with a diagonal covariance matrix $\gamma_{\text{th}} = \text{diag}(V, V)$ so that the variances of both quadratures are $V > 1$ and the state does not have the minimum uncertainty. The quadrature variance V is related to the mean photon number of a thermal state as $V = 2\langle \hat{n} \rangle_{\text{th}} + 1$. A thermal state with zero mean photons reduces to the vacuum state with $V = 1$.

Introducing the Gaussian purity, expressed through the determinant of the covariance matrix as $\mu = 1/\sqrt{\det \gamma}$ (Paris *et al.*, 2003), we notice that coherent and squeezed states are pure with $\mu = 1$, while a thermal state is not.

The two-mode squeezed vacuum state (TMSV) is an entangled two-mode Gaussian state, which, in the Fock representation, is given by

$$|\lambda\rangle = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} (-\lambda)^n |n, n\rangle, \quad (6)$$

where the state parameter λ is expressed through the squeezing as $\lambda = \tanh r$ and $|n, n\rangle$ represents the number

state with the same number of photons n in each of the two squeezed vacuum modes. TMSV states have zero displacement and their two-mode covariance matrix reads

$$\gamma_{\text{TMSV}} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2 - 1}\mathbb{Z} \\ \sqrt{V^2 - 1}\mathbb{Z} & V\mathbb{I} \end{pmatrix}, \quad (7)$$

where the quadrature variance $V = \cosh 2r$. Each of the two modes of a TMSV state is in a thermal state (after tracing out another mode), which is mixed, yet the overall two-mode state is pure with $\det(\gamma_{\text{TMSV}}) = 1$. It can be therefore seen as a purification of a single-mode thermal state. TMSV states are quadrature-entangled, providing maximum entanglement for the given mean photon number. In the limit of infinite squeezing $r \rightarrow \infty$ with perfect correlation (anti-correlation) between $\hat{x}$ ($\hat{p}$) quadratures in each of the modes, TMSV states become equivalent to an EPR pair in quantum mechanics (named after the famous Einstein-Podolsky-Rosen paradox) and are sometimes also referred to as CV EPR states.

2. Gaussian operations

In the description and analysis of CV quantum communication, we will largely rely on the physical operations on CV Gaussian states that preserve their Gaussianity (hence, the Gaussian character of the Wigner function). Those operations, referred to as Gaussian ones (Weedbrook *et al.*, 2012a), are described in the Heisenberg picture by affine maps of the form $(S, \mathbf{d}) : \hat{\mathbf{r}} \rightarrow S\hat{\mathbf{r}} + \mathbf{d}$ with $\mathbf{d} \in \mathbb{R}^{2N}$ and S being a $2N \times 2N$ real matrix. Preservation of the commutation relations implies that the transformation is symplectic, hence $S\Omega S^T = \Omega$. Then the action on the quadrature moments is given by $\bar{\mathbf{r}} \rightarrow S\bar{\mathbf{r}} + \mathbf{d}$ and $\gamma \rightarrow S\gamma S^T$.

Displacement operation is a single-mode Gaussian unitary defined as the Bogolyubov transformation $\hat{a} \rightarrow \hat{a} + \alpha$. It transforms the quadrature operators accordingly as $\hat{\mathbf{r}} \rightarrow \hat{\mathbf{r}} + \mathbf{d}_\alpha$ through the displacement vector $\mathbf{d}_\alpha = \{2\text{Re}(\alpha), 2\text{Im}(\alpha)\}$, therefore shifting the quadrature mean values by the elements of the displacement vector and leaving the covariance matrix unchanged (hence the transformation matrix $S_\alpha = \mathbb{I}$ is the 2×2 identity matrix, $\mathbb{I} = \text{diag}(1, 1)$). The coherent state can be obtained by a displacement operation acting on a vacuum state.

Phase rotation, another single-mode Gaussian unitary, being the Bogolyubov transformation $\hat{a} \rightarrow e^{i\theta}\hat{a}$, transforms the quadratures as $\hat{\mathbf{r}} \rightarrow S_\theta \hat{\mathbf{r}}$ and is characterized by zero displacement and the transformation matrix

$$S_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}. \quad (8)$$

Single-mode squeezing is represented by the transformation $\hat{a} \rightarrow \hat{a} \cosh r - \hat{a}^\dagger \sinh r$ with the squeezing parameter $r \in \mathbb{R}$, which is equivalent to mapping $\hat{\mathbf{r}} \rightarrow S_r \hat{\mathbf{r}}$ with

$$S_r = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^r \end{pmatrix}. \quad (9)$$

Squeezed states can then be obtained by the action of the single-mode squeezing operation on a vacuum or a coherent state.

Beam splitter transformation is a two-mode Gaussian unitary, characterized for the modes 1 and 2 with operators $\hat{a}_1$ and $\hat{a}_2$ by the Bogolyubov transformation

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \rightarrow \begin{pmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \quad (10)$$

where the coupling ratio $\sqrt{T}$ defines the transmittance T and reflectance $1-T$ of the beam splitter. Equivalently, the two-mode quadrature vector $\hat{\mathbf{r}}_{12} = \{\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2\}^T$ is transformed as $\hat{\mathbf{r}}_{12} \rightarrow S_T \hat{\mathbf{r}}_{12}$ with the transformation matrix

$$S_T = \begin{pmatrix} \sqrt{T}\mathbb{I} & \sqrt{1-T}\mathbb{I} \\ -\sqrt{1-T}\mathbb{I} & \sqrt{T}\mathbb{I} \end{pmatrix}. \quad (11)$$

Finally, the *two-mode squeezing* operation on the modes 1 and 2 is defined by $\hat{a}_1 \rightarrow \hat{a}_1 \cosh r + \hat{a}_2^\dagger \sinh r$ and $\hat{a}_2 \rightarrow \hat{a}_2 \cosh r + \hat{a}_1^\dagger \sinh r$ through the two-mode squeezing parameter $r \in \mathbb{R}$. The respective transformation for the quadrature vector $\hat{\mathbf{r}}_{12}$ then reads $\hat{\mathbf{r}}_{12} \rightarrow S_{2r} \hat{\mathbf{r}}_{12}$ with the transformation matrix for the two-mode squeezing

$$S_{2r} = \begin{pmatrix} \cosh r \mathbb{I} & \sinh r \mathbb{Z} \\ \sinh r \mathbb{Z} & \cosh r \mathbb{I} \end{pmatrix}, \quad (12)$$

where the Pauli matrix $\mathbb{Z} = \text{diag}(1, -1)$. TMSV states can then be obtained by the two-mode squeezing operation acting on a two-mode vacuum state.

3. Gaussian channels

In CV-QKD, the most typical communication scenario is an optical fiber, which is a specific type of bosonic Gaussian channel. A Gaussian channel is a completely-positive trace-preserving map $\mathcal{E}$ transforming Gaussian states into Gaussian states. In particular, a single-mode Gaussian channel can be represented by the following transformations on the first two statistical moments, $\bar{\mathbf{r}}$ and γ , of an input Gaussian state

$$\bar{\mathbf{r}} \rightarrow \mathbf{T}\bar{\mathbf{r}} + \mathbf{d}, \quad \gamma \rightarrow \mathbf{T}\gamma\mathbf{T}^T + \mathbf{N}, \quad (13)$$

where $\mathbf{d}$ is a 2-dimensional displacement vector, while the 2×2 transmittance matrix $\mathbf{T}$ and noise matrix $\mathbf{N}$ satisfy the properties $\mathbf{N}^T = \mathbf{N} > 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2$.

A single-mode Gaussian channel can be reduced to a ‘canonical form’ for which $\mathbf{d} = \mathbf{0}$ and the matrices above take diagonal expressions (Weedbrook *et al.*, 2012a). The most important form is certainly the thermal-loss channel, which is characterized by $\mathbf{T} = \sqrt{T}\mathbb{I}$ and $\mathbf{N} = (1-T)(2\bar{n}_N + 1)\mathbb{I}$. Here the transmittance T represents the fraction of photons surviving at the output of the channel, while the thermal noise $\bar{n}_N$ describes extra thermal photons that are injected into the channel from the

external environment (this noise is often rewritten in the form of excess noise as we discuss later).

The dilation of a thermal-loss channel is a beam splitter transformation with the same transmittance T , where the environmental port is used to inject $\bar{n}_N$ thermal photons. By purifying the environmental thermal state, it is further dilated into an entangling cloner, where one mode of a TMSV state is injected into the beam splitter. This is what forms the entangling cloner attack, discussed in Sec. III.B.2.

Other relevant canonical forms of a single-mode Gaussian channel are the quantum amplifier and the additive-noise channel. However, these forms play a minor role in QKD communications, where loss is always present. In general, any canonical form can be dilated into a collective Gaussian attack (Pirandola *et al.*, 2008a).

4. Coherent detection

The quadrature observables are measured by means of coherent detection, which, for a single-quadrature measurement, is called *homodyne detection* and is the major detection type used in CV quantum information. This is in contrast to the DV protocols, which are largely based on direct photodetection either using avalanche photodiodes, working in the Geiger mode, and registering the presence of an incoming signal on a single-photon level, or using photon-number resolving detectors. Homodyne detection results in the value x or p of the $\hat{x}$ or $\hat{p}$ quadrature respectively and is therefore a projective measurement on the infinitely-squeezed eigenstates of the quadrature operators, $|x\rangle$ or $|p\rangle$. The quadrature probability distributions are the marginal integrals of the Wigner function over the complementary quadrature,

$$P(x) = \int_{\mathbb{R}} W(x, p) dp, \quad P(p) = \int_{\mathbb{R}} W(x, p) dx. \quad (14)$$

In practice, homodyne detection is realized by coupling an incoming signal mode s with another mode, which is in a strongly displaced coherent state (referred to as the local oscillator, LO), on a balanced beam splitter (hence, $T = 1/2$), see Fig. 2(a). The two output modes of the beam splitter are individually measured by two photodetectors, which produce photocurrents proportional to the number of incoming photons. Those photon numbers are then subtracted and the resulting quantity is proportional to the value of a quadrature, defined by the phase of the LO. Indeed, by transforming the field operators of the signal mode $\hat{a}_s$ and the LO $\hat{a}_{\text{LO}}$ after the balanced beam splitter (10) as $\hat{a}' = (\hat{a}_s + \hat{a}_{\text{LO}})/\sqrt{2}$, $\hat{a}'_{\text{LO}} = (-\hat{a}_s + \hat{a}_{\text{LO}})/\sqrt{2}$ and parametrizing the strong coherent LO as $\hat{a}_{\text{LO}} = \alpha_{\text{LO}} e^{i\phi}$, where $\alpha_{\text{LO}} \in \mathbb{R}$ and ϕ is the LO phase, we obtain that the photon number difference between the beam splitter outputs is $\hat{a}'_s^\dagger \hat{a}'_s - \hat{a}'_{\text{LO}}^\dagger \hat{a}'_{\text{LO}} = \hat{a}^\dagger \alpha_{\text{LO}} e^{i\phi} + \hat{a} \alpha_{\text{LO}} e^{-i\phi}$. Hence, by setting either $\phi = 0$ or $\phi = \pi/2$ one can detect either $\hat{x}$ or $\hat{p}$ quadrature observables of the single mode, thereby compensating the

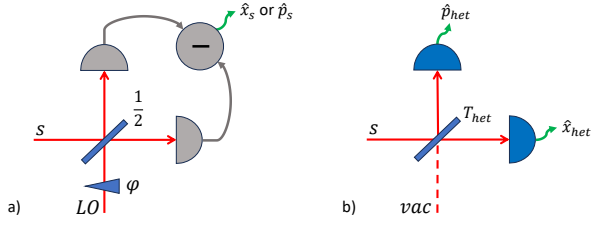


FIG. 2 Left (a): homodyne detection of an incoming signal in mode s , based on a balanced coupling with the local oscillator LO and subsequent subtraction and scaling of the signals from the photodetectors (given in grey), resulting in the measured value of an $\hat{x}_s$ or $\hat{p}_s$ quadrature observable of the signal; Right (b): heterodyne (double homodyne) detection of an incoming signal in mode s , based on a generally unbalanced splitting coupling to a vacuum mode vac with transmittance T_{het} and subsequent measurement of the $\hat{x}_{het}$ and $\hat{p}_{het}$ quadrature observables, being the linear combinations of the quadratures in modes s and vac , by the homodyne detectors on the outputs of the beam splitter (given in blue). The LO modes and the structure of each of the two homodyne detectors (balanced coupling to LO, photocurrent difference scheme), are omitted for simplicity.

photon-number fluctuations of the signal and the LO. Moreover, by continuously changing the phase of the LO one can perform state tomography and reconstruct the Wigner function (2). In the case of an N -mode system the probability distribution of a measured quadrature (14) is obtained by integrating the Wigner function over the complementary quadrature in the same mode and the quadratures of all other $N-1$ modes. The covariance matrix of the conditional state of the residual $N-1$ modes of system A after knowing the outcome $q_B \in \{x_B, p_B\}$ of a $\hat{q}_B \in \{\hat{x}_B, \hat{p}_B\}$ quadrature measurement on the single-mode system B is given by (Eisert *et al.*, 2002; Fiurášek, 2002)

$$\gamma_{A|q_B} = \gamma_A - \sigma_{A,B}(Q\gamma_B Q)^{MP}\sigma_{A,B}^T, \quad (15)$$

where γ_A and γ_B are the covariance matrices of the subsystems A and B , $\sigma_{A,B}$ is the correlation matrix between the subsystems A and B before the measurement, so that the state of the overall N -mode system AB before the measurement is characterized by the covariance matrix

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{A,B} \\ \sigma_{A,B} & \gamma_B \end{pmatrix} \quad (16)$$

(note, that the covariance matrix can be always rearranged so that a single-mode system B resides in mode N), MP stands for the Moore-Penrose (pseudo)-inverse of a generally singular matrix, and matrix $Q = \text{diag}(1, 0)$ for the $\hat{x}_B$ quadrature measurement and $Q = \text{diag}(0, 1)$ for the measurement of the quadrature $\hat{p}_B$.

A homodyne measurement yields the value of the measured quadrature, while being fully uninformative about the complementary one. As an alternative, the *heterodyne detection* (also referred to as the double homodyne

detection), which projects the measured state on a coherent one, yields information on both of the complementary quadratures in the measured mode, while being limited by the uncertainty principle. In practice, the heterodyne measurement is realized by a balanced splitting of a signal mode on a beam splitter with $T = 1/2$ and then $\hat{x}$ and $\hat{p}$ quadrature homodyne measurements on the outputs of the beam splitter (set by the phases of the respective LO beams). The conditional state of a subsystem A of a generally N -mode system AB after the heterodyne measurement on the single-mode subsystem B is then given by (Weedbrook *et al.*, 2012a)

$$\gamma_{A|x_B, p_B} = \gamma_A - \sigma_{A,B}(\gamma_B + \mathbb{I})^{MP}\sigma_{A,B}^T. \quad (17)$$

Heterodyne measurement can be generally unbalanced, which is set by the beam splitter transmittance T_{het} , as shown in Fig. 2(b). The quadratures measured on the beam splitter outputs are then the linear combinations of the input quadratures according to (10) and read $\hat{x}_{het} = \sqrt{T_{het}}\hat{x}_s + \sqrt{1-T_{het}}\hat{x}_{vac}$ and $\hat{p}_{het} = -\sqrt{1-T_{het}}\hat{p}_s + \sqrt{T_{het}}\hat{p}_{vac}$, where $\hat{x}_{vac}$, $\hat{p}_{vac}$ are the quadratures of the vacuum mode. The variances of the measured quadratures are then equal to $T_{het}V_s^x + 1 - T_{het}$ and $(1-T_{het})V_s^p + T_{het}$, where $V_s^{\{x,p\}}$ are $\hat{x}$ and $\hat{p}$ quadrature variances of the signal, combined with the fractions of vacuum noise, which can be seen as a penalty for the simultaneous measurements of the complementary quadratures. The covariance matrix of a generally N -mode state conditioned on the generally unbalanced heterodyne measurement can be obtained by introducing the vacuum state in mode $N+1$, splitting the measured mode N with this vacuum mode with the ratio T_{het} and double application of the conditioning (15) on $\hat{x}$ - and $\hat{p}$ -quadrature measurements in modes $N, N+1$.

D. Continuous-variable quantum information theory

The outcomes of the measurements on continuous-variable states are typically discretized and represented by discretely distributed classical random variables. Information contained in such variable X , which takes values from the support (encoding alphabet) $\mathbb{X}$ with the probability distribution $p(X)$ is well known to be defined by the *Shannon entropy* $H(X) = -\sum_{X \in \mathbb{X}} p(X) \log p(X)$. We omit the logarithm base here, but further, with no loss of generality, we take logarithms for the entropic measures base two and quantify the information in Shannon units or bits. Similarly, joint $H(X, Y) = -\sum_{X \in \mathbb{X}, Y \in \mathbb{Y}} p(X, Y) \log p(X, Y)$ and conditional $H(X|Y) = -\sum_{X \in \mathbb{X}, Y \in \mathbb{Y}} p(X, Y) \log [p(X, Y)/p(Y)]$ entropies can be defined by adding the random variable Y with support $\mathbb{Y}$ and with individual $p(Y)$ and joint $p(X, Y)$ probability distributions. The mutual entropy $H(X : Y)$, which we will refer to as the *mutual information* $I_{XY} = -\sum_{X \in \mathbb{X}, Y \in \mathbb{Y}} p(X, Y) \log (p(X, Y)/[p(X)p(Y)]) =$

$H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X, Y)$ quantifies the capacity of a classical channel with discrete input and output X and Y .

Theoretical evaluation of properties of continuous-variable states can be efficiently performed by considering the observables as continuously distributed random variables. For such a variable X with the probability density function $f(X)$ on support $\mathbb{X}$, the information contained in this variable is characterized by the differential entropy $h(X) = -\int_{\mathbb{X}} f(x) \log f(x) dx$. Similarly, the conditional $h(X|Y) = -\int_{\mathbb{X}, \mathbb{Y}} f(x, y) \log f(x|y) dx dy$ entropy can be defined with continuous variable Y on $\mathbb{Y}$ with $f(y)$ and conditional density function $f(x|y) = f(x, y)/f(y)$, expressed through the joint density function $f(x, y)$. The mutual information between the continuous variables X, Y is then $I_{XY} = -\int_{\mathbb{X}} \int_{\mathbb{Y}} f(x, y) \log [f(x, y)/(f(x)f(y))] dx dy$.

For a Gaussian-distributed random variable X with variance V_X the integration of differential entropy simplifies to $H(X) = \frac{1}{2} \log V_X + C$, defined up to a constant C . Similarly, the conditional entropy on variable Y with variance V_Y becomes $H(X|Y) = \frac{1}{2} \log V_{X|Y} + C$, where the conditional variance $V_{X|Y} = V_X - C_{XY}^2/V_Y$ is expressed through the correlation (covariance) $C_{XY} = \langle xy \rangle$ between the values x, y of the variables X, Y . Then the mutual information for two Gaussian random variables $I_{XY} = \frac{1}{2} \log [(V_X V_Y)/(V_X V_Y - C_{XY}^2)]$ is independent of the scaling and can be equivalently expressed as

$$I_{XY} = \frac{1}{2} \log \frac{V_X}{V_{X|Y}} = \frac{1}{2} \log \frac{V_Y}{V_{Y|X}}. \quad (18)$$

The amount of information contained in a quantum state with density matrix $\hat{\rho}$ is given by the (quantum) *von Neumann entropy* $S(\hat{\rho}) = -\text{Tr} \hat{\rho} \log \hat{\rho}$. The von Neumann entropy of a pure state is then 0, while a thermal state maximizes the von Neumann entropy at the given mean photon number. The quantum entropy can be extended to definitions of conditional, joint and mutual entropies, similarly to the classical case.

If a classical discrete random variable X with support $\mathbb{X}$ and probability distribution $p(X)$ is encoded by the alphabet of quantum states $\hat{\rho}(X)$, then the information on X , which can be extracted from the measurements of the resulting quantum ensemble with outcomes Y is upper limited as $I_{XY} \leq \chi(P(X), \hat{\rho}(X))$ by the *Holevo bound* (also referred to as the Holevo information or Holevo quantity):

$$\chi(P(X), \hat{\rho}(X)) = S\left(\sum_{\mathbb{X}} p(X) \hat{\rho}(X)\right) - \sum_{\mathbb{X}} p(X) S(\hat{\rho}(X)). \quad (19)$$

For continuously distributed classical random variables the sums in the expression (19) turn into integrals over the continuous support of the random variable X .

If we consider a classical, generally noisy channel $\mathcal{N}$, which maps the input X to the output Y , $X \xrightarrow{\mathcal{N}} Y$, then the channel capacity is given by the mutual information

I_{XY} maximized over all possible input sets X . Similarly, the classical capacity of a memoryless quantum channel $\mathcal{M}$, independently mapping quantum input states to the output ones, $\hat{\rho}(X) \xrightarrow{\mathcal{M}} \mathcal{M}[\hat{\rho}(X)]$, is given by the Holevo bound $\chi(P(X), \mathcal{M}[\hat{\rho}(X)])$, maximized over all possible sources $p(X), \hat{\rho}(X)$.

By choosing the orthogonal basis $|i\rangle$, in which the density matrix of a state is diagonal, $\hat{\rho} = \sum_i \lambda_i |i\rangle \langle i|$, the von Neumann entropy can be expressed as the Shannon entropy of the eigenvalues λ_i , $S(\hat{\rho}) = -\sum_i \lambda_i \log \lambda_i$. For Gaussian states such diagonalization can be performed in terms of the covariance matrix γ by applying a symplectic transformation S such that

$$S\gamma S^T = \bigoplus_{k=1}^N \begin{pmatrix} \lambda_k & 0 \\ 0 & \lambda_k \end{pmatrix} := \gamma^\oplus, \quad (20)$$

where $\{\lambda_k\}$ are the *symplectic eigenvalues* of the covariance matrix γ and the diagonal matrix $\gamma^\oplus$ is referred to as the *Williamson form* of the covariance matrix (following the Williamson theorem (Williamson, 1936), proving that the diagonalization is always possible for any $2N \times 2N$ real positive-definite matrix). The symplectic eigenvalues can be found as the eigenvalues of the matrix $|i\Omega\gamma|$ and define the von Neumann entropy of a state with the covariance matrix γ as (Serafini *et al.*, 2004)

$$S(\gamma) = \sum_i^N G\left(\frac{\lambda_i - 1}{2}\right), \quad (21)$$

where $G(x) = (x+1) \log(x+1) - x \log x$ is the bosonic entropy function (Serafini *et al.*, 2005). A symplectic transformation therefore represents a Gaussian state as a direct product of thermal states with variances λ_i , whose entropies are then expressed through the mean photon numbers $\bar{n}_i$ and sum up to the von Neumann entropy of the whole state.

Having defined the CV quantum states, their observables, typical measurements, operations, and information quantities, we can proceed to the description of CV quantum communication, starting with the major application of quantum key distribution.

III. CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION

The idea to use quadrature observables measured by homodyne detection for QKD was first stated in (Ralph, 1999b) using simple binary encoding and analyzed in terms of the quantum bit error rate (QBER) introduced by an eavesdropper while intercepting the key bits. While using coherent signal states was shown inefficient within this framework, the EPR correlations obtained by coupling two displaced squeezed states, subsequently sent to the remote trusted party after a random time delay on one of the beams, can be advantageous in protecting the key bits against practical attacks, resulting in higher

QBER for each intercepted bit. The use of modulated single-mode squeezed vacuum states for CV-QKD was suggested in (Hillery, 2000) to overcome the vulnerability of the binary-encoded coherent-state protocol to practical attacks such as the beam splitting or intercept-resend attack, when an eavesdropper measures the incoming signal and then re-sends the modulated signal according to the measured results. The security of the scheme was generalized in (Gottesman and Preskill, 2001) using quantum error-correcting codes for encoding qubits in the infinite-dimensional Hilbert space of the CV quantum systems. The possibility of using entangled CV states prepared using modulated coherent states entering a nondegenerate parametric amplifier and measured separately by the trusted parties for binary CV-QKD was discussed in (Reid, 2000) considering practical eavesdropping attacks.

The distribution of continuous Gaussian keys was first proposed using squeezed states in (Cerf *et al.*, 2001). This all-continuous CV-QKD protocol allowed evaluation of information shared between the trusted parties and leaking to an eavesdropper upon Gaussian individual attacks (which we discuss in Sec. III.B) using the above-described formalism of Gaussian quantum information. The Gaussian CV-QKD protocol using experimentally more feasible coherent states was subsequently proposed in (Grosshans and Grangier, 2002), known as GG02 protocol, and was also shown secure against individual attacks at channel transmittance above 50%. To overcome this limitation, the coherent-state CV-QKD protocol using post-selection was proposed in (Silberhorn *et al.*, 2002b). Alternatively, the use of reverse reconciliation was shown to provide theoretical security of the coherent-state protocol at any level of channel attenuation in (Grosshans *et al.*, 2003b). This result indicated the practical feasibility of CV-QKD and led to its rapid development and implementation, while defining the basic principles of Gaussian CV-QKD. However, the applicability of the protocols was still largely limited by the post-processing (error correction) efficiency for Gaussian-distributed data (Lodewyck *et al.*, 2007), which we discuss in detail in Sec. III.E. In order to overcome this limitation, discrete-modulated (DM) CV-QKD was proposed in (Leverrier and Grangier, 2009). The subsequent development of CV-QKD then continued along the lines of Gaussian/DM protocols, toward improving their applicability and security, as we discuss in the next sections.

A. CV-QKD protocols

A generic CV-QKD protocol between two trusted parties, which are traditionally denoted as Alice (A) and Bob (B), consists of the following major steps, as illustrated in Fig. 3:

1. **State preparation.** Alice generates random data sequences (strings) $\mathbf{x}_M, \mathbf{p}_M$, containing key

values to be encoded in the modulated quantum states¹. Those random values are either taken from the zero-centered Gaussian distributions $\mathcal{N}(0, V_x), \mathcal{N}(0, V_p)$ in case of the Gaussian protocols, or follow a discrete modulation profile (binary, quaternary or more complex constellations with different probability distributions). Alice then prepares a signal state (coherent or squeezed) and applies displacement to one or both of the quadratures, depending on a particular protocol. In a standard Gaussian scheme (e.g., GG02), Alice modulates the signal up a symmetrical thermal state, but asymmetrical modulation profiles are also possible as we discuss below. Alice verifies the modulation by monitoring the modulated signal (tapping off a part or switching to fully measuring it with her local detector).

2. **State distribution.** The modulated states are sent to the receiving party, Bob, through a quantum channel, which is assumed to be fully controlled by an eavesdropper, Eve.
3. **State measurement.** The remote (receiving) party, Bob, performs the detection of the incoming signal, using homodyne or heterodyne detection, hence obtaining data sequences $\mathbf{x}_B, \mathbf{p}_B$. In case of the homodyne detection, Bob randomly switches between measuring $\hat{x}$ and $\hat{p}$ quadratures. This case implies the necessity of a key sifting (bases reconciliation) procedure, where Alice and Bob keep the data, encoded in and decoded from the same quadratures. The state measurement concludes the quantum phase of the protocol.
4. **Post-processing.** In the post-processing stage, the trusted parties perform all necessary procedures with the classical data encoded and obtained from the measurements. This typically includes error correction, when a reference trusted party sends the correcting trusted party the syndromes of their data, which are compared and the respective data is discarded in case of mismatch or kept otherwise. The case, when Alice, who is the sender of the quantum signals, is also the reference side of the error correction, sending her syndromes to Bob, is called direct reconciliation (DR). The opposite situation, when Bob is the reference side of the error correction, is referred to as the reverse reconciliation (RR). Further in the post-processing stage the trusted parties also typically perform the parameter estimation, by estimating the relevant param-

¹ We omit discussion of random number generation for QKD and other quantum communication tasks as it goes beyond the scope of this review. Quantum random number generators (particularly, based on continuous variables) can be used for this purpose, as reviewed in (Herrero-Collantes and Garcia-Escartin, 2017)

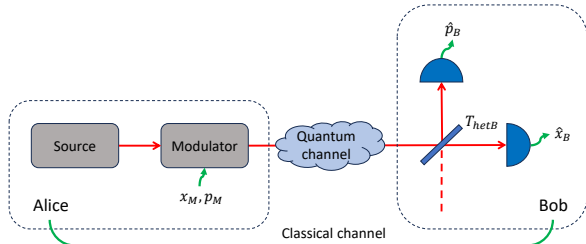


FIG. 3 Generic P&M CV-QKD scheme. Alice generates a signal state using the Source, applies the displacement according to the pre-generated states x_M, p_M on the Modulator, and sends the modulated states through the Quantum channel to the remote party Bob, who performs the heterodyne detection with balancing T_{hetB} , obtaining his data from the measurement of $\hat{x}_B, \hat{p}_B$. The trusted parties then use the authenticated Classical channel to perform error correction and privacy amplification.

ters of their states and the quantum channel. This allows the trusted parties to bound the information leaked to the eavesdropper Eve. Depending on the protocol and implementation, the parameter estimation can be performed either after or before the error correction. The trusted parties can also apply post-selection on their data, as we discuss in Sec. III.E.3. Finally, they perform privacy amplification in order to minimize the information on the key, which is available to Eve. This procedure results in the secret keys, which are ideally identical and completely unknown to the eavesdropper. We discuss the post-processing procedures in detail in Sec. III.E.

The scheme, described above, in which Alice prepares the modulated signal states according to her pre-generated data, and Bob performs the detection, to obtain his measured data, is the P&M version of CV-QKD. Alternatively and equivalently, Gaussian CV-QKD protocols can be implemented so that both of the trusted parties are measuring respective parts of a bi-partite entangled state - typically a TMSV in the case of symmetrical modulation, while a more advanced entangled state preparation is needed for asymmetrical modulations, as we discuss below and summarize in Table III. Such EB realization of CV-QKD is shown in Fig. 4 for the standard (generic) Gaussian protocols. In this case, the state preparation consists of generating an entangled state and Alice is also performing a measurement (homodyne or heterodyne) on her side to obtain her data sequences. The non-Gaussian DM protocols can be equivalently approximated by the EB schemes. Since Eve ideally cannot distinguish between P&M and EB versions of the protocols, the latter became not only a technical alternative, but also an ansatz for theoretical security analysis, as we discuss in Sec. III.B.

While being harder to implement in practice, EB CV-QKD can have several advantages. First of all, there is no need to pre-generate the random keys in the case of

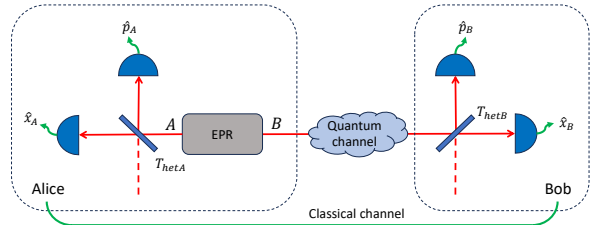


FIG. 4 Generic EB CV-QKD scheme. Alice generates a two-mode entangled state using the source EPR (a TMSV state in practice), performs the heterodyne detection on her mode A with balancing T_{hetA} , obtaining her data from the measurement of $\hat{x}_A, \hat{p}_A$ and sends the mode B through the Quantum channel to the remote party Bob, who performs the heterodyne detection with balancing T_{hetB} , obtaining his data from the measurement of $\hat{x}_B, \hat{p}_B$. The trusted parties then use the authenticated Classical channel to perform error correction and privacy amplification.

an EB protocol, as the data sequences are obtained from the measurements and their randomness is provided by the stochastic nature of the quantum measurement. Second, the trusted parties directly characterize the bipartite state, shared over the quantum channel, which simplifies the parameter estimation and the evaluation of the information leakage. Otherwise, in the P&M protocol, the trusted parties generally have to derive an equivalent entangled state in order to perform the security analysis of the protocol, as we discuss in Sec. III.B. Finally, strongly nonclassical features of the entangled states can provide better efficiency and robustness of the protocols, compared to the P&M realizations based on coherent states, as we discuss in Sec. III.C.4. Nevertheless, coherent-state P&M protocols remain more technically feasible and are a standard choice for current CV-QKD implementations.

Note, that the schemes in Fig. 3 and 4 represent the conceptual design of the CV-QKD protocols. They omit essential technical details, in particular, the signal monitoring on the sender side and the LO beams needed for the homodyne detectors. The details of the practical realization are discussed in Sec. III.C.

1. Coherent-state protocols

The aforementioned GG02 protocol (Grosshans *et al.*, 2003b) is based on symmetrical Gaussian modulation in both quadratures of coherent states and subsequent homodyne detection on the receiving side, hence Bob is randomly switching between the quadrature measurements by choosing $T_{hetB} = \{0, 1\}$. This implies key sifting to be performed by Alice and Bob. The no-switching protocol (Weedbrook *et al.*, 2004) is similarly based on symmetrical Gaussian modulation of coherent states and heterodyne detection at Bob's side ($T_{hetB} = 1/2$) and does not require key sifting, as key bits are obtained simultaneously from both of the quadratures. Importantly, the phase-space symmetries of the no-switching

protocol enable the most general security proofs for this type of protocol (finite-size composable security against general attacks) (Leverrier, 2015), while most of the other CV-QKD protocols rely on the security against collective attacks, taking into account some finite-size effects, as we discuss in Sec. III.B. The uni-dimensional (UD) coherent-state CV-QKD protocol (Usenko and Grosshans, 2015) uses Gaussian modulation in one of the quadratures and homodyne detection of the same (note, that measurement of the unmodulated quadrature is still needed for parameter estimation). The DM coherent-state protocols (Leverrier and Grangier, 2009) assume a whole plethora of discrete, non-Gaussian modulation profiles and homodyne or heterodyne modulation. The security and performance of those schemes will be discussed in detail in Sec. III.B.

2. Squeezed-state protocols

The first Gaussian CV-QKD protocol (Cerf *et al.*, 2001) is based on the symmetrical Gaussian modulation of squeezed states, when Alice randomly switches between squeezing of two orthogonal quadratures and applies Gaussian modulation to the squeezed one. Bob then performs homodyne detection by switching between $T_{\text{hetB}} = \{0, 1\}$ and the trusted parties perform bases reconciliation, keeping those elements of the key that were modulated and measured in the same squeezed quadrature. With certain adaptations and thanks to the intrinsic symmetry, the squeezed-state homodyne-detection protocol also enables composable security against general attacks (Furrer *et al.*, 2012), as we discuss in Sec. III.B. The squeezed-state protocol with heterodyne detection is also possible, but was shown to be theoretically sub-optimal (García-Patrón, 2007) in the asymptotic regime, as it does not benefit from measurement of the anti-squeezed quadrature, while containing the vacuum noise from the balanced coupling of the heterodyne detection. However, heterodyne detection may become useful in the finite-size regime, where measurement of the anti-squeezed quadrature may improve the parameter estimation and the resulting key rate (Oruganti *et al.*, 2025). The Gaussian UD protocol can also be extended to squeezed signal states (Usenko, 2018). Signal squeezing was shown helpful to improve the robustness of the protocols to channel noise (García-Patrón and Cerf, 2009), especially when additional modulation of squeezed states beyond the level of anti-squeezing is used (Madsen *et al.*, 2012) (as we discuss in detail in Sec. III.C.4), and to inefficient post-processing (Usenko and Filip, 2011). Squeezed signal states can also be used to perform DM CV-QKD (Denys *et al.*, 2021), but this avenue, up to the best of our knowledge, has not been explored in practice.

3. Entanglement-based protocols

Entanglement-based Gaussian CV-QKD protocols as shown in Fig. 4 are generally equivalent to the P&M ones (Grosshans *et al.*, 2003a). A conceptual difference occurs when an entangled source is placed in the middle of the channel (Weedbrook, 2013) (the scheme, accordingly referred to as entanglement-in-the-middle). However, the presence of the channel in both arms of the entangled state makes the protocol effectively combine DR and RR scenarios and limits the tolerable channel transmittance, as we discuss in Sec. III.B.6.

4. Two-way protocols

CV-QKD can be extended to the two-way protocols when one of the trusted parties (e.g., Bob) prepares the modulated coherent or squeezed state, and sends it to another trusted party (respectively, Alice) through an untrusted quantum channel, Alice then performs additional modulation on the state and sends it through the same quantum channel back to Bob, who performs homodyne or heterodyne detection. The main variants of the two-way CV-QKD protocols, both P&M and EB, were introduced in (Pirandola *et al.*, 2008c). Later extensions involved its realization at different wavelengths (Weedbrook *et al.*, 2014). These protocols enable higher robustness to channel noise compared to one-way protocols.

5. Measurement-device independent protocols

CV quantum states and homodyne detection can be used to implement MDI protocols, as first demonstrated in (Pirandola *et al.*, 2015b) (see Fig. 5). Alice and Bob independently perform state preparation (signal state generation and modulation) on their sides, encoding their key data. The modulated signal travels through the quantum channels to a middle station (relay), where the signals are interfered, and detected in complementary quadratures (this is also known as CV Bell measurement, first proposed in the context of CV quantum teleportation (Braunstein and Kimble, 1998) as discussed in Sec. IV.F). The detection results are broadcast, which allows Alice and Bob to establish correlations between their data and perform error correction, parameter estimation, and privacy amplification. The measurement in this case can be fully controlled by Eve, because its imperfections are attributed to the channel. Simultaneously, this makes the protocol sensitive to device imperfections and the configuration with the relay in the middle is the least optimal as we discuss in Sec. III.B.6.

6. Thermal-state protocols

In CV-QKD, while typically pure coherent states are used, studies have shown that “noisy” thermal states are

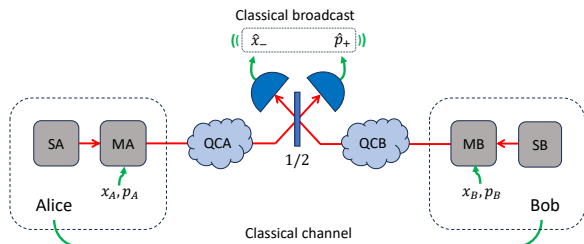


FIG. 5 CV-MDI-QKD scheme. Alice and Bob generate their signal states using each their own source (SA and SB) and perform modulation to encode their data on a respective modulator (MA and MB). The modulated signal travels through the quantum channels (QCA and QCB) to the middle station, where they are coupled on a balanced beam splitter with transmittance $1/2$, the outputs $\hat{x}_-$ and $\hat{p}_+$ are measured and classically broadcasted. The trusted parties then use the authenticated classical channel to perform error correction and privacy amplification.

also viable. Initial research (Filip, 2008; Usenko and Filip, 2010) demonstrated their effectiveness with RR and signal purification. Other studies (Papanastasiou *et al.*, 2018; Papanastasiou and Pirandola, 2021; Weedbrook *et al.*, 2014, 2010, 2012b) showed that thermal states could be directly employed in CV-QKD (without input purification). This led to extending CV-QKD to longer wavelengths. In this context, (Ottaviani *et al.*, 2020) explored the use of the terahertz spectrum for short-range terrestrial communications. Finally, the composable finite-size security of microwave wireless communications was shown in (Pirandola, 2021a).

B. Theoretical security

Theoretical security of QKD protocols relies on the set of assumptions, made about the protocol implementation and the capabilities of an eavesdropper. The underlying assumption of any security proof is that the trusted parties properly follow the protocol steps. However, deviations from a perfect implementation are unavoidable in practice and should be properly taken into account as we discuss in Sec. III.D. Theoretical security then first focuses on eavesdropping attacks in the quantum channel, which is assumed to be fully controlled by an eavesdropper. In addition, implementation-specific attacks can target and exploit practical device imperfections and side channels. The attacks in the quantum channel follow the general scenario of Eve preparing her ancillary states, performing interaction of the ancillae with the quantum signal states, sent through the channel, and measuring the ancilla states to obtain the information on the key. The task of the theoretical security analysis is then to evaluate the upper bound on Eve's information based on the disturbance introduced to the signals.

The most basic type of eavesdropping attack in the quantum channel is the *individual attack*, when Eve in-

dividually (one by one) prepares her ancillae and also individually measures them after the interaction with the signal. In the asymptotic limit of infinitely many signals, exchanged by Alice and Bob, which implies perfect parameter estimation, Eve's information on the key is then bounded by the classical (Shannon) mutual information between her data and the data of the reference side of the post-processing (Alice in DR scenario and Bob in RR). The Csiszár-Körner theorem for classical secure communication (Csiszár and Körner, 1978) can be then applied to QKD (Maurer, 1993) so that the amount of secret key that can be extracted from the data shared between Alice and Bob is lower-bounded by their information advantage over Eve:

$$\Delta I^{\rightarrow} = I_{AB} - I_{AE}, \Delta I^{\leftarrow} = I_{AB} - I_{BE} \quad (22)$$

in either of the reconciliation scenarios, denoted as $\rightarrow$ for DR and $\leftarrow$ for RR.

In the case of more advanced *collective attacks*, Eve is able to store her ancilla states in a quantum memory and later apply an optimal collective measurement after the bases reconciliation, reaching the amount of information given by the Holevo bound (19) between Eve's system (set of ancilla states) and the subsystem measured by the trusted party, which is the reference side of the post-processing. The secret key is then lower-bounded by the *Devetak-Winter rate* (Devetak and Winter, 2005), in the asymptotic regime for either of the reconciliation scenarios given by

$$R^{\rightarrow} = I_{AB} - \chi_{AE}, R^{\leftarrow} = I_{AB} - \chi_{BE} \quad (23)$$

The most general case of *coherent* (also called general) attacks implies that Eve is able to not only collectively measure her ancilla states, but to also collectively optimally prepare them. In the asymptotic limit, coherent attacks on CV-QKD are usually reduced to the collective ones as the signal states are independent and identically distributed (i.i.d.) and collective preparation does not bring any advantage to Eve, but if this is not the case or the data ensembles are limited, a rigorous treatment of coherent attacks is required, as we discuss in the next sections.

In the finite-size regime, the efficiency of parameter estimation is limited and should be taken into account. The most general security analysis of QKD then also takes into account the fact that key distribution is part of a more complex cryptographic system and should be described in a composable way, allowing to quantify the security of the key.

1. Notions of composable security

The primary purpose behind generating cryptographic keys lies in their application within larger cryptographic settings, such as in conjunction with one-time pad encryption. Consequently, the security of the generated

key must be guaranteed, regardless of its subsequent use. Composable security, in essence, leverages the security of subprotocols to establish the security of the entire cryptographic scheme. Historically, early QKD security proofs relied on a non-composable security definition, e.g., (Shor and Preskill, 2000), where the information gathered by an adversary was quantified. However, this approach was shown to be insecure when applied within a larger framework (König *et al.*, 2007). Inspired by the development of composability in classical cryptography (Canetti, 2000, 2001; Pfitzmann and Waidner, 2001), this notion was extended to the quantum realm by (Ben-Or *et al.*, 2005; Ben-Or and Mayers, 2004; Renner, 2006; Unruh, 2004). In the subsequent discussion, we will loosely follow (Portmann and Renner, 2022) and direct interested readers to this review for a more detailed exploration of composability.

In contrast to earlier security definitions, for composable security, we do not aim to quantify the amount of information an adversary has gathered, but rather ‘avoid’ defining security directly by instead comparing the real protocol with the ideal version of the protocol. This approach is known as the real-world-ideal-world paradigm. It can be illustrated as a virtual game, where the adversary is presented with two black boxes, one containing the real and the other containing the ideal protocol, without any indication of which box corresponds to which protocol. The adversary’s task is to act as a distinguisher, attempting to tell apart the real protocol from the ideal one. They may choose inputs and receive all outputs that are not private to Alice or Bob according to the protocol, randomly (with probability $\frac{1}{2}$) either from the box containing the real or the ideal protocol.

Within this paradigm, a real cryptographic system is called perfectly secure if the adversary cannot distinguish the black box containing the real protocol from the one containing the ideal protocol, i.e. if their guessing probability is exactly $\frac{1}{2}$, which is equal to the probability of random guessing.

To describe this idea in a mathematical framework, suppose we have two protocols $\mathcal{P}_0$ and $\mathcal{P}_1$ and assume a distinguisher $\mathcal{D}$ is provided with the outputs of both protocols with equal probability. The distinguisher then makes a guess $G \in \{0, 1\}$, and $C = 0$ or $C = 1$ denotes which protocol produced the output. The distinguishability then is defined as

$$d(\mathcal{P}_0, \mathcal{P}_1) := \sup_{\mathcal{D}} |\Pr[G = 0 | C = 0] - \Pr[G = 0 | C = 1]|, \quad (24)$$

where the supremum is taken over all distinguishers $\mathcal{D}$. It can be shown that for quantum states the right measure to capture the notion of distinguishability is half the trace norm (see, for example, (Barnett, 2009, Chapter 4) for an explanation),

$$d(\mathcal{P}_0, \mathcal{P}_1) = \frac{1}{2} \|\rho_{K_A K_B E}^{\text{ideal}} - \rho_{K_A K_B E}^{\text{real}}\|_1, \quad (25)$$

where the key of an ideal protocol is completely ran-

dom, uniformly distributed, and completely decoupled from the adversary’s knowledge, hence in tensor-product structure with Eve’s system,

$$\rho_{K_A K_B E}^{\text{ideal}} := p^\perp |\perp_A, \perp_B\rangle\langle\perp_A, \perp_B| \otimes \rho_E^\perp + \tau_{UU} \otimes \rho_E, \quad (26)$$

where $\tau_{UU} := \frac{1}{N} \sum_{x=0}^{N-1} |x, x\rangle\langle x, x|$, while the density matrix corresponding to the real protocol has the more general form

$$\rho_{K_A K_B E}^{\text{real}} = p^\perp |\perp_A, \perp_B\rangle\langle\perp_A, \perp_B| \otimes \rho_E^\perp + \sum_{x,y=0}^{N-1} P_{x,y} |x, y\rangle\langle x, y| \otimes \rho_E^{x,y}. \quad (27)$$

Here $\perp$ denotes the event of the protocol aborting and $p^\perp$ is the probability of that event.

Generally, one cannot expect to achieve perfect security in (real) cryptographic routines. However, we may allow the adversary a certain small distinguishing advantage $\epsilon \geq 0$. Additionally, a QKD protocol might abort sometimes in which case it is trivially secure as no key is produced. Then, we call a QKD protocol ϵ -secure if

$$(1 - p^\perp) \frac{1}{2} \|\rho_{K_A K_B E}^{\text{ideal}} - \rho_{K_A K_B E}^{\text{real}}\|_1 \leq \epsilon. \quad (28)$$

By applying the triangle inequality this can be rewritten as

$$(1 - p^\perp) \frac{1}{2} \|\rho_{K_A K_B E}^{\text{ideal}} - \rho_{K_A K_B E}^{\text{real}}\|_1 \leq \Pr[K_A \neq K_B] + (1 - p^\perp) \frac{1}{2} \|\rho_{AE}^{\text{real}'} - \tau_U \otimes \rho_E'\|_1.$$

The first term,

$$\Pr[K_A \neq K_B] \leq \epsilon_{\text{cor}} \quad (29)$$

is called correctness condition and ϵ_{cor} bounds the probability that the protocol does not abort and Alice and Bob do not share the same key, while the second term

$$(1 - p^\perp) \frac{1}{2} \|\rho_{AE}^{\text{real}'} - \tau_U \otimes \rho_E'\|_1 \leq \epsilon_{\text{sec}}, \quad (30)$$

is called secrecy condition and ϵ_{sec} bounds the joint probability of not aborting and the private information being known to Eve. Thus, if one manages to prove a protocol ϵ_{cor} -correct and ϵ_{sec} -secret, this implies that the protocol is $\epsilon := \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$ secure.

As previously mentioned, a protocol that aborts all the time is trivially secure, albeit not very useful. This notion is captured by the completeness or robustness of a protocol. A QKD protocol is called ϵ_{comp} -complete, if

$$\Pr[\perp | \text{HONEST}] \leq \epsilon_{\text{comp}}. \quad (31)$$

By HONEST we denote the honest implementation of the protocol, wherein all devices and the channel act as expected. In particular, no eavesdropping is taking place. Thus, if the protocol is ϵ_{comp} -complete, under honest conditions, it does not abort, except with probability ϵ_{comp} .

2. Individual attacks and channel models

Security of Gaussian CV-QKD against individual attacks was first shown for the coherent-state protocol in (Grosshans *et al.*, 2003b) and then extended to the squeezed-state protocol using equivalent EB representation. The security argument is based on the Heisenberg uncertainty principle, which prevents Eve from precisely simultaneously measuring both $\hat{x}$ and $\hat{p}$ quadratures. We assume that Alice and Bob ideally share a pure two-mode entangled state in modes A and B , and mode E is available to Eve for individual measurements after the interaction with mode B in a quantum channel. Then, after the projective quadrature measurements on modes A and E or B and E , the uncertainty principle can be generalized in terms of the conditional variances as

$$V_{A|B}V_{A|E} \geq 1, V_{B|A}V_{B|E} \geq 1. \quad (32)$$

This allows to bound the asymptotic key rate (22) using the expression (18) for the Shannon mutual information of the Gaussian-distributed data as

$$\Delta I_{\infty}^{\rightarrow} \geq \log \frac{1}{V_{A|B}}, \Delta I_{\infty}^{\leftarrow} \geq \log \frac{1}{V_{B|A}}. \quad (33)$$

Here and further we evaluate the key rate in bits (taking logarithm base 2) per transmitted symbol, i.e., a signal state, which is also called bits per pulse or bits per channel use, being independent of the system clock (repetition) rate. In the practical realizations of QKD the relevant figure of merit is bits per second (bps), which characterizes the actual speed of secret key distribution, and is scaled by the system clock rate.

A typical quantum channel, which describes well the optical fiber links, is the *thermal-loss* Gaussian channel defined by the channel transmittance (also referred to as channel loss or attenuation) T and excess noise of variance ν , characterized with respect to the channel input. The quadrature observable measured at the receiver is then $\hat{x}_B = \sqrt{T}(\hat{x}_S + \hat{x}_M + \hat{x}_N) + \sqrt{1-T}\hat{x}_0$, where $\hat{x}_S$ is the quadrature of the signal state prior to modulation with variance V_S (so that $V_S = 1$ for coherent-state protocol), $\hat{x}_M$ is the value of modulation (displacement) applied by the sender, taken from a zero-centered Gaussian distribution with variance V_M , $\hat{x}_N$ is the contribution from the channel excess noise with variance ν , and $\hat{x}_0$ is the contribution from the vacuum noise with variance 1, same for the $\hat{p}$ quadrature. The modulated signal of variance $V = V_S + V_M$ in either of the quadratures is then changed to $T(V + \nu) + 1 - T$ on the channel output. Note that often the channel noise introduced by the channel with respect to the input is joined into a single parameter $\chi = \nu + (1 - T)/T$, which simplifies the expression for the variance of the signal on the channel output to $T(V + \chi)$. The channel excess noise can be caused by numerous factors, such as, e.g., residual modulation noise, coupling to other optical modes (particularly, in the co-existence with other optical signals), or imperfect noise

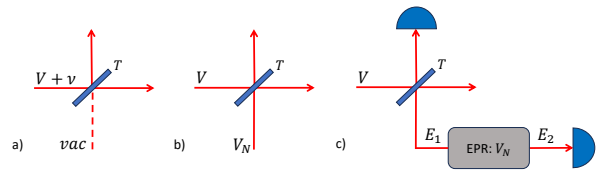


FIG. 6 Left (a): Gaussian thermal-loss channel, characterized by the excess noise ν , added to the modulated signal of variance V at the channel input, followed by pure loss T as coupling to a vacuum mode (vac). Middle (b): equivalent representation of the channel as coupling T of the modulated signal V to a thermal-noise mode with variance V_N . Right (c): entangling cloner attack as the purification of the thermal noise V_N by a TMSV (EPR) source with variance V_N in modes E_1 (coupled to the signal) and E_2 , both available for Eve for individual/collective measurements.

estimation in the finite-size regime. The parametrization of the channel noise by ν (or χ), which is then down-scaled by the channel transmittance T , as often used in the theoretical predictions of CV-QKD performance, can therefore be less relevant for the practical scenarios, where total noise from different sources if observed on the channel output. An equivalent parametrization of the excess noise on the channel output (hence, the noise beyond the vacuum noise due to losses) as $\nu_{\text{out}} = T\nu$, such that the variance measured by Bob is $TV + 1 - T + \nu_{\text{out}}$, can then be more adequate for predicting the performance of the protocols (and is used in the plot in Fig. 12).

For a perfectly implemented P&M protocol, the correlation between Alice's data, having variance V_M , and the data measured by Bob, is also down-scaled by the channel transmittance as $\sqrt{T}V_M$. Equivalently, the thermal-loss channel can be represented as a coupling of the signal mode to a thermal-noise mode with variance V_N at the coupling ratio T , as shown in Fig. 6(b). Equivalence then holds at $V_N = 1 + T\nu/(1 - T)$. Eve's optimal individual attack in such a channel, which allows her to saturate the bounds (32) set by the uncertainty principle, can be realized by means of an entangling cloner (Grosshans *et al.*, 2003a), as shown in Fig. 6(c). An entangling cloner is a TMSV state with quadrature variance V_N in modes $E_{1,2}$, so that one mode is coupled to the signal, and both modes are available to Eve for individual measurement. Such an attack can be seen as Eve's purification of the noise V_N , which allows her to improve the knowledge of the noise added in the channel, by conditionally preparing a squeezed state of variance $1/V_N$.

While individual attacks are the most restrictive for an eavesdropper and hence optimistic for the trusted parties, they still give important theoretical insights into the limitations of the protocols, particularly as insecurity against individual attacks implies insecurity against more advanced attack types such as collective or coherent attacks. Consequently, the key rate for individual attacks is an upper bound on the key rates for collective and coherent attacks. In the following subsections we proceed to security of CV-QKD against collective attacks.

3. Asymptotic security via Gaussian extremality

An important tool for showing security of the Gaussian CV-QKD is the Gaussian extremality theorem (Wolf *et al.*, 2006), which states that for fixed first and second moments, the distillable secret key rate against collective attacks is lower bounded by the secret key rate provided by a Gaussian state with these first and second moments,

$$R^{\text{coll}}(\rho) \geq R^{\text{coll}}(\rho_{\text{Gauss}}). \quad (34)$$

This theorem turned into the workhorse of CV security analyses and gave rise to a whole family of security proofs that rely on estimating the covariance matrix of the objective quantum state. Eqn. (34) and consequently the obtained secure key rates, are tight if the modulation is Gaussian and essentially tight if the modulation is close to Gaussian. Therefore, arguments of this type have been applied to both Gaussian-modulated as well as DM protocols, as we will elaborate on in what follows.

a. Gaussian modulated CV-QKD protocols For collective attacks the Devetak-Winter formula $R_{\infty}^{\rightarrow}, R_{\infty}^{\leftarrow}$ (23) gives a bound for the secure key rate in the asymptotic limit. While the mutual information between trusted parties I_{AB} is assessed similarly to be individual attacks case, described above (as it does not depend on the type of attack in the given quantum channel), the estimation of the bound on Eve's information is different for collective attacks. Early applications of the Gaussian extremality theorem (Wolf *et al.*, 2006) to Gaussian-modulated protocols proved the optimality of Gaussian attacks (García-Patrón and Cerf, 2006; Navascués *et al.*, 2006). In the case of pure loss (thermal-loss channel with no excess noise, $\nu = 0$), the information available to Eve and described by the Holevo bound can be then directly obtained from the state in the initial vacuum mode after the beam splitter T , as shown in Fig. 6(a) (Grosshans, 2005). For the noisy channels, $\nu > 0$, the purification argument is used to assess Eve's information: since Eve is able to control all the untrusted noise, added in the quantum channel, the overall state of the three-partite system ABE is pure. The entropic triangle inequality (Araki and Lieb, 1970) turns into $S(E) = S(AB)$. Similarly, after projective homodyne measurements at Alice's or Bob's systems A or B , the equalities $S(E|A) = S(AB|A) = S(B|A)$ and $S(E|B) = S(AB|B) = S(A|B)$ hold. Therefore, the Holevo bound can be directly evaluated from the state shared between Alice and Bob using the expression (21), without the need to explicitly model the quantum channel (and allowing for multiple instances of such), so that all the impurity (noise) in the bipartite state of AB is attributed to Eve. Note that it requires purification (by building equivalent EPR states) of all presumably trusted noise in the devices of Alice and Bob. Typically the trust assumption applies to the sending and receiving stations (given inside the dashed boxes in Fig. 3). We discuss

the incorporation of this noise into the security analysis in Sec. III.D. Security of CV-MDI-QKD is obtained similarly after conditioning the covariance matrix, shared between the trusted parties in the EB version of the protocol, by the publicly announced outcomes of the measurements on $\hat{x}_{-}$ and $\hat{p}_{+}$. Note, that alternatively to the above-described purification-based approach, the Holevo bound, limiting Eve's accessible information in case of collective attacks on CV-QKD, can be obtained from the two-mode entangling cloner, as shown in Fig. 6(c). While for a single-mode quantum channel it yields the same results as the purification-based analysis, it requires additional optimization in the multi-mode case (Pirandola *et al.*, 2015b) to account for possible correlations between the cloners.

Gaussian collective attacks on coherent-state CV-QKD were generalized in the asymptotic regime in (Pirandola *et al.*, 2008a), showing the extremality of canonical attacks, which correspond to the thermal-loss channels, and can be explicitly described by the entangling cloner model, as shown in Fig. 6(c).

Security against collective attacks in the asymptotic regime can be directly extended to security against general (coherent) attacks, using de Finetti representation theorem for infinite-dimensional systems (Renner and Cirac, 2009). On the other hand, in the case of passive eavesdropping (noiseless channels with $\nu = 0$), asymptotic collective attacks reduce to the individual ones.

While practical security of QKD protocols can only be shown in the finite-size regime, the asymptotic security proofs remain essential for establishing theoretical security bounds of the protocols and can be used to preliminarily assess the possibility of performing QKD under given conditions. Particularly, asymptotic bounds can be used to establish limits on the performance of the protocols, as we discuss later.

b. DM CV-QKD protocols As mentioned in the introductory paragraph to this section, the Gaussian extremality argument applies generally and, therefore – at the cost of introducing looseness for modulation patterns that do not resemble Gaussian modulation well – can also be used to analyze the security of DM CV-QKD protocols. This was first carried out in (Leverrier *et al.*, 2009), where the authors analyzed a four-state protocol with coherent states known as quadrature phase shift keying (QPSK). Although this work showed that in regimes of low signal-to-noise ratio (SNR), DM protocols can outperform Gaussian-modulated ones due to more efficient error-correction codes, the reported key rates are still pessimistic, as they overestimate the adversary's knowledge about the key.

More recent methods for DM protocols combine the Gaussian extremality argument with semi-definite programming (SDP) theory. Historically first, (Ghorai *et al.*, 2019b) analyses a QPSK protocol with heterodyne detection. They quantify the quality of the correlations

between Alice and Bob by two experimentally accessible parameters, the ‘variance’ v and the ‘covariance’ c . While Alice’s variance V_A is known and Bob’s variance $V_B = v$ is determined via measurements, the only unknown quantity in the covariance matrix $\begin{pmatrix} V_A \mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & V_B \mathbb{1}_2 \end{pmatrix}$ (see also Eq. 16) representing Alice’s and Bob’s joint state is the covariance σ_{AB} , denoted by the authors as Z , which can be calculated via

$$Z = \text{Tr}\{(ab + a^\dagger b^\dagger) \rho_{AB}\}. \quad (35)$$

It is well-established that for fixed V_A and V_B , the Holevo quantity $\chi(Y : E)$ is a decreasing function in Z . Thus, finding the smallest Z yields the maximum $\chi(Y : E)$ and consequently minimizes R^∞ . Therefore, let Π be the orthogonal projector onto the space spanned by the four coherent states prepared by Alice and define $C := \Pi \hat{a} \Pi \otimes \hat{b} + \Pi \hat{a}^\dagger \Pi \otimes \hat{b}^\dagger$. The minimal Z compatible with Bob’s measurements is determined by solving the following semi-definite program

$$\begin{aligned} & \min \text{Tr}\{CX\} \\ & \text{s.t.} \\ & \text{Tr}\{B_0 X\} = v, \\ & \text{Tr}\{B_1 X\} = c, \\ & \text{Tr}_B \{X\} = \sigma_A, \\ & X \geq 0. \end{aligned} \quad (36)$$

In this context, B_0 and B_1 are operators related to the measurement of v and c , and $(\sigma_A)_{k,l} := \frac{1}{4} \langle \alpha_k | \alpha_l \rangle$ is given by the overlap between Alice’s (coherent) signal states. The final constraint requires X to be positive semi-definite. The found optimum Z^* can be used to calculate the Holevo quantity through standard techniques.

The present optimization problem can be solved numerically with standard SDP solvers. However, the numerical implementation on a computer requires to cutoff the Fock basis, which is used to formulate the optimization problem, at some number N_c . We discuss this cutoff within the course of the subsequent method, where a similar cutoff assumption had to be made. It is noteworthy that the method by (Ghorai *et al.*, 2019a) can be generalized to higher constellations. However, due to the increased computational demands of the numerical optimization for a larger number of signal states, transitioning to more complex constellations is deemed infeasible with present-day technology.

Due to the computational complexity of numerical methods, the analysis of quadrature amplitude modulation (QAM) constellations with 64 or more signal states appears to be currently beyond reach. Therefore, in what follows, we explore analytical methods that cover this regime. The work by (Denys *et al.*, 2021) adopts an approach akin to (Ghorai *et al.*, 2019a), using a Gaussian optimality argument. However, they give a complete analytic solution, feasible for general modulation schemes. The main idea of their method is the following. While

the first term in the Devetak-Winter formula is essentially known, they optimize the Holevo quantity over all quantum channels compatible with Bob’s measurement results, which turns out to be the more challenging task. By applying Gaussian extremality, they upper-bound the optimization by a supremum of the Holevo quantity over all Gaussian states compatible with Bob’s observations. Since Gaussian states are fully characterized by their covariance matrix, this simplifies the task significantly. The only unknown is the covariance Z . While this quantity can be calculated easily for Gaussian protocols, this is not the case for DM protocols. However, the authors formulate the objective optimization problem as a semi-definite program of the form

$$\begin{aligned} & \min \text{Tr}\{(ab + a^\dagger b^\dagger) \rho\} \\ & \text{s.t.} \\ & \text{Tr}\{C_1 \rho\} = 2c_1, \\ & \text{Tr}\{C_2 \rho\} = 2c_2, \\ & \text{Tr}\{N_B \rho\} = n_B, \\ & \text{Tr}_B \{\rho\} = \bar{\tau}, \\ & X \geq 0, \end{aligned} \quad (37)$$

where C_1, C_2 and N_B are observables with expectations c_1, c_2 and n_B , and $\bar{\tau}$ is Alice’s reduced density matrix given by the overlap between her signal states. Authors then provide analytical bounds for the value of Z , with the lower bound reading

$$Z \geq 2c_1 - 2\sqrt{w \left(n_B - \frac{c_2}{\langle n \rangle} \right)}. \quad (38)$$

This lower bound is a function of the experimentally accessible quantities c_1, c_2 and n_B (with the latter being the received photon number on Bob’s side) and w and $\langle n \rangle$ which quantify the modulation strength, thus are functions of protocol parameters. This finally allows the calculation of the Holevo quantity via symplectic eigenvalues and, therefore, gives a lower bound on the secure key rate. For coherent state protocols, the obtained bounds recover the rates known from Gaussian modulation and closely match the numerical bounds by (Ghorai *et al.*, 2019a) in most practical regimes. The authors state that their proof is already essentially tight for modulations with 64-QAM and higher.

The proof presented by (Kaur *et al.*, 2021) follows a distinctive approach, in addition to incorporating a Gaussian extremality argument. The authors utilize a method to approximate Gaussian probability distributions using a finite-size Gauss-Hermite constellation, and they bound the approximation error in trace norm. Eve’s information for this approximated constellation, which is bounded by the Holevo quantity, closely approaches the Holevo information for a Gaussian modulated protocol. The error made can be bounded by a function of the approximation error in trace norm, employing an entropic continuity bound. In contrast to (Denys *et al.*, 2021), the

authors assert that their method requires a constellation with about 5000 states to achieve results close enough to Gaussian modulation, which suggests that the bounds provided by (Denys *et al.*, 2021) are tighter already for lower constellation sizes and that bounds tend to be loose for smaller constellations. However, they essentially align with the results known from Gaussian modulation when dealing with sufficiently large constellations.

While the Gaussian extremality argument is tight for Gaussian protocols, it can overestimate the adversary's knowledge about the key for DM protocols, in particular, if the modulation pattern is very far from Gaussian.

4. Asymptotic security without Gaussian extremality

In the previous section, we have seen that Gaussian extremality-based arguments introduce looseness in the key rates of DM CV-QKD protocols, in particular for modulation patterns with a low number of signal states. However, technical challenges and implementation difficulties for Gaussian CV-QKD protocols that persist to date motivated the development of techniques that directly evaluate the Devetak-Winter formula given in Eq. (23) for the employed quantum states. This, however, is a notoriously difficult task, that requires new techniques.

a. Restriction to purely lossy channels. Early security analyses not only focused on the asymptotic regime but relied on the simplifying assumption of purely lossy (i.e., zero noise, $\nu = 0$) channels. One of the pioneering works traces back to (Heid and Lütkenhaus, 2006). In this study, a protocol with binary modulation in which Bob performs heterodyne measurements is analyzed. Under the simplifying assumption of a loss-only channel with transmittance T , the optimal attack is known to be the beam splitter attack, where Eve replaces the channel with a beam splitter and branches off $|\pm\sqrt{1-T}\alpha\rangle$, while Bob receives $|\pm\sqrt{T}\alpha\rangle$. Mathematically, Bob's heterodyne measurement is a projection onto coherent states, enabling him to confirm that he received a pure state. Eve's share has a tensor-product structure with Bob's pure state and is unitarily equivalent to $|\epsilon_i\rangle := |(-1)^i\sqrt{1-T}\alpha\rangle$, $i = 0, 1$. In both direct and reverse reconciliation this allows straightforward calculation of the Holevo quantity. Since the mutual information between Alice and Bob follows from purely classical considerations, we already hold all the ingredients to evaluate the Devetak-Winter formula to obtain secure key rates. Additionally, by slight modifications, this approach allows taking post-selection as well as trusted detector noise into account. Although the proof in this work was explicitly carried out for two states, the idea can be generalized to higher constellations, as demonstrated in (Sych and Leuchs, 2010) for 2-8 states, for an arbitrary number of signal states as a side-result in (Kanitschar and Pacher,

2022, Appendix A) and recently even to the multi-user scenario (Kanitschar and Pacher, 2024).

b. Noisy channels and specific constellations. One of the pioneering approaches that considered excess noise was presented in (Zhao *et al.*, 2009). They analyzed a two-(coherent)-state CV-QKD protocol with homodyne detection in the asymptotic limit and proved security against collective attacks. The authors employed a method developed in (Rigas, 2006), which estimates the largest eigenvalue and corresponding eigenvector, based on first and second moment measurements. Subsequently, they use Bob's homodyne measurement results to construct a statistical model of Eve's quantum state, which needs to be compatible with Bob's measurements. Under the worst-case scenario, where Eve gains the most information, this approach provides a lower bound on the secure key rate. The crucial steps rely on two properties of the binary Shannon entropy, namely the monotonicity and the concavity as a function of the absolute value of the overlap of the two states. While proving these properties for two states is feasible, generalizing them poses a considerable challenge. In (Bradler and Weedbrook, 2018), the main idea was to establish both properties for the ternary Shannon entropy which is used to complete the security proof for a phase-shift keying protocol with three signal states. This extended the proof idea to a three-state phase-shift keying protocol. However, generalizing monotonicity and concavity to the N state case in a similar fashion is challenging, if not currently infeasible. As concluded by the authors in (Bradler and Weedbrook, 2018), it is likely that a more general argument is needed to establish similar properties for suitably generalized entropic quantities, thus extending this proof further to $N > 3$. This suggests the necessity of a fundamentally different approach for a higher number of signal states. Additionally, compared to the more recent proofs to be discussed subsequently, the key rates turn out to be pessimistic.

c. General discrete constellations. By the end of the last decade, the incorporation of SDP for secure key rate calculations opened the door to a new generation of security proofs, with a representative not exploiting Gaussian extremality being (Lin *et al.*, 2019), which is part of the numerical framework by Lütkenhaus *et al.* (Coles *et al.*, 2016; Winick *et al.*, 2018).

The Devetak-Winter rate is reformulated as

$$R^\infty = \min_{\rho_{AB} \in \mathcal{S}} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}(\mathcal{G}(\rho_{AB}))) - p_{\text{pass}} \delta_{EC}, \quad (39)$$

where $D(\cdot || \cdot)$ denotes the quantum relative entropy, $\mathcal{G}$ is a completely positive trace non-increasing map describing the classical postprocessing and $\mathcal{Z}$ is a pinching channel describing the key map, δ_{EC} denotes the leakage per signal and p_{pass} is the sifting probability. The optimization

is carried out over the set $\mathcal{S}$, which is defined by Bob's observations and the requirement that ρ_{AB} is the joint quantum state of Alice and Bob. Thus, the main idea of this proof method can be summarized as finding the worst-case density matrix that is physical and compatible with Bob's observations. This problem turns out to be a semi-definite program which then needs to be solved efficiently.

Assuming Alice prepares one out of N_{St} coherent states $|\psi_i\rangle$ with probability p_i , this leads to the following optimization problem

$$\begin{aligned}
& \text{minimize } D(\mathcal{G}(\rho_{AB}) || \mathcal{G}(\mathcal{Z}(\rho_{AB}))) \\
& \text{subject to:} \\
& \text{Tr}\{\rho_{AB} (|k\rangle\langle k|_A \otimes \hat{x})\} = p_k \langle \hat{x} \rangle_k \\
& \text{Tr}\{\rho_{AB} (|k\rangle\langle k|_A \otimes \hat{p})\} = p_k \langle \hat{p} \rangle_k \\
& \text{Tr}\{\rho_{AB} (|k\rangle\langle k|_A \otimes \hat{n})\} = p_k \langle \hat{n} \rangle_k \\
& \text{Tr}\left\{\rho_{AB} \left(|k\rangle\langle k|_A \otimes \hat{d}\right)\right\} = p_k \langle \hat{d} \rangle_k \\
& \text{Tr}_B \{\rho_{AB}\} = \sum_{i,j=0}^{N_{\text{St}}-1} \sqrt{p_i p_j} \langle \psi_j | \psi_i \rangle |i\rangle\langle j|_A \\
& \rho_{AB} \geq 0,
\end{aligned} \tag{40}$$

where $\hat{x}$ and $\hat{p}$ are the quadrature operators, $\hat{n}$ is the photon-number operator and $\hat{d} := \hat{x}^2 - \hat{p}^2$ is another second-moment operator. The objective function is convex and highly non-linear. This problem is addressed by employing the numerical security proof framework by (Coles *et al.*, 2016; Winick *et al.*, 2018), which involves a two-step process. In the first step, the nonlinear objective function is linearized and solved approximately. This can be accomplished, for instance, through an iterative first-order algorithm like the Frank-Wolfe algorithm (Frank and Wolfe, 1956). As we cannot expect to find the exact minimum, the output of the first step serves only as an upper bound on the secure key rate. Therefore, in the second step, this approximate solution is transformed into a secure lower bound by combining another linearization and SDP duality theory. Additionally, the application of a relaxation theorem (Winick *et al.*, 2018) takes numerical imprecision into account. The authors of (Lin *et al.*, 2019) demonstrate their approach both for a two-state protocol with homodyne detection and a four-state QPSK protocol with heterodyne detection. Other studies extended the method to higher constellations (8PSK, 12PSK, two-ring constellation) (Kanitschar and Pacher, 2022; Kanitschar, 2021; Wang *et al.*, 2023), broadened the framework to include trusted detectors (Lin and Lütkenhaus, 2020), optimized key mapping for QPSK encoding to achieve higher noise tolerance (Liu *et al.*, 2021), and generalized the framework to the multi-user scenario (Kanitschar and Pacher, 2024). While the nonlinear objective function in (Lin *et al.*, 2019) necessitates an iterative approach and is numerically more intense and demanding than the method proposed by (Ghorai *et al.*, 2019a), the key rates obtained

by (Lin *et al.*, 2019) are significantly higher, particularly for scenarios with medium to high loss. This highlights the advantages of DM CV-QKD security proofs without Gaussian extremality argument. An illustration can be found in (Lin *et al.*, 2019, Figure 9). Additionally, it is noteworthy that the method by (Lin *et al.*, 2019) allows post-selection, which can increase key rates further.

As in the case of the proof by (Ghorai *et al.*, 2019a), the optimization has to be carried out numerically on a computer (for example, via the numerical packages based on (Grant and Boyd, 2008, 2014; Toh *et al.*, 1999; Tütüncü *et al.*, 2003)). Consequently, the (Fock) basis used to describe the generally infinite-dimensional density matrix and operators must be truncated at a certain value N_c to allow representation on a computer. While the computed rates numerically saturate when increasing the value of the cutoff, suggesting that the error introduced by the truncation becomes negligible, it potentially introduces a vulnerability in both security arguments. This concern was addressed by (Upadhyaya *et al.*, 2021), which eliminated this photon-number cutoff assumption. They develop a continuity-bound argument that allows the quantification of the error introduced when substituting the evaluation of the objective function on the original infinite-dimensional state by a finite-dimensional cutoff version. Moreover, they describe a method to calculate the weight of the original state outside of the cutoff space. This weight, in turn, leads to a correction term for the key rate, ensuring security while eliminating the photon-number cutoff assumption. We note that the correction term was improved in (Upadhyaya, 2021).

5. Finite-size security

So far, our discussions have focused on security proofs in the asymptotic regime, i.e., operating under the simplifying assumption that Alice and Bob exchange an infinite number of signals. However, in practical scenarios, Alice and Bob are constrained by real-world limitations and must cease quantum signal exchanges after a certain duration to start generating keys. Consequently, ultimately, it requires security proofs within the finite-size regime. Additionally, the obtained key should be usable safely in any larger cryptographic protocol, which means the key needs to be composable secure (see Section III.B.1 for details). Compared to the asymptotic case, this poses several challenges for security analyses in the finite-size regime. Firstly, the Devetak-Winter formula offers a secure key rate expression based on von Neumann entropy, an asymptotic measure. However, deriving an equivalent bound for the finite-size regime is more intricate. Secondly, while in the asymptotic scenario protocol observables are deterministically known, statistical fluctuations and the exclusion of testing rounds for key generation purposes must now be considered. In essence, while in the asymptotic regime the channel parameters (like loss

and noise) were basically predetermined, they remain uncertain even after protocol execution in the finite-size regime. Thirdly, we cannot expect to prove our protocol secure with certainty anymore but instead must accept a small error probability ϵ . Furthermore, whereas in the asymptotic regime collective attacks were deemed to be effectively optimal (Christandl *et al.*, 2009), this is not necessarily the case in the finite-size regime anymore. In summary, the need for more sophisticated security arguments is evident, and it is expected that finite-size key rates will be lower compared to those achievable in the asymptotic regime. However, the goal is to derive expressions that reconcile the asymptotic key rates in the limit of an infinite number of rounds, $N \rightarrow \infty$. It is worth noting that various authors employ slightly different total ϵ parameters, which quantify the error probability of their protocols, when presenting secure key rates, making direct comparisons challenging. Nonetheless, given the prevalence of values around $\epsilon = 10^{-10}$ in literature, qualitative comparisons between different studies remain feasible. Having addressed the challenges, we now present the status of finite-size security proofs for CV-QKD protocols.

a. Finite-size security of Gaussian CV-QKD protocols via Gaussian extremality. The extension of Gaussian CV-QKD security analysis to the finite-size regime was performed in (Leverrier *et al.*, 2010) following the formalism developed in (Renner, 2006) and applied to DV protocols in (Scarani and Renner, 2008), by taking into account the finite-size effects in the parameter estimation. This included the reduction of the key rate due to use of the fraction m of the overall data set $N = m + n$ for parameter estimation, redefinition of the Holevo bound as $\chi_{\epsilon_{PE}}(E : y)$, being the maximum channel capacity between the reference side of the post-processing y and the eavesdropper's system E , compatible with the measurement statistics, except with a given probability of failure ϵ_{PE} , and introduction of the correction term $\Delta(n)$, related to security of privacy amplification and dominated by the speed of convergence of the smooth min-entropy of an i.i.d. state toward the von Neumann entropy. The resulting modified Devetak-Winter bound then reads

$$k = \frac{n}{N} [\beta I(x : y) - \chi_{\epsilon_{PE}}(E : y) - \Delta(n)], \quad (41)$$

where the post-processing (error correction) efficiency β , which prevents the trusted parties possessing the data x, y from reaching the Shannon mutual information $I(x : y)$, as we discuss in Sec. III.E, is taken into account. Evaluation of the modified Holevo bound $\chi_{\epsilon_{PE}}$ is then based on the derivation of the equivalent two-mode entangled state, similarly to the asymptotic case, but expressed through the minimum value of transmittance and maximum value of channel noise, compatible with the sampled data except with a pre-defined probability $\epsilon_{PE}/2$. The correction $\Delta(n)$ on the other hand

can be for the binary encoded data well approximated by $7\sqrt{\log(2/\bar{\epsilon})/n}$, where $\bar{\epsilon}$ is a pre-defined smoothing parameter and is largely governed by the data size n .

The described approach was the first step toward finite-size security analysis of CV-QKD and can be seen as the patch to the asymptotic security proofs, which is valid in the assumption that Gaussian attacks remain optimal in the finite-size regime. However, it demonstrated the importance of finite-size effects in the practical security of the protocols. This approach to finite-size security of Gaussian CV-QKD was extended to arbitrary signal states and optimized in (Ruppert *et al.*, 2014) and then applied to CV-MDI-QKD protocols in (Papanastasiou *et al.*, 2017).

b. Composable security of Gaussian CV-QKD protocols. Composable finite-size security against collective attacks was rigorously proven for the no-switching protocol (coherent states and heterodyne detection) in (Leverrier, 2015), taking into account discretization of the continuous-variable parameters and estimation of the symmetrized covariance matrix of an equivalent entangled state. The leftover hashing lemma (LHL) (Tomamichel *et al.*, 2011) applied to the smooth min-entropy (Renner, 2008) is used to bound Eve's information compatible with the estimated states and probabilities of failure of the protocol procedures. The key rate of the ϵ -secure protocol with $\epsilon = 2\epsilon_{sm} + \bar{\epsilon} + \sqrt{\epsilon_{PE} + \epsilon_{cor} + \epsilon_{ent}}$, composed, respectively, of the smoothing parameters ϵ_{sm} and $\bar{\epsilon}$, parameter estimation failure probability ϵ_{PE} , error correction failure probability ϵ_{cor} , and smooth min-entropy bounding failure probability ϵ_{ent} , is then upper bounded by

$$2n \left[2\hat{H}_{MLE}(U) - f(\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}) \right] - \text{leak}_{EC} - \Delta_{AEP} - \Delta_{ent} - 2 \log \frac{1}{2\bar{\epsilon}}, \quad (42)$$

where $\hat{H}_{MLE}(U)$ is the empirical entropy (the maximum likelihood estimator of the entropy) of the discretized data obtained by Bob; $\Delta_{AEP} := \sqrt{2n} \left[(d+1)^2 + 4(d+1) \log \frac{2}{\epsilon_{sm}^2} + 2 \log \frac{2}{\epsilon_{sm}^2} \right] - 4 \frac{\epsilon_{sm} d}{\epsilon}$ is the correction to the bound on the smooth min-entropy due to asymptotic equipartition property (AEP) (Tomamichel *et al.*, 2009); $\Delta_{ent} := \log \frac{1}{\epsilon} - \sqrt{8n \log^2(4n) \log(2/\epsilon)}$; f is the Holevo information between Eve and Bob's data, computed from the Gaussian state with covariance matrix parametrized by $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$, being the worst-case values compatible with ϵ_{PE} ; and leak_{EC} is the size of the syndrome of Bob's data, sent to Alice during the error correction and defined by the pre-set error correcting code. Note that the proof was constructed for the more practical RR scenario, but can be directly applied to DR by swapping the roles of the trusted parties. Using the post-selection technique (Christandl *et al.*, 2009) in the additional

symmetrization step of the protocol, the finite-size security against collective attacks for the no-switching protocol can be extended to general attacks (Leverrier, 2015). Importantly, the achievable key rate asymptotically reaches the bound obtained in the assumption of Gaussian attacks. However, the key rates reached using the post-selection technique remained limited and the bound for the no-switching protocol in case of the general attacks in the finite-size regime was improved by applying Gaussian de Finetti reduction (Leverrier, 2017) enabled by an energy test, which allows truncation of the infinite-dimensional Hilbert (Fock) space. Hence, it is sufficient to show finite-size security of the no-switching Gaussian CV-QKD protocol against collective Gaussian attacks, using the above-described technique, in order to attain security against general attacks.

Alternatively, composable finite-size security against general attacks was shown for the squeezed-state protocol with homodyne detection (Cerf *et al.*, 2001), using the entropic uncertainty relations (Furrer *et al.*, 2012), and extended to RR scenario (Furrer, 2014). The achievable key rates are, however, still sensitive to losses and do not comply with the asymptotic rates in the limit of large data ensemble size (Leverrier, 2015) suggesting that the obtained bounds are not tight.

More recently, (Pirandola and Papanastasiou, 2024) derived an alternative formula for the composable-secure secret key rate of Gaussian CV-QKD protocols which holds for implementations where parameter estimation is done before error correction. Let $N = n + m$ be the total states in a block, where m are used for PE, while the remaining n are for key generation. According to Eq. (68) of (Pirandola and Papanastasiou, 2024), one can achieve the key rate

$$R \leq \frac{p_{\text{ec}}[n\hat{R}_{\infty}^{\text{pe}} - n\delta_{\text{ent}} - \sqrt{n}\delta_{\text{aep}} + \theta]}{N}, \quad (43)$$

where p_{ec} is the probability of successfully correcting a block, $\hat{R}_{\infty}^{\text{pe}}$ is the asymptotic key rate computed from the m -state parameter estimation (with error ϵ_{pe}), $\delta_{\text{ent}} = \log(n)\sqrt{2n^{-1}\ln(2/\epsilon_{\text{ent}})}$ accounts for the imperfect estimation of Bob's entropy (with error ϵ_{ent}), $\delta_{\text{aep}} \simeq 4\log(2^{d/2} + 2)\sqrt{\log(2/\epsilon_s^2)}$ accounts for AEP (with digitalization d and smoothing parameter ϵ_s), while $\theta := \log(2\epsilon_h^2\epsilon_{\text{cor}})$ depends on the hashing parameter ϵ_h and the epsilon-correctness ϵ_{cor} . This rate is valid against collective Gaussian attacks with epsilon secrecy $\epsilon_{\text{sec}} = \epsilon_s + \epsilon_h$ and total epsilon security $\epsilon = \epsilon_{\text{cor}} + \epsilon_{\text{sec}} + \epsilon_{\text{ent}} + 2\epsilon_{\text{pe}}$ (note that this is the residual error affecting each block). Finally, using the energy test procedure described above, the key rate formula in Eq. (43) can be extended to security against coherent attacks for the specific case of the no-switching protocol.

Composable finite-size security of Gaussian CV-MDI-QKD against general attacks was initially discussed in (Lupo *et al.*, 2018) by first considering the finite-size security against collective Gaussian attacks and then applying Gaussian de Finetti reduction. The security proof

was later refined and improved in (Papanastasiou *et al.*, 2023) where the explicit methods for data processing were also provided. (Ghalaii and Pirandola, 2023) extended the security of Gaussian CV-MDI-QKD to free space channels, generally affected by diffraction, pointing errors, and turbulence effects. More generally, (Ghalaii *et al.*, 2022) extended the composable security to Gaussian quantum networks with untrusted relays.

Finally, by generalizing the security proof techniques applied to the no-switching protocol, the composable finite-size security against general attacks was also shown in (Ghorai *et al.*, 2019a) for two-way Gaussian CV-QKD with heterodyne detection.

c. Finite-size security of DM CV-QKD protocols via Gaussian extremality. Similarly to asymptotic proofs, methods for proving the security of DM CV-QKD protocols relying on Gaussian extremality arguments emerged. In (Papanastasiou and Pirandola, 2021) the authors undertake a thorough analysis of the composable finite-size security of a CV-QKD protocol using phase-encoded coherent states and heterodyne detection against Gaussian collective attacks. Their investigation assumes the presence of trusted thermal noise and does not consider post-selection. By leveraging the LHL against quantum side-information (Tomamichel *et al.*, 2011), they derive a bound on the secure key rate. Exploiting the tensor-product structure of the quantum state, which follows from the collective attack assumption, and using AEP they express their key rate formula in terms of the von Neumann entropy. This formulation allows them to establish a connection between finite-size key rates and asymptotic key rates, accounting for finite-size correction terms. Parameter estimation is conducted through maximum likelihood estimators. The resulting key rate formula then is evaluated numerically, with the introduction of a cutoff to make the problem computationally feasible. However, this cutoff remains as an assumption. The paper focuses on the case involving two and three signal states as already for this limited number of states, the computational demand seems to be considerable, specifically, achieving a higher number of significant digits necessary for low transmission (i.e., high distances). While the approach is rather general, it remains uncertain whether it can be effectively extended to accommodate a larger number of signal states.

The study by (Lupo and Ouyang, 2022) analyses the composable finite-size security of a DM CV-QKD protocol with coherent states against collective attacks. A key aspect of their approach involves considering the limitations inherent in real detectors, such as finite detection range and precision. They exploit this to establish a bound on the probability that the pulse Bob receives contains an extensive number of photons, which is used to define the numerical cutoff. Subsequently, Winter's gentle measurement lemma (Winter, 1999) allows the bounding of the trace-norm between Alice's and Bob's actual

(infinite-dimensional) quantum state and a cutoff version thereof. Shirokov’s continuity bound for the Holevo quantity (Shirokov, 2017) is utilized to quantify the effect of this cutoff on the Holevo information by introducing a penalty term. Finally, a Gaussian extremality argument and additional adjustments due to the application of the AEP (Tomamichel *et al.*, 2009) lead to a semi-definite program for the secure key rate that can be solved by methods presented in (Ghorai *et al.*, 2019a), all without relying on a cutoff. Following the idea proposed by (Leverrier, 2015), the composable finite-size parameter estimation procedure takes place after error-correction and is based on a Chernoff-bound argument. The authors report non-zero key rates for block-sizes of $N = 10^{10}$ and larger, and for large N , their key rates converge to their own asymptotic key rates (including detector limitations) as well as to those reported by (Ghorai *et al.*, 2019a).

d. Finite-size security without Gaussian extremality. For similar reasons as for the asymptotic regime, for DM CV-QKD protocols with low modulation patterns, methods that do not rely on Gaussian extremality arguments can yield significantly higher finite-size key rates.

The work by (Matsuura *et al.*, 2021) follows a phase-error rate-based idea composable security of a binary phase-modulated CV-QKD protocol with heterodyne detection in the finite-size regime. The central idea revolves around a new method used to estimate the fidelity between the received optical state and a coherent state and a conversion of the unbounded expectation values obtained by heterodyne measurements into bounded values. This allows for reducing the problem similar to earlier Shor-Preskill-style security proofs for DV-QKD protocols. Notably, heterodyne detection is utilized for testing purposes, while homodyne detection is employed for signal generation. This requirement of both homodyne and heterodyne measurement was removed in (Yamano *et al.*, 2024). While this work marks the first general security proof for a DM CV-QKD protocol, their analysis does not include the option to trust parts of the noise or to perform post-selection and the obtained key rates for realistic settings are rather limited. Additionally, it is not clear if the proof method can be generalized to higher modulations, posing a challenge for its application in more complex scenarios.

Thus, we shift our focus to finite-size security proofs for general modulation patterns. Both methods discussed build up upon (Lin *et al.*, 2019), which we already discussed in Section III.B.4. Consequently, in principle, these methods are independent of the modulation pattern. However, due to computational constraints, they are practically restricted to a low number of signal states. As a result, both studies showcase their secure key rates using the QPSK protocol.

The work by (Kanitschar *et al.*, 2023) establishes composable finite-size security for DM CV-QKD protocols using coherent states against collective attacks. The

authors introduce a novel energy testing theorem, enabling to bound the weight of Alice’s and Bob’s state outside a finite-dimensional Hilbert space and prove security within Renner’s ϵ -security framework (Renner, 2006). They utilize an argument based on the finite-detection range of real detectors to derive bounds for Bob’s observables and Hoeffding’s inequality to define an acceptance set. For states passing both the energy test and the acceptance test (the composable finite-size version of parameter estimation), the LHL against infinite-dimensional side-information (Tomamichel *et al.*, 2011) establishes a relationship between the achievable secure key length and the smooth-min entropy of the considered state. The application of AEP allows the rewriting of the smooth min-entropy in terms of the von Neumann entropy. To rigorously account for the numerical cutoff, a generalized version of the dimension reduction argument by (Upadhyaya *et al.*, 2021) is applied, which introduces an additional weight-dependent correction term in the key rate formula. Subsequently, the secure key rate is numerically evaluated using an extended version of the framework proposed by (Coles *et al.*, 2016; Lin *et al.*, 2019; Winick *et al.*, 2018), where optimization over the density matrices in the acceptance set is performed. The method accommodates post-selection and considers non-ideal and trusted detectors. They report secure key rates for block sizes of $N = 10^9$ and beyond under experimentally viable conditions. Additionally, in the limit of $N \rightarrow \infty$ their secure key rates converge to the rates reported by (Lin *et al.*, 2019; Upadhyaya *et al.*, 2021). Furthermore, they discuss and address realistic and practically relevant non-unique acceptance scenarios, coining the notion of expected key rates under honest channel behavior, and attributing the non-zero abort probability of real protocols.

Finally, we turn to applications of entropy accumulation arguments. A study by (Bäuml *et al.*, 2024) establishes composable finite-size security for DM CV-QKD protocols using coherent states against general attacks, albeit still relying on a photon number cutoff. The authors apply the entropy accumulation theorem (EAT) (Dupuis and Fawzi, 2019; Dupuis *et al.*, 2020) which allows the lower bounding of the conditional smooth-min entropy of an unstructured (thus general) state in terms of a so-called min-tradeoff function. However, encountering challenges in satisfying a Markov condition necessary for the application of the EAT in the P&M version of the analyzed DM CV-QKD protocol, the authors introduce an additional round of testing and invent a state-tomography procedure that allows to certify correlations between Alice and Bob. Subsequently, the min-tradeoff function is computed using the numerical method by (Coles *et al.*, 2016; Lin *et al.*, 2019; Winick *et al.*, 2018), assuming a numerical cutoff, leading to numerical key rates. The authors report composable secure finite-size keys for block sizes of $N = 10^{12}$ and larger under practically relevant conditions. Importantly, the asymptotic behavior of this method closely resembles the

secure key rates reported by (Lin *et al.*, 2019). A more recent version following this approach (Pascual-García *et al.*, 2025) employs the generalized EAT (Metger *et al.*, 2022) as well as alternative advanced conic optimization routines (Lorente *et al.*, 2024). This improves the stability and precision of the numerical algorithm and, in certain scenarios, allows non-zero key rates for block sizes of 5×10^8 (as opposed to 5×10^{12} for the earlier version). However, the work still assumes a cutoff. This assumption is lifted in (Primaatmaja *et al.*, 2024), marking the first security proof against sequential coherent attacks without photon number cutoff assumption. In this work, the authors apply the generalized EAT to a DM CV-QKD protocol that estimates probability distributions rather than moments. They propose a novel reduction technique, taking care of numerical cutoffs rigorously, which, unfortunately, lowers the secure key rate via comparably large finite-size correction terms, and does not lead to convergence to the known asymptotic key rates. The authors note that the main loss in key rate is due to working with probabilities rather than observables, which was necessitated by applying entropy accumulation, along with losses in key rate due to using low order Gauss-Radau quadrature when applying the numerical method by (Araújo *et al.*, 2023) to evaluating key rates.

Finally, note that arguments based on the generalized EAT usually rely on a sequential assumption (Metger and Renner, 2023). This means Eve may only access one of the quantum systems sent from Alice to Bob at the same time, which can easily be enforced by either requiring confirmation of arrival or a certain temporal schedule for sending the signals. Both, however, limit the number of signals sent per time interval severely, particularly for CV systems that usually operate at high repetition rates. While this assumption, in principle, can be lifted to the case where Eve has access to not more than s subsequent signals at the same time, this leads to increased second-order corrections.

6. Limits of CV-QKD

Ideal models of CV-QKD provide the highest achievable theoretical key rates, close to the secret-key capacity of the bosonic lossy channel (the standard transmission model through an optical fiber). The exploration of the limits of CV-QKD started with the definitions of direct and reverse secret key capacities of a quantum channel K_D and K_R (Pirandola *et al.*, 2009). These capacities represent the maximum rates achievable by CV (and DV) QKD in direct and reverse reconciliation. They can be lower-bounded by the coherent information I_c (Lloyd, 1997; Schumacher and Nielsen, 1996) and the reverse coherent information (RCI) I_{rc} (García-Patrón *et al.*, 2009). In particular, for a bosonic lossy channel with transmittance T , we find $K_D \geq I_c = \log \frac{T}{1-T}$ and the RCI lower bound $K_R \geq I_{rc} = \log \frac{1}{1-T}$ (Pirandola *et al.*, 2009).

Remarkably, these rates can be achieved by specific CV-QKD protocols working in direct and reverse reconciliation, even if they are not implementable in practice since they require infinite two-mode squeezing and a quantum memory (so that Bob can always perform homodyne detection in the correct quadrature). That being said, practical CV-QKD protocols, based on coherent states and the heterodyne detection can reach half of I_{rc} in the ideal asymptotic scenario (Usenko and Filip, 2016).

An optimal CV-QKD protocol does not need to be restricted to one-way classical communication (as in direct and reverse reconciliation) but may exploit more general two-way classical communication and be adaptive, meaning that the classical information exchanged in a round may be used to improve the quantum communication in the next rounds. The optimization over two-way classically-assisted QKD protocols (both CV and DV ones) defines the secret-key capacity of a quantum channel $K \geq \max(K_D, K_R)$.

Following the initial studies on the one-way classically-assisted capacities K_D and K_R (Pirandola *et al.*, 2009), upper bounds were later developed for two-way classically-assisted capacity K , with a preliminary approach based on the squashed entanglement (Takeoka *et al.*, 2014). More recently, (Pirandola *et al.*, 2017) adopted a completely different approach where the key rate of an arbitrary two-way classically-assisted QKD protocol is upper-bounded by the channel's relative entropy of entanglement, suitably simplified via a technique of teleportation simulation.

Using this approach, (Pirandola *et al.*, 2017) showed that $K \leq \log \frac{1}{1-T}$, strictly bounding the rate of any QKD protocol implemented over a bosonic lossy channel with transmittance T , a result known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound. Because the PLOB bound coincides with the RCI lower bound, it exactly establishes the secret-key capacity $K = \log \frac{1}{1-T}$ of the bosonic lossy channel.

The PLOB bound represents the optimal QKD rate over a lossy channel without intermediate repeaters (repeaterless bound). Other versions exist for repeater-assisted communications and quantum networks (Pirandola, 2019), as well as for free-space quantum communications (Pirandola, 2021b).

While the limit of CV-QKD (and all QKD) is clear on a lossy channel, different is the situation for a more general thermal-loss channel, whose structure is discussed in Sec. II.C.3. This is a bosonic channel that is characterized by transmittance T and thermal noise $\bar{n}_N$, the latter being mean number of environmental photons so that $V_N = 2\bar{n}_N + 1$. This noise can equivalently be represented as excess noise, via the formula $\nu = 2T^{-1}(1-T)\bar{n}_N$. In the presence of excess noise, we do not know the formula of the secret-key capacity $K = K(T, \bar{n}_N)$, but we can only write a sandwich $K_{LB} \leq K \leq K_{UB}$ using the bounds from (Pirandola *et al.*, 2009, 2017). The lower bound K_{LB} has been slightly improved using optimized Gaussian-modulated CV-QKD protocols with engineered

loss and thermal noise at the detector setups (Ottaviani *et al.*, 2016) and by the engineering of an entanglement distribution protocol able to provide positive rate where the reverse coherent information is zero (Mele *et al.*, 2025). The discovery of $K(T, \bar{n}_N)$ is a central question in CV-QKD and quantum information theory.

It is evident from the expression of K_D and K_R that, while RR CV-QKD can theoretically provide security for any pure channel attenuation (which is, however, limited by practical finite-size effects and device imperfections), DR protocols are fundamentally limited by $T = 0.5$, hence by 3 dB of channel loss. For the entanglement-in-the-middle protocol and the CV-MDI protocol with detection in the middle of the channel, the optimal key rates correspond to K_D and K_R for DR and RR respectively, up to the subtracted term $1/\ln b$, with b being the information unit, hence base of the logarithms used to calculate the entropic quantities (Lasota *et al.*, 2023). The perfectly implemented entanglement-in-the-middle scheme is therefore limited by the channel transmittance of $T \approx 0.63$ and the symmetrical CV-MDI scheme is limited by $T \approx 0.73$.

As mentioned above, CV-QKD protocols are also limited by channel noise. Even in conditions of a perfectly transmitting channel, $T = 1$, the maximum tolerable channel excess noise ν is limited by about 0.8 SNU (in both DR and RR). Furthermore, it continuously decreases by decreasing the transmittance T (Usenko and Filip, 2016). Two-way protocols make the dependence slower and improve the robustness to channel noise (Pirandola *et al.*, 2008c). For a generic P&M CV-QKD protocol, the maximum tolerable channel noise V_N , as shown in Fig. 6(b), can be approximated through the Lambert W function as $1 + 2e^{1+W_{-1}(-T/e)}$ (Lasota *et al.*, 2017).

C. Practical implementation of CV-QKD

After several theoretical proposals of CV-QKD (Cerf *et al.*, 2001; Grosshans and Grangier, 2002; Hillery, 2000; Ralph, 1999b), the first experimental proof-of-principle test was reported in (Grosshans *et al.*, 2003b) at 780 nm wavelength using Gaussian quadrature modulation (performed as amplitude modulation with an electro-optical Mach-Zehnder interferometer and phase scanning by a piezoelectric transducer), homodyne detection and RR post-processing. The table-top experiment resulted in 1.7 megabits per second (Mbps) secret key rate (secure against individual attacks, considered in the asymptotic limit) in the loss-free channel and 75 Kbps upon 3.1 dB attenuation.

The first practical demonstration of coherent-state CV-QKD was reported in (Lodewyck *et al.*, 2007), where 2 Kbps secret key rate, secure against collective attacks in the asymptotic regime, was obtained in a 25 km long fiber channel (with the loss of 5.2 dB) by the system operating at the telecom wavelength of 1550 nm and employing time multiplexing between co-propagating signal and

LO. The modulation was performed and fine-tuned using automated electro-optical amplitude and phase modulators and an attenuator. The purification-based security analysis was adopted and incorporated detector imperfections. The work revealed the importance of error correction efficiency, which limits the applicable signal modulation and the overall performance of the protocol. The efficiency β obtained using low-density parity-check (LDPC) codes, discussed in Sec. III.E.5, was approx. 0.9.

The field test of coherent-state CV-QKD prototype at the telecom wavelength was reported in (Fossier *et al.*, 2009b) using time and polarization multiplexing for LO propagation and advanced error correction codes with 90% efficiency. The achieved secret key rate, secure against collective attacks in the asymptotic limit, was 8 Kbps (average after 3 days of operation), over an optical fiber with 3 dB loss (corresponding to 15 km distance).

The secure distance of coherent-state CV-QKD was extended to 80 km of optical fiber at the telecom wavelength in (Jouguet *et al.*, 2013b) using error correcting codes with efficiency of 95%. The achieved key rates ranged from 10 Kbps in the 25 km channel, few Kbps over 53 km and around 200 bps over 80 km channel, with security analyzed against collective attacks in the finite-size regime.

By controlling the noise of the setup (using high-sensitive homodyne detectors tolerating co-propagated LO attenuation, and high-precision phase compensation), the performance of coherent-state CV-QKD was improved to approx 0.5 Kbps secret key rate (secure against collective attacks in the finite-size regime of 10^{10} block size enabled by highly stable setup) over 100 km long fiber (Huang *et al.*, 2016), with error correction efficiency of 95.6%. Over the shorter distance of 25 km the secret key rate of 1 Mbps was achieved using high-speed (1 GHz) homodyne detection and 50 MHz clock rate (Huang *et al.*, 2015c).

The record-breaking distance of over 200 km in ultra low-loss fiber, reaching a secret key rate of about 6 bps, was reported for coherent-state CV-QKD in (Zhang *et al.*, 2020) using a highly stable setup and error correcting codes with 98% efficiency.

Composable security against collective attacks for the practical long-distance coherent-state CV-QKD was demonstrated in (Jain *et al.*, 2022) over 20 km fiber using phase compensation enforced by machine learning techniques, which enabled the secret key rate of 4.7 Mbps.

High-speed Gaussian modulated coherent-state “local” local oscillator (LLO) CV-QKD, as described in Sec. III.C, was demonstrated in (Huang *et al.*, 2015a), reaching about 100 Kbps over 25 km link with 97% error correction efficiency, while a long-distance implementation of the LLO protocol was reported in (Hajomer *et al.*, 2024c), reaching 25.4 Kbps over 100 km telecom fiber, both implementations with the finite-size collective-attack security.

Coherent-state DM CV-QKD was implemented

in (Tian *et al.*, 2023) using 16-state constellations, reaching 49.02 Mbps and 2.11 Mbps of asymptotic collective-attack secret key rates over 25 km and 80 km optical fibers, respectively, corresponding to 67.4% and 66.5% of the Gaussian CV-QKD key rates in the same channels. A high-speed implementation operating at 10 GHz using 16, 32 and 64 coherent state constellations was reported in (Hajomer *et al.*, 2024b) over 5 and 10 km reaching about 900 and 500 Mbps. The experiment in (Roumestan *et al.*, 2024) reported secret key rates of 92 and 24 Mbps over 10 and 25 km, respectively, using a probabilistically shaped 64-QAM modulation, based on the security proof of (Denys *et al.*, 2021) and a worst-case finite-size security analysis. Composable security for collective attacks was achieved using a QPSK constellation over a 20 km fiber channel (Hajomer *et al.*, 2025b) and a 3 dB free-space channel which was simulated in the lab (Jaksch *et al.*, 2024).

CV-MDI-QKD was tested in (Pirandola *et al.*, 2015b) with 0.1 Kb of asymptotic secret key per relay use obtained at 4 dB loss. Another test of the MDI protocol was reported in (Tian *et al.*, 2022), reaching 0.43 and 0.19 bits per symbol over 5 and 10 km fiber links, respectively. An experimental implementation operating at 20 MHz achieving a secure key rate of 2.6 Mbps over a 10 km fiber link operating in the finite-size regime against collective attacks was demonstrated in (Hajomer *et al.*, 2025a).

Entanglement-based protocols remain on the level of proof-of-principle tests with a full-scale implementation yet to be performed. Entanglement-based CV-QKD was first tested in (Su *et al.*, 2009), reporting 83 and 3 Kbps of key, secure against asymptotic collective attacks, upon 80% and 40% transmittance respectively. Modulation was reported to improve EB CV-QKD over noisy channels, tested in (Madsen *et al.*, 2012), reaching $4 \cdot 10^{-3}$ bits per symbol in a highly noisy channel (where the coherent-state protocol would fail). Entanglement-based protocol with composable and one-sided-device independent security was tested in (Gehring *et al.*, 2015), reaching 0.1 bits per symbol at 0.76 dB of channel attenuation (corresponding to 2.7 km telecom fibre).

Many more experimental tests and implementations were reported in addition to the above mentioned milestones. It is often hard to compare different realizations because of the unmatched security assumptions (types of attacks, finite-size vs asymptotic analysis). Practical CV-QKD is still in the process of development toward higher key rates for the full-scale implementations in the most general security scenarios and over long-distance channels. In the next subsections we discuss the main state-of-the-art techniques and methods used in the practical realizations of CV-QKD.

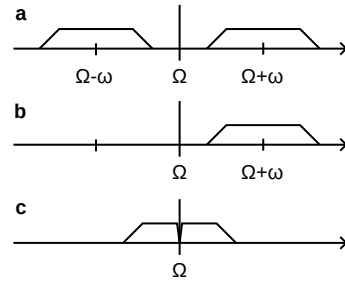


FIG. 7 Different possibilities for physical realizations of coherent state modulation based on the displacement of vacuum states. The angular frequency of the laser is Ω , the center modulation sideband angular frequency is ω .

1. Quadrature modulation

The quantum states on which a CV-QKD protocol realization is based have certain physical properties. Among those are the wavelength or light frequency, temporal shape and polarization. The physical properties define the mode in which the coherent or squeezed states reside, and which has to be measured by the detector for optimal performance. Several different physical realizations have been investigated.

The basis of all implementations is light produced by a laser at a certain carrier angular frequency Ω and described by its electric field $E \exp(i\Omega t)$, where E is the electric field amplitude and t is time. To implement the random quadrature displacement in P&M coherent-state or squeezed-state protocols quadrature modulation is used. For this purpose the light is passed through an electro-optic modulator modulating the phase or amplitude of the light by changing the refractive index through an applied electric field.

An often used implementation is based on a pulsed laser which at a typical repetition rate in the MHz range emits hundreds of ns long pulses of light (Jouguet *et al.*, 2013b; Zhang *et al.*, 2020), or laser pulses that are carved into a continuous-wave (CW) laser beam using a high-extinction intensity modulator which achieves higher repetition rates of currently up to 250 MHz (Laudenbach *et al.*, 2019). After optical attenuation to on average a couple of photons per pulse, the pulses are in a coherent state whose amplitude is randomly changed with an amplitude modulator, and moved to all four quadrants of the phase space by a phase modulator which has to be driven up to its half-wave voltage.

In other implementations, the vacuum state at a sideband frequency of the carrier is displaced instead of using the carrier itself (Jain *et al.*, 2022; Kleis *et al.*, 2017; Pirandola *et al.*, 2015b). Those implementations use CW lasers and the temporal shape of the coherent states is defined by the electrical waveform driving the modulators. Since a vacuum state and not an excited coherent state is displaced, smaller driving voltages can be used and the modulator is operated in its linear regime. Generally, three different sideband modulation techniques have

been explored which are sketched in Fig. 7 and outlined below.

Amplitude and phase modulation generates two frequency sidebands symmetric around the laser's carrier frequency. The rate at which the complex amplitude of the coherent states is changed is directly reflected into how much bandwidth is occupied in the Fourier domain with the roll-off given by the lowpass filter defining the temporal shape. The first modulation technique, shown in Fig. 7(a) uses up-conversion of the modulation to an intermediate carrier frequency ω , such that the electric field is $E(t) \propto \alpha(t) \exp(i(\Omega + \omega)t) + \alpha^*(t) \exp(i(\Omega - \omega)t)$ with $\alpha(t)$ describing the coherent state amplitude. The receiver has to measure both sidebands, which is possible with homodyne and intradyne detection, see below. To avoid having to measure both sidebands and to enable radio-frequency heterodyne detection, one of the sidebands can be suppressed, leading to single-sideband modulation as shown in Fig. 7(b). This can be achieved by appropriate modulation using an IQ modulator, which removes one of the sidebands by optical interference (Jain *et al.*, 2021; Kleis *et al.*, 2017). The resulting electric field is given by $E(t) \approx \frac{\mu}{2} \alpha(t) \exp(i(\Omega + \omega)t) + \frac{\delta}{2} \alpha^*(t) \exp(i(\Omega - \omega)t)$ with μ being the modulation index and $\delta < \mu$ the effective modulation index taking the sideband suppression ratio into account. While the suppressed sidebands usually have around 30 dB lower power than the desired sidebands, their existence leads to a potential side channel that has to be appropriately taken into account in the security analysis (Jain *et al.*, 2021). Using baseband modulation instead, which is shown in Fig. 7(c), can avoid this side channel (Hajomer *et al.*, 2022b). Here, the up-conversion of the modulation is removed, i.e. $\omega = 0$. However, to avoid the strong carrier and the laser noise close to the carrier, a highpass filter has to be introduced. This highpass filter has to be optimized to reduce correlations between quantum states to the largest possible extent (Hajomer *et al.*, 2022b). An advantage of this modulation scheme is that it is the most transmitter bandwidth efficient, important for CV-QKD at high speed (Hajomer *et al.*, 2024b).

Besides the coherent states for the CV-QKD protocol, auxiliary signals have been generated that are time or frequency multiplexed. Those usually aid DSP procedures in the receiver, for instance, for phase recovery and clock synchronization (Chin *et al.*, 2022). Typical signals are pilot tones and signals of higher power than the quantum states using, for instance, QPSK modulation formats.

2. Coherent detection

At the receiver, the quantum states are typically measured with quadrature detectors which can be divided into two types: receivers measuring one quadrature at a time, i.e. homodyne detection, and receivers measuring both the amplitude and phase quadratures simultaneously, often called heterodyne detection in the quantum

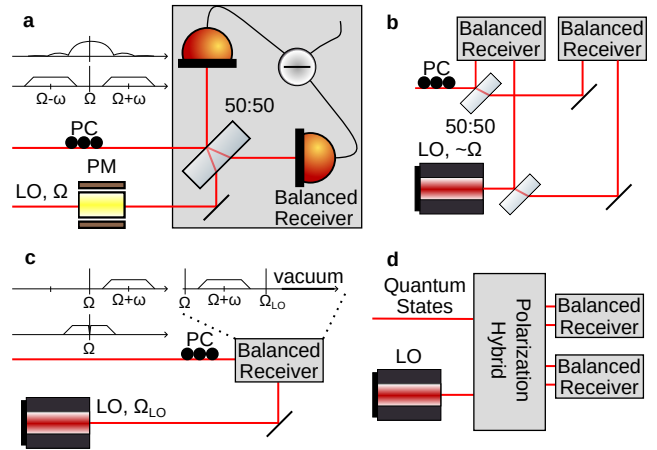


FIG. 8 CV-QKD receiver schemes. a) Homodyne receiver, b) Heterodyne (phase-diverse) receiver, c) RF heterodyne receiver, d) Polarization diverse RF heterodyne receiver. LO: Local Oscillator, PM: Phase Modulator, PC: Polarization Controller.

optics community.

In a homodyne receiver the LO beam is interfered with the quantum states at a balanced beam splitter whose outputs are detected by pin-photodiodes as shown in Fig. 8(a). Having the same frequency as the carrier of the coherent states, the phase of the LO determines the measured quadrature. To follow the protocol, the measured quadrature has to be chosen randomly for each received quantum state which can be implemented most practically when pulsed lasers or pulse-carved laser beams are used. Nevertheless, the switching speed is limited and therefore it has only been implemented with state repetition rates up to 5 MHz (Zhang *et al.*, 2020). To achieve a stable phase relation the LO is usually derived from the transmitter and sent to the receiver through a fiber. Recently, remote homodyne detection of a squeezed state has been achieved with a separate laser for the LO using an optical phase-locked loop (Suleiman *et al.*, 2022).

Heterodyne detection avoids active basis choice. A common implementation is to split the quantum states at a balanced beam splitter and to detect its outputs with two homodyne detectors measuring orthogonal quadratures. This is shown in Fig. 8(b). The orthogonality of the measured quadratures can automatically be ensured by using 90° optical hybrids which utilize polarization optics to turn the phase of the LO in one arm by 90° with respect to the other. The introduction of optical hybrids into CV-QKD systems has enabled the development of LLO schemes (Huang *et al.*, 2015b; Qi *et al.*, 2015; Soh *et al.*, 2015), aimed at removing the attacks on the LO, as described in Sec. III.C. For those, the LO is derived from a laser located at the receiver, which is independent of the laser used at the transmitter. The frequency of the LO laser can be tuned close to that of the transmitter laser which yields a phase drift proportional to the frequency difference, corrupted by phase noise of

the lasers. The phase drift and noise have to be measured and can be compensated in post-processing by applying simple rotations in the phase space spanned by the measured orthogonal quadratures. The detection scheme is called intradyne detection and works well for frequency differences of the lasers lower than half the bandwidth of the quantum states. It can be implemented for both the modulation schemes based on displacing coherent states and baseband modulation, i.e. the displacement of vacuum states.

A second implementation approach to heterodyne detection is known as radio-frequency (RF) heterodyne detection, depicted in Fig. 8(c). Here, the LO is detuned from the frequency band occupied by the quantum states. Since a detuned LO also interferes with the image band to the frequency band occupied by the quantum states, a simple balanced receiver setup with one detector is sufficient to measure both quadratures simultaneously. As a single balanced detector is enough, an advantage in comparison to an optical hybrid is that the splitting ratio of the quantum states is exactly 50:50 and that the quantum efficiency is the same for both quadratures. RF heterodyne detection is best used with single-sideband or baseband modulation schemes.

Another dimension is polarization. For balanced reception to work efficiently the polarization of the LO and the quantum states have to match. Most often this is achieved by polarization controllers optimizing the polarization of the quantum states after transmission through the channel as shown in Fig. 8. Lately, also polarization hybrids have been introduced, splitting the polarization into two components as depicted in Fig. 8(d) (Chin *et al.*, 2024; Pereira *et al.*, 2023a). Those are then measured independently and combined using digital signal processing (DSP), as discussed in the next subsection.

3. Digital signal processing

With the introduction of LLO schemes and the use of some form of heterodyne detection, DSP has become of more and more importance to experimental implementations as it allows to compensate impairments digitally instead of doing it in the analog domain. Some of those impairments DSP deals with are phase noise, polarization mismatch, and clock desynchronization. DSP is also sometimes used to achieve mode matching between the received and the transmitted quantum states.

One of the most challenging tasks is carrier frequency and phase recovery, compensating for phase noise originating from the free-running transmitter and receiver lasers, and – to a lesser extent – from the channel. Phase noise from the lasers is generally the largest source of excess noise in experimental implementations (Hajomer *et al.*, 2024c), in particular when compared to implementations using transmitted LO (Zhang *et al.*, 2020). To achieve phase matching, the phase of the quantum signal with respect to the LO has to be measured, estimated,

and compensated for. For this purpose, usually either frequency (and sometimes polarization) multiplexed pilot tones or time multiplexed reference symbols of higher power are used. In the case of pilot tones, the measured signal can be described by

$$A \sin(i\Omega_{\text{LO-Pilot-Beat}}(t)t + \phi(t)) + X_{\text{meas}}(t),$$

where $\Omega_{\text{LO-Pilot-Beat}}(t)$ is the time varying beat frequency of the pilot tone with the LO, $\phi(t)$ is the phase noise, t is time and $(A/\sqrt{2})^2/\text{Var}(X_{\text{meas}})$ is the SNR given by the pilot tone power $A^2/2$ and the power of the quadrature noise, $\text{Var}(X_{\text{meas}})$, induced by the measurement (often shot noise and electronic noise). After the measurement, the phase $\phi(t)$ has to be estimated from the measurements. This can be conveniently achieved by taking either the arctangent of the two measured quadrature components (phase-diverse reception) or the measured signal and its Hilbert transform (RF heterodyne reception). However, while computationally inexpensive, this estimation method is not statistically optimal. Statistically optimal are methods based on Bayesian inference (Särkkä, 2013). Kalman filters produce estimates of unknown time varying variables in the presence of noise. Their extended and unscented versions can deal with the nonlinearity of the measurement equation with respect to phase and have shown exceptional performance down to much lower SNRs than the arctangent-method (Chin *et al.*, 2021; Kleis and Schaeffer, 2019; Su *et al.*, 2019). The required prior model in Bayesian inference is usually taken from a Wiener model of phase noise whose linewidth parameters are learned from the data. Alternative approaches have used neural networks for phase estimation (Long *et al.*, 2023; Xing *et al.*, 2022).

Since eventually the SNR of the pilot tone or reference symbols is the figure of merit to achieve high quality phase estimation, some experiments have used polarization multiplexing to accommodate higher power pilot tones and low power quantum states (Laudenbach *et al.*, 2019). A recent study showed that 10 kHz linewidth lasers can be used with SNRs above 28 dB, however higher linewidth lasers require higher SNR which are experimentally challenging to achieve without impacting the linearity of the receivers.

In transmitted LO implementations, clock synchronization can simply be achieved by measuring a fraction of the LO pulse (Jouguet and Kunz-Jacques, 2014). Modern DSP-based systems often use oversampling by an asynchronous analog-to-digital converter and a timing error detector based on one or more auxiliary signals of known frequency difference to determine the correct sampling points (Chin *et al.*, 2022; Kleis *et al.*, 2017; Wang *et al.*, 2022).

DSP has also been used to compensate for imperfect modulator (Hajomer *et al.*, 2024b) or receiver characteristics (Jain *et al.*, 2022). Machine learning techniques such as neural network based auto-encoders have also been used to compensate for nonlinear distortions (Long *et al.*, 2023; Zhang *et al.*, 2022). It has also been the fo-

cus of an open-source modular software platform benchmarked on multiple CV-QKD configurations and developed to stimulate further explorations (Piétri *et al.*, 2024a).

Indeed, although the exploration of DSP for CV-QKD is still at its early stages, it represents a promising path toward simpler photonic circuits with lower-quality components, which are crucial for the envisioned cost reduction of QKD systems.

4. Squeezed signal states

A few proof-of-concept implementations of QKD based on squeezed states have been demonstrated to date. These schemes, detailed in Section III.A, introduce promising advancements for CV-QKD, including a modulation-free approach (Su *et al.*, 2009), extended operational range (Madsen *et al.*, 2012), enabling composable security (Gehring *et al.*, 2015), one-sided device independence (Walk *et al.*, 2016) and the elimination of information leakage to eavesdroppers (Jacobsen *et al.*, 2018), which reduces post-processing requirements. In the following paragraphs, we delve into the experimental tools used in these implementations and highlight their key findings.

Parametric down-conversion (PDC) has been the dominant method for generating squeezed light (Andersen *et al.*, 2016) since its first demonstration in (Wu *et al.*, 1986), where noise suppression of 3.5 dB beyond the shot noise limit was achieved. Since that time, squeezed light of up to 15 dB noise suppression has been realized using the PDC process (Vahlbruch *et al.*, 2016). In PDC, a pump wave with frequency ω_p interacts with a χ^2 -nonlinear medium to produce two quantum-correlated (entangled) waves, known as the signal and idler (Boyd, 2020). When these waves are degenerate across all degrees of freedom – spatial, polarization, frequency, and temporal mode – their entanglement translates into quadrature squeezing of the resulting single mode. Efficient squeezing generation relies on several key conditions: high power density in the crystal, which can be achieved using pulsed lasers, placing the crystal in a cavity, or employing an optical waveguide; and precise phase matching of the parametric process, achieved through methods such as temperature tuning of the crystal, adjusting the pump wavelength, or periodically poling the crystal. As of today, the most effective strategy for generating quadrature squeezed light is to use a CW pump beam and integrate a periodically poled crystal (e.g. potassium titanyl phosphate, KTP, or LiNbO₃) inside a low-loss cavity that is resonant at the signal-idler wavelength (and potentially also at the pump wavelength). This method has been employed in all existing demonstrations of squeezed-light-based CV-QKD.

While many other methods exist for generating squeezed light (Andersen *et al.*, 2016), it is crucial to select a process that produces squeezed light suitable

for QKD. For fiber-based QKD, the wavelength of the squeezed light should fall within the telecom band to minimize fiber transmission losses. For free-space QKD, suitable wavelengths are 800 nm-850 nm, 1064 nm and 1550 nm, where atmospheric attenuation is relatively low depending on the weather and where laser sources are commonly available. For example, a KTP crystal-based PDC process can generate squeezed light at all these wavelengths, whereas atomic-based squeezed light sources are often limited to specific atomic transition wavelengths, such as Cesium at 852 nm and Rubidium at 795 nm. Another advantage of the PDC process is its bandwidth, ideally constrained only by the frequency band where phase matching occurs, which can extend into the Terahertz range. However, as noted, the bandwidth of the PDC process is often limited by the cavity used to enhance it, narrowing it to the cavity's linewidth – often still considerable (several GHz). Another important factor is the temporal mode of the squeezed state. To improve the efficiency of homodyne detection and to mitigate issues with dispersion, it is beneficial to produce the squeezed state in a CW or quasi-CW mode. CW operation also provides considerable flexibility in digitally defining the temporal mode via DSP. This preference for CW operation makes the cavity-enhanced PDC process the most obvious choice, although recent reports on CW squeezed light produced in a waveguide are also encouraging (Kashiwazaki *et al.*, 2023).

In all experiments on CV EB QKD conducted to date, squeezed light was generated using cavity-enhanced PDC with periodically poled KTP crystals housed in high-quality linear optical cavities. In few experiments (Su *et al.*, 2009; Wang *et al.*, 2018), the CV entanglement – also known as two-mode squeezed (TMSV) states – was directly produced by operating the PDC process in a non-degenerate mode, whereas in the other experiments (Gehring *et al.*, 2015; Madsen *et al.*, 2012; Walk *et al.*, 2016), entanglement was achieved by combining two single-mode squeezed states at a balanced beam splitter. In each setup, one mode of the two-mode squeezed state was measured with high-efficiency homodyne detection at the transmitting station, while the other mode was transmitted through free space to the receiving station, where homodyne or heterodyne measurements were performed. The transmitter's measurements influenced the state observed at Bob's station, resulting in a Gaussian distribution of amplitude or phase quadrature squeezed states, effectively simulating a single-mode P&M squeezed state protocol. The noise suppression achieved below the shot noise level was measured at 3.0 dB at 1080 nm (Su *et al.*, 2009), 3.5 dB at 1064 nm (Madsen *et al.*, 2012), and 10.5 dB at 1550 nm (Gehring *et al.*, 2015). Although the theoretical clock rate in these experiments could approach the bandwidths of the cavity-enhanced parametric amplifiers (20 MHz, 21 MHz and 63 MHz, respectively), the effective operational bandwidth was restricted to a few kHz

by electronic filtering in post-processing.

QKD schemes based on two-mode squeezed states do not require electro-optical modulators to define the alphabet. As described above, the result of a quadrature measurement on one mode of a two-mode squeezed state directly produces a Gaussian alphabet of squeezed states, eliminating the need for physical electro-optical modulators. In this approach, the modulation arises naturally from the intrinsic quantum randomness of measuring the two-mode squeezed state, meaning that the randomness used for key generation is inherent to the measurement process itself rather than relying on an external quantum random number generator. The preparation basis choice is then performed by measurement on one of the modes of an EPR state (Silberhorn *et al.*, 2002a). A proof-of-concept for such a modulation-free scheme was first demonstrated by Su *et al.* (Su *et al.*, 2009), where an early-stage security analysis showed secret key rates of 84 kbits/s and 3 kbits/s for transmission efficiencies of 80% and 40%, respectively, under the assumption of Gaussian collective attacks.

In systems using squeezed states, the alphabet size is typically constrained by the degree of anti-squeezing, limiting the potential to maximize the key rate based on modulation depth. However, (Madsen *et al.*, 2012) demonstrated that expanding the Gaussian alphabet through conventional amplitude and phase modulation at Alice's station enhances the system's resilience to excess noise, allowing for secure communications over greater distances. This protocol can be equivalently realized using the EB scheme, which leaves Alice with two sets of data: the homodyne measurement results, X_{HD} , and the Gaussian modulation values, X_M . To optimize the protocol's resilience to excess noise, these two sets of data were combined with an optimal weighting, $X_M + gX_{HD}$, where the factor g depends on the strength and purity of the squeezed states. For large, pure squeezing, the two data sets should be equally weighted, $g = 1$, whereas for lower squeezing, a greater weight should be assigned to the modulation data, with $g \rightarrow 0$ as the squeezing vanishes and the protocol changes to the coherent-state one. Using such a weighting strategy, the squeezed state scheme outperforms the coherent state scheme for all levels of squeezing. In (Madsen *et al.*, 2012), two-mode squeezed states with 3.5 dB of noise suppression and 8.2 dB of anti-squeezing were produced, with coherent modulation levels varied from 0 dB to 15 dB. Specifically, with a modulation of 23.4 SNU, channel transmission of 95%, and a channel excess noise of 0.45 SNU, a key rate of 0.004 bit per state was achieved in the asymptotic limit under collective attacks (and perfect post-processing $\beta = 1$). Notably, neither a coherent-state protocol nor a non-modulated squeezed-state protocol could generate a key under these conditions. Additionally, they identified the tolerable levels of excess noise for secure key generation in a 10% transmissive channel across various modulation strengths, and found that modulated squeezed-light realizations consistently out-

performed the coherent-state protocol under all tested conditions. Although these experimental tests assumed ideal post-processing efficiency, (Madsen *et al.*, 2012) also demonstrated that the squeezed-state protocol is inherently more robust than the coherent-state protocol in the presence of post-processing inefficiencies.

In these initial demonstrations of EB CV-QKD, the security proofs typically addressed only collective attacks and did not guarantee composability against coherent attacks. However, (Gehring *et al.*, 2015) reported the first implementation of a CV-QKD protocol that achieves composable security against coherent attacks while being 1sDI. Using highly squeezed EPR-entangled states, they achieved a composable secure key generation rate of 0.1 bit per sample for a channel loss of 0.76 dB (equivalent to 2.7 km of fiber) and a reconciliation efficiency of 94.3%. The experiment demonstrated robustness against intensity fluctuation attacks on the LO and Trojan-horse attacks, with the EPR source located at Alice's station ensuring security even when Bob's devices were untrusted. Building on this work, (Walk *et al.*, 2016) extended the scope of CV-1sDI-QKD by implementing a range of Gaussian protocols, including both P&M and EB schemes using TMSV states. In their experiment with TMSV states (operating at 1064 nm), they demonstrated secure key generation over distances of up to 7.5 km of effective optical fiber transmission using reverse reconciliation, highlighting the practicality of 1sDI-QKD with current technology.

While most squeezing-based QKD implementations leverage two-mode squeezed states, as discussed above, there have also been successful demonstrations utilizing single-mode squeezed states. These approaches reduce experimental complexity by simplifying the optical setup while maintaining compatibility with QKD protocols. One such implementation by (Eberle *et al.*, 2013) employed a single-mode squeezed state of 11.1 dB quantum noise suppression at 1550 nm to generate asymmetric entanglement by interfering the squeezed state with vacuum on a balanced beam splitter. This setup established quantum correlations between one pair of quadratures (e.g., the amplitude quadrature for an amplitude-squeezed state) while the conjugate quadratures (e.g., phase) remained uncorrelated. Despite this asymmetry, the source was proven suitable for QKD with composable security, supporting secure key distribution over distances of up to 10 km.

Another notable experiment (Jacobsen *et al.*, 2018), used single-mode squeezed states to encode information into displacements along a single quadrature, creating a unidimensional Gaussian alphabet (Usenko and Grosshans, 2015). For instance, an amplitude-squeezed state was solely displaced in the amplitude quadrature direction using an amplitude modulator. By aligning the displacement with the squeezed quadrature, this approach achieved a significant security advantage. Specifically, it was demonstrated that for a purely lossy transmission channel, an eavesdropper's information can be

completely eliminated when the variance of the squeezed alphabet matches the variance of the vacuum state. In the experiment, a 3dB squeezed state at 1064nm was displaced with an amplitude modulator with varying modulation depths. It was observed that for a specific modulation depth, where the alphabet size coincided with the width of the vacuum noise, Eve's Holevo information dropped to exactly zero. This effect was tested across four different transmission coefficients of a simulated lossy channel (using a variable beam splitter), and in all cases, complete elimination of the Holevo information was achieved. This suppression of eavesdropper information arises because the amplitude quadrature correlations between Eve and Bob vanish entirely when the variance of the alphabet equals the variance of the vacuum state (corresponding to the noise floor assumed in Eve's beam splitter attack). By eliminating Eve's ability to gain information, this protocol not only ensures security but also significantly reduces the computational complexity of post-processing, making it an attractive option for future CV-QKD systems, particularly in scenarios where low computational overhead are critical.

All the above-mentioned proof-of-concept experiments with squeezed light employed a LO derived from the same laser used to generate the squeezed light. This approach simplifies the experimental setup due to the inherent frequency matching and phase stability between the squeezed light and the LO. However, in practical QKD scenarios, transmitting the LO alongside the quantum signal poses significant challenges. Transmitting high-power LOs over long distances not only creates issues with nonlinear induced mode distortion and light scattering but also opens the door to eavesdropping strategies that exploit the transmitted LO to compromise the coherent detection at the trusted receiver. To address these vulnerabilities, it is preferable to generate the LO locally at the receiving nodes. Generating the LO locally introduces its own challenges, particularly the need for real-time control of the phase difference between the signal and the LO. Without frequency locking between the two independent lasers, maintaining stable phase coherence can be difficult. In (Suleiman *et al.*, 2022), the authors reported on the generation, transmission, and homodyne detection of single-mode squeezed states of light at 1550 nm using a locally generated LO with real-time phase control. By implementing a real-time feedback system, they achieved precise control over the frequency and phase of the LO. This enabled homodyne detection of a squeezed state with a phase uncertainty of only 2.51° , even after the squeezed state had propagated through up to 40 km of telecom fiber. This demonstration represents a crucial step toward practical implementations of squeezed-light-based CV-QKD. By overcoming the challenges of locally generated LOs and maintaining stable phase control, this work lays the foundation for future QKD schemes that combine the security advantages of squeezed light with realistic deployment in telecom networks.

5. Measurement-device independent protocols

CV-MDI-QKD eliminates all side-channel attacks on detectors by performing a CV Bell measurement at an untrusted relay. While this feature provides strong security, the protocol's practical implementation is more complex compared to one-way CV-QKD, leading to relatively few experimental demonstrations despite significant theoretical progress. Below is a review of recent advancements in CV-MDI-QKD implementation.

The first proof-of-concept experiment, conducted in 2015 (Pirandola *et al.*, 2015b), used a free-space optical setup with a shared 1064 nm CW laser modulated to prepare coherent states. Phase locking between Alice's and Bob's signals was achieved using piezoelectric transducers, while the CV Bell measurement was performed with a balanced beam splitter and homodyne detectors. Although this experiment demonstrated the feasibility of CV-MDI-QKD, it lacked critical practical features, such as telecom-compatible wavelengths, independent lasers, and real fiber channels, limiting its applicability for in-field deployment.

To address these limitations, a more practical CV-MDI-QKD implementation was reported in 2022 (Tian *et al.*, 2022). This system employed a 10 km standard single-mode fiber channel and independent lasers operating at the telecom wavelength of 1550 nm. Frequency locking was achieved via phase-locked loops, and phase drift was compensated using a combination of pilot and phase-reference pulses. While the system achieved a low excess noise of 0.0045 SNU and a secret key rate of 0.19 bits per relay use, it remained complex due to the need for heterodyne receivers for phase locking, additional modulators for pulse carving, and polarization and time multiplexing.

A significant step toward simplifying CV-MDI-QKD was achieved with a system design based on DSP (Hajomer *et al.*, 2022a). This design eliminated the need for phase locking by sharing a single laser source and replaced traditional pulse carving with digital pulse shaping using root-raised cosine filters. These innovations enabled a tenfold increase in the symbol rate, reaching 5 MBaud. Furthermore, the CV Bell measurement was implemented with a simplified relay structure based on a polarization-based 90-degree hybrid. These advancements resulted in a key rate of 0.12 bits per relay use over a 2 dB channel loss. However, further work is required to integrate clock synchronization and adapt the system for deployment over fiber channels.

Recent advancements have focused on practical integration and achieving higher key rates. A notable system design (Hajomer *et al.*, 2025a) addressed challenges such as clock synchronization and coexistence with classical communication channels. By colocating the relay at Alice's station and using a digital signal processing module for quantum state preparation, the system achieved CV Bell measurement at 20 MBaud. Synchronization was achieved with a 1310 nm optical clock co-

propagating with the quantum signal, complemented by real-time phase locking. This setup demonstrated a secure key rate of 2.6 Mbit/s against collective attacks in the finite-size regime over a 10 km fiber link. Despite these advancements, further improvements are needed, particularly in the post-processing phase.

6. Fiber and free-space channels

Most of the tests and realizations of CV-QKD were performed over fiber channels, which is main type of links for optical communications due to high and stable transmittance at the telecom wavelengths (typically 1550 nm), low noise, especially in single-mode fibers, if free from other optical signals, and availability due to the existing telecom infrastructure. A fiber channel is characterized by transmittance T and is modeled by a respective beam splitter, which couples the quantum signal to a vacuum mode. The telecom fibers, usually made of silica, nominally have a transmittance of -0.2 dB per kilometer (which can be also referred to as 0.2 dB of channel loss), but deployed fiber commonly has higher loss due to splices and connectors. Ultra low-loss telecom fibers with transmittance of -0.15-0.16 dB/km are also available and were used in laboratory experiments to demonstrate long-distance CV-QKD (Hajomer *et al.*, 2024c; Zhang *et al.*, 2022). Fiber attenuation is mainly caused by scattering and absorption and dominantly contributes to the signal loss. In any practical implementation, the channel transmittance has to be precisely estimated and controlled, and should be clearly distinguished from the losses in the trusted devices.

Typical noise sources introduced by fiber channels are phase and polarization fluctuations which have to be suppressed by the QKD system (Laudenbach *et al.*, 2018; Liu *et al.*, 2020b). The excess noise created by phase fluctuations not only depends on the amount of residual phase noise after phase compensation, but also on the modulation variance (Marie and Alléaume, 2017). Therefore the QKD system not only has to excel in phase compensation, but also has to optimize the modulation variance to achieve best performance (Hajomer *et al.*, 2024c). The amount of polarization fluctuations stemming from the fiber channel depends on whether a fiber is on a spool in a laboratory, deployed underground or is aerial (Jain *et al.*, 2024). Noise also arises when the quantum states coexist in a fiber with classical telecom signals through wavelength division multiplexing (Eriksson *et al.*, 2019a), especially through Raman scattering. However, also amplified spontaneous emission from the lasers used for high-rate data transmission creates noise, which can be suppressed with optical filters before the light is multiplexed with the quantum states. The precise estimation of channel noise is crucial for system performance and imperfect estimation in the finite-size regime implies pessimistic assumptions on the noise levels. Similarly to the channel transmittance, the noise has not only to be

carefully characterized but also distinguished from the noise in the trusted devices.

The situation is different in free-space atmospheric channels, where turbulence effects and background light drastically affect optical quantum communication. CV-QKD, however, can be particularly robust against background light, because the narrow-band LO acts as a filter so that the homodyne detector does not register light, not matching the LO wavelength. This makes CV-QKD particularly promising for day-light operations, where DV protocols would need additional filtering, which introduces extra loss to the overall optical budget of the link. Free-space implementations define the suitable wavelengths of 800 nm-850 nm, 1064 nm and 1550 nm, on which the optical signals are better transmitted through the atmosphere. Atmospheric turbulence however complicates things for CV-QKD, leading to effective transmittance fluctuations, also referred to as channel fading. Fading is mostly caused by the beam deformation and wander effect, which dominate the channels with weak turbulence, where transmittance fluctuations are well described by the log-negative Weibull distribution, and additional broadening and deformation of the beam in the strong turbulence with smooth transmittance probability distributions (Vasylyev *et al.*, 2016). Fading channels are non-Gaussian (Dong *et al.*, 2010) and result in the fading-related channel excess noise $\nu_f = \text{Var}(\sqrt{T})(V_S + V_M - 1)$, governed by the variance of the coupling to vacuum (square root of transmittance) $\text{Var}(\sqrt{T})$ and signal and modulation variances in the given quadrature V_S and V_M respectively (Usenko *et al.*, 2012). Such noise has to be assumed untrusted, as the transmittance fluctuations can be controlled by Eve, limiting applicability of CV-QKD over fading channels, and requiring additional optimization of the signal and modulation. It was shown that signal squeezing can be helpful in fading channels, but has to be optimized due the fading-related noise in the anti-squeezed quadrature, where the variance of the signal is largely above shot noise (Derkach *et al.*, 2020).

The negative impact of transmittance fluctuations in CV-QKD can be partially compensated using adaptive optics e.g. by beam expansion (Usenko *et al.*, 2018) or wavefront correction (Chai *et al.*, 2020; Marulanda Acosta *et al.*, 2024). Alternatively, the transmittance distribution can be optimally divided into clusters, where the variance of the fluctuations is lower, and QKD security can be analyzed for those clusters separately, which increases the overall secret key rate (Ruppert *et al.*, 2019). This technique is promising for realizations of CV-QKD over satellite channels using coherent (Dequal *et al.*, 2021) and squeezed states (Derkach and Usenko, 2020). Comprehensive analysis of free-space CV-QKD in the composable finite-size security framework was performed in (Pirandola, 2021b), establishing the bounds on free-space CV-QKD and showing that coherent-state protocol can perform close to those bounds. Composable finite-size security of no-switching protocol in free-space channels was also studied in (Hosseinidehaj *et al.*, 2021),

confirming the advantage of channel clusterization.

CV-QKD was tested in free-space atmospheric channels using single-quadrature encoding with 0.152 Kbps secret key rate, secure against collective attacks in the asymptotic limit, reported over a 460 m channel (Shen *et al.*, 2019).

D. Implementation security

Practical implementation of QKD is never ideal due to device imperfections, which have to be taken into account in the security analysis. Usually, practical imperfections are distinguished between normal device operation in accordance with their specification, such as finite detection efficiency and electronic noise of the detectors, which can be observed by the trusted parties and directly accounted for, and undocumented features or their combinations, which can lead to security loopholes, when the trusted parties are not even aware of the possible information leakage, the famous example being detector blinding in DV-QKD (Lydersen *et al.*, 2010). Therefore, the practical security of QKD relies on the best existing knowledge of the setup and its components and requires a thorough investigation of the component specification as well as their study aimed at finding possible quantum exploits. We start the review of the practical security of CV-QKD with a description of the major known device imperfections, that directly affect the performance of the protocols. We will base our discussion on the Gaussian protocols in the collective attacks scenario assuming asymptotic data sizes, which can be directly extended to finite-size Gaussian collective attack analysis for all Gaussian protocols following the techniques from (Leverrier *et al.*, 2010) and to composable security against Gaussian collective and general attacks using the proof (Leverrier, 2015) and the Gaussian de Finetti reduction (Leverrier, 2017) for the no-switching protocol. This most general CV-QKD security in the case of the major practical imperfections was recently analyzed in (Pirandola, 2021a). The comprehensive analysis of practical imperfections in the DM CV-QKD security is yet to be performed, therefore we limit our review to Gaussian protocols.

Before we go into details of the practical security of CV-QKD it is important to introduce the *trust assumption*. The trusted parties decide which parts of the setup they assume to be out of control of an eavesdropper, refer to these parts as trusted and adapt their security analysis accordingly. The typical trust assumption is that the devices located in Alice's and Bob's laboratories are properly characterized and isolated so that no other party can control the noise which is introduced by those devices or receive the information leakage from the trusted devices. Those trusted parts of the protocol are given in dashed boxes in Fig. 3 and typically include the source of the signal states, the modulator, and the detector. The trust assumption on the detectors can be waived in the MDI protocol shown in Fig. 5. Assuming that a de-

vice is untrusted typically means that the related noise is attributed to the channel, which strongly limits the performance of the protocols. Therefore, in this review, we keep to the standard assumption of trusted sender and receiver stations, unless specified otherwise.

1. Source and detection imperfections

The generated and modulated states can contain excess noise, originating either from the signal source (laser or source of squeezed states in case of coherent- or squeezed-state protocols respectively) or from the imperfect modulation. If the trusted parties can characterize this noise separately from the channel noise and localize it to the preparation part of their setup (by monitoring the signal in front of the channel using a tap-off or optical switch for back-to-back measurements in the sending station), they can consider this noise to be trusted. Such excess noise, referred to as *preparation noise*, was studied in (Filip, 2008) for purely lossy (noiseless channels) and extended to noisy channels in (Usenko and Filip, 2010). In the context of purification-based theoretical security analysis the trusted preparation noise is then purified using an entangled source in modes P_1, P_2 , similar to the untrusted noise purification by entangling cloner E_1, E_2 , shown in Fig. 6(c). One of the entangled modes is coupled to the signal mode prior to the channel on a beam splitter with transmittance T_P and the variance of the entangled state is set to $V_P/(1 - T_P)$, where V_P is the variance of the preparation excess noise. For $T_P \rightarrow 1$ the noise addition is then performed approximately losslessly (without attenuating the signal). The modes P_1, P_2 are not available for the measurement neither to the trusted parties, nor to the eavesdropper, and are used to keep the trusted preparation noise out of Eve's purification. The Holevo bound is then obtained as $S(A, B, P_1, P_2) - S(A, P_1, P_2|B)$ from the entropy of the four-mode state in modes A, B, P_1, P_2 and the entropy of the conditional state after measurement on Bob's side in the RR scenario (or from the entropy $S(B, P_1, P_2|A)$ of the conditional state after measurement on Alice's side in case of DR). While the trusted preparation noise does not directly contribute to Eve's information (being kept out of Eve's purification of the channel noise), it reduces the mutual information between the trusted parties and therefore the resulting key rate as well. It was shown, that the bound on the trusted preparation noise in RR in the purely lossy channels with transmittance T , in the asymptotic limit and in the limit of infinite modulation $V \rightarrow \infty$ reads $1/(1 - T)$ for the coherent-state protocol (Filip, 2008) and generalizes to $(2 - T)/(1 - T) - V_S$ for an arbitrary signal state variance V_S (Usenko and Filip, 2016). Controllable attenuation was suggested to compensate for the trusted preparation noise in RR (Filip, 2008). On the other hand, the trusted preparation noise is harmless in the DR scenario (Weedbrook *et al.*, 2010) and even improves the security of the protocol in the

noisy channels (Weedbrook *et al.*, 2012b), which potentially enables CV-QKD in the wavelengths beyond the optical domain, up to the microwave regime.

On the receiver side, the homodyne detectors are inclined to losses (due to the limited detection efficiency) and electronic noise, which, in the purification-based theoretical security analysis, is modeled similarly to the preparation noise by introducing a two-mode entangled state with variance $V_D/(1 - T_D)$, where V_D is the electronic noise and T_D is the detection efficiency (Lodewyck *et al.*, 2007). Similarly to the preparation noise, this implies a Holevo bound evaluation from a four-mode state (or from a six-mode state if both preparation and detection noise are to be taken into account). Similarly to the preparation noise, the trusted *detection noise* only limits the mutual information between Alice and Bob, but, unlike the preparation noise, it limits the applicability of the protocols in DR. Robustness of CV-QKD with DR and noisy detection is bounded by $(2T - 1)/(1 - T)$ SNU of detection noise regardless of the signal variance (Usenko and Filip, 2016) already in the purely lossy channels in the asymptotic limit. However, in case of RR, the detection noise can be even helpful for the protocols in noisy channels (García-Patrón and Cerf, 2009). This detection-noise RR counterpart of the positive effect of the preparation noise in DR protocols is known as “fighting noise with noise”, when the trusted noise on the reference side of the error correction protocols (Alice in DR and Bob in RR) helps the trusted parties to decouple Eve, who performs active attacks in the noisy channels, from the key data (Usenko and Filip, 2016). The trusted noise addition can be optimized to maximize the improvement to the security of CV-QKD over noisy channels (Madsen *et al.*, 2012).

Besides the excess noise and signal attenuation, the imperfections of Alice’s and Bob’s devices may lead to other unwanted effects, such as imperfect shot-noise calibrations or phase noise, with results in random phase rotations between the sent and the received data. Those imperfections were studied in (Jouguet *et al.*, 2012) for coherent-state CV-QKD, taking into account finite size effects for Gaussian collective attacks. It was shown that the phase noise degrades the correlations between the trusted parties, which also limits the performance of the protocols. By properly characterizing the phase noise, the trusted parties can however put tighter bounds on Eve’s information (Jouguet *et al.*, 2012).

Systematic analysis of trusted noise in realistic coherent-state CV-QKD was performed in (Laudenbach *et al.*, 2018) by developing models for various sources of noise, including source and LO intensity fluctuations, imperfect modulation, phase noise, common-mode rejection ratio in a homodyne detector, detection noise and quantization noise of the analog-to-digital converter. Those models allow to efficiently predict the performance of practical CV-QKD systems. However, the security of a particular implementation can only be based on the actually measured data and subsequent characterization of

trusted and untrusted noise, to be incorporated to the security analysis.

Analysis of practical imperfections in the composable finite-size security framework was performed for the no-switching protocol in (Pirandola, 2021a), considering different trust levels of the setup components.

2. Security side channels and loopholes

Besides the losses and noise in the sending and receiving stations, which can be assumed either trusted or untrusted, security of CV-QKD can be affected by *side channels*, providing an eavesdropper with partial knowledge on the distributed key data or on the noise, which is added to the key data. Side-channel leakage from the sending station and side-channel noise addition in the receiving station were theoretically analyzed in (Derkach *et al.*, 2016) and shown potentially harmful for RR and DR protocols respectively. Besides isolation of the trusted stations to prevent signal leakage and noise addition, the trusted parties may implement controllable noise insertion to the leaking mode or noise monitoring and subtraction of the side-channel noise. Leakage of the generated signal, prior to its modulation, can be harmful to the squeezed-state protocols, while coherent states are immune to such leakage, providing no additional correlations with the leaking mode (Derkach *et al.*, 2017). On the other hand, leakage of the modulated signal can directly provide an eavesdropper with the modulation data and remain unknown to the trusted parties. This was shown for the CV-QKD system using an optical in-phase and quadrature modulator with imperfect suppression of the side-bands, which are modulated, but are not measured by the receiver (Jain *et al.*, 2021), emphasizing the importance of good single side-band suppression in the sending station and careful characterization of the transmitted modes. The negative role of imperfect state preparation in parameter estimation, potentially leading to overestimation of secret key rate, was studied in (Liu *et al.*, 2017), also suggesting the methods for proper calibration of imperfect CV-QKD setups.

In addition to obtaining information on the key from side-channel leakage, Eve may send a light pulse to the sending station to learn the modulator settings in the so-called *Trojan horse attack*, well known for DV-QKD protocols (Gisin *et al.*, 2006). Such attacks can threaten the security of CV-QKD (Pereira and Pirandola, 2018) by providing Eve with side-information, which is equivalent to worsening the channel parameters. Such attacks can be ruled out by an additional sensing system in the sending station for monitoring the incoming and outgoing light (Pereira and Pirandola, 2018).

Besides attempting to learn the modulator settings using light probes, Eve may temper with the state preparation in the quantum hacking attacks on the sending station. In particular, Eve can perform an *attack on the optical attenuator* used for state preparation in the send-

ing station (Zheng *et al.*, 2019a). By sending bright light, Eve can damage the variable optical attenuator and reduce its attenuation level. This way Eve can also make trusted parties to overestimate the channel transmittance (hence underestimate Eve's attack), which can result in a security breach. The attack on the optical attenuator can be ruled out by optical isolation or, more efficiently, by continuous monitoring of signal modulation prior to sending the states to the channel (Zheng *et al.*, 2019a). Eve can also perform the *laser seeding attack* by injecting controllable CW laser light into a semiconductor laser source in order to manipulate the intensity of the laser used on the trusted sender side for signal state generation. This way Eve can scale up the displacements of the signals sent to the channel and force the trusted parties to underestimate the channel attenuation and, respectively, overestimate the bounds on the key rate, hence leading to a security breach (Zheng *et al.*, 2019b). The attack was shown to be particularly harmful for CV-MDI-QKD, but can also break the security of conventional CV-QKD schemes. An optical isolator can be used to block the injected laser seeding light, but it can also be laser-damaged by Eve. Alternatively, a real-time monitoring of LO intensity can be used to reveal and compensate for the laser seeding attack in the CV-QKD systems with LO generation on the sending side.

On the receiver side, additional detection noise may originate from imperfect mode matching in case of multimode signals (Usenko *et al.*, 2014) and should be assumed untrusted as being potentially under Eve's control due to propagation through the channel. This noise can be reduced or removed by mode filtering or increasing the brightness of the LO (Kovalenko *et al.*, 2019). The impact of the electronic noise of the detectors on security of CV-QKD can be on the other hand reduced by using multimode signals (Kumar *et al.*, 2019), which improve signal-to-noise ratio and the resulting secret key rate. Insufficient bandwidth of a balanced homodyne detector can lead to wrong parameter estimation of a CV-QKD system and affect its performance, which requires optimization of signal repetition rate and modulation pattern (Liu *et al.*, 2022a).

The homodyne detection based on the LO beam transmitted through the untrusted channel can be a target to numerous hacking attacks, when Eve can obtain information on the key, while hiding her attack by forcing the trusted parties to incorrectly estimate the channel parameters. In particular, Eve can carry out the *LO intensity attack* (Häseler *et al.*, 2008), an intercept-resend attack with an optimized detection and with the same amplitudes for the re-sent signal and the LO, leading to lower variances obtained from the measurements on the receiving side and hence lower estimated channel noise. Another possibility for Eve is to introduce *fluctuations to the LO intensity* (Ma *et al.*, 2013a), which also allows Eve to compromise channel noise estimation and force the trusted parties to underestimate the collective attack in the quantum channel, particularly in the RR scenario.

The intensity attack on the LO using introduced fluctuations was also recently reported for the DM CV-QKD protocols (Fan *et al.*, 2023). The intensity attacks on the LO can be prevented by LO monitoring, which can be, however, challenging for detecting the simulated fluctuations (Ma *et al.*, 2013a). The trusted parties can also vary the LO intensity in the sending station to prevent the LO intensity attacks and even improve the robustness of the protocols to the channel noise (Ma *et al.*, 2014). In addition to manipulating the LO intensity, Eve can perform the *wavelength attack* on the LO by intercepting both the signal and the LO and then re-emitting the signal and the LO at different wavelengths so that the wavelength-dependent beam splitter in Bob's heterodyne detector becomes properly unbalanced (Huang *et al.*, 2013; Ma *et al.*, 2013b). This allows Eve to impose required outcomes on Bob's detector and hide her attack under the shot noise contribution of the heterodyne detector. The wavelength attack can also be implemented against protocols with homodyne detection (Huang *et al.*, 2014) by affecting the shot-noise measurements, leading to wrong estimation of the channel noise. Such attacks can be compensated by randomly applying wavelength filters or controllable attenuation in the receiver and advanced real-time shot-noise monitoring (Huang *et al.*, 2014).

Estimation of shot noise can be affected by Eve using a *calibration attack* on the LO (Jouguet *et al.*, 2013a). This is done by attenuating the beginning of an LO pulse, introducing a delay to the trigger signal for the homodyne detector, which decreases the detection response slope. The trusted parties then overestimate the value of the shot noise and, subsequently, underestimate the channel noise, which hides Eve's attack in the quantum channel and leads to a security break. This type of quantum hacking attack can be repelled by real-time shot noise measurements, such as random strong attenuation applied to the incoming light in the receiver or introduction of a beam splitter and subsequent calibration of the relative sensitivity of the two homodyne detectors (Jouguet *et al.*, 2013a). Calibration in the CV-QKD measurement can also be exploited by Eve using a *polarization attack* (Zhao *et al.*, 2018) on systems using polarization multiplexing of the signal and the propagated LO. In such schemes the polarization drift of the incoming light is compensated using polarization monitoring of the LO and real-time feedback control. However, only part of the pulses is measured due to the limited detection rate. It even can change the polarization of the remaining LO pulses, leading to the leakage of the LO into the signal after demultiplexing (without interference with the signal due to time delay) and to reduction of the LO intensity. The measured shot noise is then reduced, which again leads to underestimation of the channel noise. Such attack can be removed by polarization monitoring on all the pulses (Zhao *et al.*, 2018) or by a real-time shot-noise monitoring (Kunz-Jacques and Jouguet, 2015).

Attacks on the transmitted LO and the subsequent parameter estimation can be removed by the local gen-

eration of the LO in the LLO (“local local oscillator”) schemes. In this case, Alice generates reference pulses (pilot tones), which are used by Bob to phase-lock his local strong coherent LO with Alice’s prepared signal (Marie and Alléaume, 2017; Qi *et al.*, 2015; Soh *et al.*, 2015). The residual phase drift between the measurement and preparation bases should be then removed by the data post-processing as discussed in Sec. III.E. Recently, the time-variant parameter estimation and compensation was proposed in (Xu *et al.*, 2024) to improve robustness of LLO-based schemes.

However, the LLO systems can be vulnerable to an attack on the pilot tones referred to as the *reference pulse attack* (Ren *et al.*, 2019). Within the trust assumption on the phase noise due to the bases mismatch, Eve can identify the reference pulses and propagate those through an ideal channel, this way reducing the phase noise. Then, within the total estimated excess noise at the receiver, Eve can increase the fraction related to the channel noise by performing a stronger eavesdropping attack in the quantum channel, which remains hidden and can lead to a security breach. In order to prevent these attacks, the trusted parties can assume perfect transmission of the reference pulses, while keeping the trust assumption on the phase noise. A more efficient countermeasure for the trusted parties is to continuously monitor the intensity of the pilot tones and calibrate the phase noise accordingly (Ren *et al.*, 2019). LLO schemes can also be vulnerable to the polarization attack similarly to the conventional protocols with the shared LO (Shao *et al.*, 2022). To avoid attacks on a shared phase reference, be it LO or pilot tones, the shared-reference-frame-independent CV-QKD protocol was proposed recently in (Usenko, 2025), based on UD encoding, heterodyne detection, and subsequent bases alignment on the receiver side by a suitable phase-space rotation of the measured data.

As an alternative to the attacks on the phase reference, Eve can perform the *saturation attack* on CV-QKD (Qin *et al.*, 2016) by strongly displacing the incoming signals in order to reach the nonlinear response regime of the homodyne detector. The measured quadrature variance then becomes reduced, which leads to underestimation of the channel excess noise and to a security breach of the protocol. In order to prevent this type of attack the trusted parties should ensure the linear regime of the detector, e.g. by post-selection tests or by introducing a variable attenuator before the detection (the attenuator has to be wavelength-insensitive to avoid opening another loophole). Furthermore, the homodyne detection in CV-QKD can be compromised by the *blinding attack* (Qin *et al.*, 2018) similarly to the well-known hacking attack on the single-photon detectors in DV-QKD (Lydersen *et al.*, 2010). By sending bright light to the homodyne receiver with an imbalance between two photodetectors, Eve can produce the signal current displacement, resulting in saturation of the electronic amplifier in the receiver. Similarly to the saturation attack, the detection becomes nonlinear, leading to a security breach. Contrary to the sat-

uration attack, however, Eve does not need to phase lock the injected light with the signal in order to carry out the blinding attack, which make this type of quantum hacking more feasible than the saturation attack. This type of attack can also be ruled out by verifying the linearity of the detection (Qin *et al.*, 2018). Both attacks were experimentally studied in the context of attacks rating, aimed at quantifying the risks for practical CV-QKD systems (Kumar *et al.*, 2021).

The MDI protocols, which waive the trust assumption on the measurement in CV-QKD, are immune to any type of detector attacks described above but can be vulnerable to attacks on the sources, such as the Trojan horse attack.

3. Security certification

As CV-QKD is approaching technological maturity, yet still being the subject for active research and development, its practical use is closely related to certification of its security. In this process the QKD products undergo rigorous tests and assessments to confirm they meet defined security standards and requirements.

Despite the availability of commercial QKD products for more than 20 years, no independent security evaluation and certification has been performed yet, due to the absence of required standards and of a complete ecosystem.

Security certification is characterized by evaluation assurance level (EAL), which ranges from 1 (functionally tested) to 7 (formally designed and verified). Achieving a high-assurance security certification with EAL above 4 for QKD systems will represent a significant milestone, as it will establish a high level of trust in QKD products and unlock access to strategic, and highly regulated, sectors that require certification for secure communications products, such as government and defense, finance and banking, healthcare, telecommunication and critical infrastructures. Increasing amounts of efforts are currently invested towards this goal, with significant progress over the past years.

The methodology for achieving high-assurance security certification in QKD systems in the Common Criteria framework² involves a collaborative process among various entities, based on several steps and documents:

- **Protection Profile (PP)** is a document that defines the target of evaluation and the security requirements that will need to be tested and validated. It is typically developed by experts and may be endorsed by national or international bodies to ensure consistency and relevance across sectors. The PP outlines criteria for evaluating the security properties of system (here QKD) covering

² see <https://www.commoncriteriaportal.org/cc/index.cfm>

both the functional requirements and threat mitigation strategies.

- **Security Target.** The manufacturer of the QKD system is responsible for designing and producing the product in alignment with the PP requirements. To illustrate this compliance, the manufacturer provides a documentation, called Security Target on the product's architecture, security features, and implementation details, which will be used by the evaluation lab during testing.
- **Evaluation Report.** An accredited third-party evaluation lab, helped by the Security Target document, performs a thorough assessment of the QKD product against the PP. The lab conducts tests to verify that the product meets the specified security standards and is resistant to the types of attacks outlined in the PP. Following the evaluation, the lab produces an Evaluation Report that details the findings, including any security weaknesses or compliance issues.
- **Certification by National Authority.** The Evaluation Report is submitted to a recognized certification body, typically a national authority or a standards organization. This body reviews the report and ensures that the QKD product meets all required security criteria for the targeted EAL. Upon satisfactory review, the certification body issues an official certificate, endorsing the QKD system as meeting the PP requirements for the targeted EAL.

It is important to note that certification of a QKD system is a risk-based process, different in nature from deriving a security proof. Yet both these approaches are compatible, and complementary. Certification provides assurance of a lower bound on the practical security of a QKD system. This requires to assess the complexity of possible attacks, using for instance attack ratings (Kumar *et al.*, 2021). An important effort is also needed to standardize some key aspects (tackled in different sections of this review) such as security proof III.B practical implementation including parameter estimation procedures III.C, vulnerability analysis III.D as well as the cryptographic use cases, i.e., how QKD is used and combined with other cryptographic primitives, to achieve a particular security service.

From the viewpoint of security evaluation and certification, CV-QKD systems have several specificities:

- **Calibration.** The parameter estimation phase requires, for most CV-QKD protocols, some quantities that can be considered as trusted (see III.C) to be calibrated. Over-estimating trusted noise can lead to attacks (Huang *et al.*, 2014) while its under-estimation leads to reduced performances. The precision with which these calibrations can be achieved

depends on the number of samples used for calibration procedure, but also on the sampling dynamic and the stability of the processes. This is notably the case for the electronic noise (Brunner *et al.*, 2020) and for the shot noise (Van Der Heide *et al.*, 2023), that are crucial procedures for which one can foresee the need for a standardized approach.

- **Digital signal processing.** Modern CV-QKD systems can leverage high-bandwidth acquisition electronics to digitally track and correct noise occurring at the optical channel level (such frequency and phase noise, dispersion, polarization drift). DSP has allowed to reach high key rates (Roumestan *et al.*, 2022) as well as high spectral efficiency (Eriksson *et al.*, 2020), but also requires to revisit calibration procedures and how the logical channel is defined (Chen *et al.*, 2023) as a function of analog and digital filters.
- **Integration and system modularity.** A specificity of CV-QKD connection is that it can be operated essentially over a single mode, with hardware subsystems (laser, modulators, coherent receivers) that are extremely close to those used by classical optical coherent communication systems. The single-mode feature reduces vulnerability to optical side-channels and moreover facilitates key aspects of network integration such as joint operation (Aymeric *et al.*, 2022) and coexistence with classical channels (Kumar *et al.*, 2015), as well as point to multi-point operation (Hajomer *et al.*, 2024a).

E. Post-processing

In general, for a typical P&M QKD protocol, after Alice has prepared a sequence of quantum states and Bob has measured these states, they jointly convert their classical information on those quantum states (e.g., preparation bases and bit values, measurement basis, and results) into a final secure shared key. This conversion process is commonly called post-processing (see (Luo *et al.*, 2024) for a recent comprehensive review of QKD post-processing) and consists of several separate steps, namely sifting, parameter estimation, information reconciliation, and privacy amplification, which must be implemented according to the security proof. To accomplish these tasks, Alice and Bob exchange messages over an authenticated channel on which Eve can learn the content of the messages but cannot modify them.

1. Post-processing performance

We start with discussing the important figures of merit, characterizing the performance of post-processing implementations.

General performance characteristics for all post-processing steps are (i) achievable throughput of secure key generated, and (ii) computing resources (computing power, memory) needed to generate one secure key bit.

We observe that in CV-QKD protocols all quantum states that Alice prepares and transmits are detected and measured by Bob. This is in contrast to DV-QKD where the detection (click) rate of the single-photon detector(s) is much smaller than the number of states prepared. Therefore, if post-processing should occur in real-time (such that no quantum states remain unused) after the sifting step a CV-QKD protocol still has to process information at a rate that is of the same order of magnitude as the state generation rate r_{gen} . In comparison, a DV-QKD protocol processes state information after sifting only at a rate that is orders of magnitudes lower, i.e., at $r_{\text{gen}} \times \mu \times T \times \eta$, where μ (typically, $\mu < 1$) is the mean photon number of the states prepared, $T \ll 1$ is the channel transmission, and $\eta < 1$ is the detection efficiency.

For the information reconciliation step, the *error correction efficiency* β is an important parameter that can be decisive for secure key generation by a QKD protocol. For reconciliation of a block of n bits, that were transmitted over a noisy quantum channel, by exchanging n_{leak} bits on the classical error-free channel, β is given by

$$\beta = \frac{n - n_{\text{leak}}}{n \times C}. \quad (44)$$

Here C is the channel capacity, which refers to the maximum rate (per channel use) at which information can be reliably (with negligible error rate) transmitted over a noisy channel. If reconciliation is performed by transmitting syndromes of linear block codes with a block size n , a syndrome length s , and a corresponding code rate $R = 1 - \frac{s}{n}$, then

$$\beta = \frac{R}{C}, \quad (45)$$

since the number of leaked bits n_{leak} is given by the length of the syndrome s .

The *frame error rate* (FER, also sometimes referred to as the word error rate), which is the ratio of the number of data frames that cannot be successfully reconciled to the total number of frames, is another important parameter that influences the secure key rate. Recently, the FER has been taken into account in a security proof in the finite-size regime against collective attacks (Hajomer *et al.*, 2025b), scaling the typically dominating component of the key rate by $(1-\text{FER})^3$. Note that the channel capacity is defined for a negligible FER. If and only if

reconciliation must have a negligible FER, $R < C$, i.e., $\beta < 1$ must hold.

Due to imperfections in codes and decoders and limited computational decoding resources, the efficiency β is typically lower than 1 even if a non-negligible FER is accepted. Values of β up to 98% were reported in CV-QKD experiments (see Table IV). However, accepting a FER of 99.99% (Johnson *et al.*, 2017) demonstrated that an LDPC code can reach an efficiency of $\beta = 1.09$.

Often, information reconciliation uses an iterative decoding algorithm, and then the number of iterations used is another important parameter, because the time needed to decode is directly proportional to the number of iterations performed. In general, using a higher number of iterations achieves a higher value of β for the same value of FER.

For the privacy amplification step, we observe that finite-size proofs typically demand a data block size of 10^{10} or even (much) larger, which can result in the need for large memories.

We further discuss the main steps and respective methods for post-processing in CV-QKD.

2. Sifting

As it was already mentioned, two detection schemes are typically used in CV-QKD: homodyne detection, where Bob measures a single quadrature (either $\hat{x}$ or $\hat{p}$), and heterodyne detection, where Bob measures both quadratures simultaneously. In the homodyne-based CV-QKD protocols Bob therefore has to randomly switch between non-commuting quadratures for each received quantum state. This is typically accomplished by adjusting the LO phase between 0 and $\frac{\pi}{2}$, often with the aid of quantum random number generator. Random switching is essential for security, as it means that in a direct attack, Eve would only match Bob's basis half the time. Even if she could retain quantum states in memory and wait until Bob reveals his basis, she would still not be able to influence the measurement outcome. This switching process, however, requires a "sifting" step, where Bob communicates with Alice his choice of quadratures for each received quantum state over an authenticated public channel, allowing Alice to retain only the data corresponding to Bob's selected quadrature, ensuring they are in agreement.

3. Post-selection

As discussed in Sec.III.F.2 in more detail, discarding information of selected states from further processing conditioned on measurement outcome can be utilized in some CV-QKD protocols to increase the secure key rate. Another advantage of post-selection relevant in the context of post-processing is that the reduced number of states leads to a reduction in the computing resources

³ This follows from combining Eqs.(2) and (3) in (Hajomer *et al.*, 2025b).

needed. During the post-selection Bob has to decide which states will be discarded.

4. Parameter estimation

After the quantum phase, where Alice and Bob prepare and measure quantum states, they move on to parameter estimation. This step enables them to estimate system parameters essential for calculating the secret key rate according to a specific security proof. Traditionally, parameter estimation involves Alice and Bob disclosing a portion of their modulated and measured quadrature values. However, this approach limits the length of the generated secret key. To address this, most recent CV-QKD implementations have reordered the post-processing steps so that information reconciliation occurs before parameter estimation (Hajomer *et al.*, 2024c; Jain *et al.*, 2022; Leverrier, 2015). This adjustment allows all measurements to contribute to both parameter estimation and secret key generation.

The parameter estimation process in DM CV-QKD differs from that of traditional Gaussian-modulated protocols. To clarify, we examine this step using the traditional Gaussian-modulated CV-QKD protocol as an example. In such a protocol, calculating the secret key rate requires constructing the covariance matrix of the P&M scheme, which can then be translated into an equivalent EB scheme for security analysis. To build this covariance matrix, Alice and Bob must estimate the channel parameters, specifically the channel transmittance T and the excess noise ν which they can achieve through the following measurements:

1. Electronic noise. Measured by turning off the LO and blocking the signal input port.
2. Vacuum noise (shot noise). Measured by blocking the signal input port while keeping the LO port open.
3. Modulated quantum states. Measured by keeping both the signal and LO ports open.
4. Back-to-back measurement. Conducted to monitor and calibrate the modulation variance at the channel input. This is typically done by connecting the transmitter and the local receiver on the sender side through a short channel (an optical switch between the local receiver and the quantum channel) or, alternatively, by tapping a small portion of the signal at the transmitter side and measuring it locally. In this setup, it is assumed that the channel transmittance is equal to one and that the excess noise is zero (hence, the channel is perfect). Given the quantum efficiency of the receiver η , the modulation variance V_m can be estimated as:

$$V_m = \frac{V_{B2B} - V_{\text{elec}} - 1}{\eta\mu}, \quad (46)$$

where V_{B2B} is the variance of the measured quadrature in shot noise units, V_{elec} is the electronic noise variance, and μ is the parameter equal to 1 for homodyne detection or 2 for heterodyne detection.

After completing these measurements, Bob normalizes his measurement using the variance of the vacuum noise. Alice and Bob can then use their shared quadrature values to estimate the channel parameters as:

$$T = \frac{z^2}{V_m\eta}, \nu = TV_m - \frac{V_B - V_{\text{elec}} - 1}{\eta\mu}, \quad (47)$$

where z^2 is the covariance (correlation) between Alice's and Bob's quadrature values.

This estimation is based on the assumption that Alice and Bob exchange an infinite number of quantum states, allowing the calculation of the secret key rate in the asymptotic regime. However, in practical systems, the number of exchanged quantum states is finite, leading to fluctuations in parameter estimates. This finite-size effect is mitigated by applying a confidence interval based on the number of exchanged states to ensure a worst-case estimation (Leverrier *et al.*, 2010) and is discussed in detail in Sec. III.B.

5. Information Reconciliation/Error Correction

Information reconciliation (also called error correction) is always needed to achieve a *correct* protocol, i.e. one that either produces identical keys for Alice and Bob or aborts with probability close to one. This process involves mapping Alice's and Bob's quadrature values into binary data and then applying an error correction algorithm, which requires exchanging information, such as syndromes, over an authenticated public channel.

In Gaussian-modulated CV-QKD, there are two main reconciliation approaches, depending on how the quadrature values are mapped to binary strings: *sliced reconciliation* (Van Assche *et al.*, 2004) and *multi-dimensional (MD) reconciliation* (Leverrier *et al.*, 2008).

Sliced reconciliation uses a multilevel encoding and multi-stage decoding process, applying different error correction codes, such as LDPC codes or polar codes, as the SNR varies across levels of coding. This approach allows encoding of more than one bit per quantum state and is typically applied at SNR values above 0 dB, making it effective for moderate distances (up to around 30 km). This distance limitation occurs because slicing is effective only when the received SNR at Bob's end is sufficiently high. With independently chosen code rates for each m slices ($R_i (1 \leq i \leq m)$), the error correction efficiency β can be computed as (Jouguet *et al.*, 2014):

$$\beta = \frac{H[Q(B)] - m + \sum_{i=1}^m R_i}{I(A; Q(B))}, \quad (48)$$

where H is the binary entropy function and Q is the quantizing function.

MD reconciliation is an alternative method designed for low-SNR regimes (below 0 dB). The core idea in MD reconciliation is to rotate Gaussian variables so that they lie on a unit sphere in a d -dimensional space, using their norm to avoid issues with small absolute values. This approach reduces the high bit error rate observed in slicing protocols at low-SNR regimes. MD reconciliation has shown superior performance over slicing at longer transmission distances, supporting ranges up to 200 km (Zhang *et al.*, 2020). Like slicing, MD reconciliation can be paired with various error-correcting codes; however, it particularly benefits from multi-edge type LDPC codes, which are optimized for MD use at very low received SNR (Mani *et al.*, 2021). In this regime, state-of-the-art decoding can achieve throughputs of 1.44 and 0.78 Gbps for code rates of 0.2 and 0.1, respectively, enabling real-time secret key generation at 71.89 Mbps for 25 km and 9.97 Mbps for 50 km (Luo *et al.*, 2024).

The efficiency of MD reconciliation, defined as $\beta(\text{SNR}) = R/C_{\text{AWGN}}(\text{SNR})$, where R is the code rate and C_{AWGN} is the capacity of the additive white Gaussian noise channel, depends on both the intrinsic efficiency of the error-correcting codes, the received SNR and efficiency of mapping. This becomes evident when the overall efficiency is expanded in terms of the code efficiency, β_{Code} , and the channel efficiency, β_{Channel} , which depend on the dimension of the mapping. The overall efficiency can be expressed as (Milicevic *et al.*, 2018):

$$\beta = \beta_{\text{Code}} \times \beta_{\text{Channel}} = \beta_{\text{Code}} \times \frac{C_d(\text{SNR})}{C_{\text{AWGN}}(\text{SNR})}, \quad (49)$$

where $C_d(\text{SNR})$ is the ergodic capacity of multi-dimensional scheme with dimension $d = 2, 4$, or 8 . Consequently, rate-adaptive error correction, which uses techniques such as puncturing and shortening to adjust the rate of error-correcting codes, has been introduced to improve efficiency in practical implementations, where SNR fluctuates over the measurements. For a comprehensive comparison of the performance of different reconciliation methods and error correcting codes, refer to Ref. (Luo *et al.*, 2024).

After information reconciliation Alice and Bob perform error confirmation to ensure that the corrected key bit strings match on both sides. This is done by Alice and Bob randomly selecting a hash function from a family of universal hash functions. They then use this function to calculate the hash values of their corrected key bits and compare these values to verify whether the error correction was successful. If the hash values are identical, the keys are further processed in the next step. If the hash values do not match, the corresponding keys are deemed incorrect. These keys are either discarded entirely or corrected by one party sending its key in plaintext to the other. The choice of method depends on the security proof. For a recent review on information reconciliation in CV-QKD refer to (Yang *et al.*, 2023).

6. Privacy amplification

Privacy amplification is a crucial step in QKD that removes information leaked about key bits that Eve might have gained during earlier stages of the QKD protocol. It is typically carried out by first choosing a hash function randomly from a so-called *family of universal hash functions*. The value that chooses which hash function from the family (set) of hash functions is used is called “seed” and is assumed to be sampled from a uniform distribution. Then this hash function is used to map the corrected bit strings of length N at both Alice and Bob to a shorter secure key of length L (Bennett *et al.*, 1995).

Among various families of universal hash functions, multiplication with a randomly chosen *Toeplitz matrix* is the most commonly used method for privacy amplification in QKD. In a Toeplitz matrix all elements along each diagonal (from the upper left to the lower right) are identical. This property allows the matrix to be efficiently constructed using only the elements of its first row and first column. Privacy amplification using a Toeplitz matrix $\mathbb{T}$ can be directly implemented through matrix multiplication, $k_{\text{sec}} = \mathbb{T}k_{\text{corr}}$, where k_{sec} is the final secure key with length L and k_{corr} is the key after error correction with length N .

However, in the finite-size CV-QKD regime, N is typically very large – in the order of at least 10^{10} . This renders direct matrix multiplication infeasible, as the direct implementation of Toeplitz matrix multiplication has a time complexity of $O(N^2)$, which would significantly slow down the privacy amplification process, especially in high-speed QKD systems.

To address this, the fast Fourier transform (FFT)-based Toeplitz method has been used in several works (Tang *et al.*, 2019). This approach reduces the time complexity to $O(N \log N)$ by converting the Toeplitz matrix into a circulant matrix, enabling more efficient computation. Using this method, privacy amplification has been implemented on various hardware platforms, including GPUs, FPGAs, and co-processors (Weerasinghe, 2024). These implementations have achieved execution speeds ranging from Mbps to Gbps, making them suitable for real-time QKD systems.

The state-of-the-art method for accelerating the implementation of the privacy amplification for CV-QKD is the number-theoretical transform (Takahashi *et al.*, 2016), which, like the FFT, reduces the time complexity from $O(N^2)$ to $O(N \log N)$. Unlike the FFT, the number-theoretical transform operates entirely in finite fields using modular arithmetic, eliminating the need for floating-point and complex variables. This reduces the memory needed and, at the same time, avoids any potential round-off errors of floating-point operations. This approach has a similar throughput as the FFT approach, reaching rates from Mbps to Gbps (Takahashi *et al.*, 2016; Yan *et al.*, 2022).

Alternatives to Toeplitz hashing that are based on multiplication with either (i) a modified Toeplitz matrix or

(ii) circulant matrix, and that are slightly faster and need a shorter seed are discussed in (Hayashi and Tsurumaru, 2016). These alternatives have also a computational complexity of $O(N \log N)$.

7. Message Authentication

As mentioned, QKD protocols consist of two main phases, namely the quantum phase, where quantum states are transmitted and detected, and the post-processing phase, which includes classical communication and data processing. To achieve information-theoretic security, the post-processing phase requires a public authenticated channel to prevent man-in-the-middle attacks.

Authentication in QKD typically relies on either pre-shared symmetric seed keys or post-quantum cryptographic (PQC) keys for encrypting (signing) and decrypting (verifying) the hash values of classical messages (Fregona *et al.*, 2024). While symmetric key-based authentication provides information-theoretically secure solutions, it faces significant scalability challenges in large networks. The number of symmetric key pairs grows quadratically with the number of users, leading to increased overhead in storage, synchronization, and management. Trusted relays can alleviate this by forming star-type networks (Fröhlich *et al.*, 2013), where each user shares keys only with the relay. However, this architecture limits direct communication between users.

In contrast, PQC-based methods utilize a public key infrastructure (Wang *et al.*, 2021), where users receive digital certificates signed by a trusted authority. This approach enables an efficient and scalable authentication for large networks. Notably, using PQC in authentication, rather than for confidentiality or key distribution, ensures that, as long as the algorithm remains secure during the authentication process, the QKD-generated keys are also secure, even if the PQC algorithm is later compromised.

Authentication protocols in QKD include methods such as encode-decode (Gilbert *et al.*, 1974), key recycling (Wegman and Carter, 1981), and ping-pong delayed authentication (Kiktenko *et al.*, 2020). Encode-decode methods provide strong security by using each key only once, but their high key consumption makes them impractical. Key recycling protocols address this limitation by reusing keys cyclically, such as encrypting tags with one-time pads, significantly reducing key usage. Ping-pong authentication further optimizes this process by consolidating multiple rounds of post-processing into a single authentication step. This method employs bidirectional authentication, where both parties alternately verify each other.

For authentication, universal hash functions such as ϵ -AU₂ (almost universal) (Abidin and Larsson, 2012), ϵ -AXU₂ (almost XOR universal) (Rogaway, 1995), and ϵ -ADU (almost delta universal) (Stinson, 1996) are in-

tegral, with advancements focusing on minimizing key consumption while maintaining security.

In practical implementations of QKD, three key aspects of authentication must be addressed to ensure overall security:

1. Security of pre-shared authentication keys. Pre-shared keys may be distributed out-of-band, e.g., by using couriers. Alternatively, post-quantum cryptographic methods have been proposed to secure these keys (Wang *et al.*, 2021).
2. Key reuse. Reusing keys for multiple authentications could potentially compromise security. Encrypting all tags with one-time pads can mitigate this risk.
3. Security of QKD-generated keys. After the initial round of authentication using pre-shared keys, QKD-generated keys are used for subsequent authentications.

For an in-depth analysis of authentication security under various non-ideal conditions, refer to Table 9 in Ref. (Luo *et al.*, 2024).

F. Advances in CV-QKD

CV-QKD remains an actively developing field of research and many methods for improving the efficiency and robustness of the protocols were suggested during the past decades. The development is ongoing toward quantitative improvement of the figures of merit, such as key rate, secure distance (or, equivalently, tolerable attenuation), tolerable channel or untrusted preparation and detection noise (particularly relevant for protocol implementations beyond the optical domain), as well as cost reduction by means of simplification and integration of devices. On the other hand, the efforts are directed toward qualitative improvements, such as reduction of security assumptions, generalization of security models as well as closing the practical loopholes.

The quantitative improvements of the protocol performance can be, first of all, achieved by optimizing the parameters of the protocol. For example, it is known already from the early implementations of CV-QKD that modulation upon the imperfect error correction has to be optimized (Lodewyck *et al.*, 2007). Controllable trusted noise, which can be added to compensate for the noise in the quantum channel (García-Patrón and Cerf, 2009) should also be optimized to provided maximum robustness to noise (Madsen *et al.*, 2012). Optimized parameter estimation can also improve the performance (Ruppert *et al.*, 2014), especially when the channels are fluctuating (Ruppert *et al.*, 2019).

In addition to parameter optimization, CV-QKD can benefit from signal state engineering, the most typical example being the use of squeezed signal states instead of coherent signals, which allows to improve performance

and robustness of the protocols (García-Patrón and Cerf, 2009; Madsen *et al.*, 2012; Navascués and Acín, 2005), also in the fluctuating free-space channels (Derkach *et al.*, 2020), where squeezing however has to be limited (optimized).

Beyond the parameter and signal state optimization, applicability and security of CV-QKD can be improved by various methods, which we discuss below.

1. Quantum amplifiers and repeaters

Amplification is well-known and widely used in classical communications, where signal amplifiers (particularly, laser amplifiers in the optical domain) increase the magnitude of the signal in order to compensate for the transmission losses. However, quantum features are typically lost in such a process and quantum communication should be performed on the dedicated fibers, free from standard classical networking equipment. However, quantum states can also be amplified, which leads to enhancement of the signal, but comes at the cost of increased noise or probabilistic outcomes.

Quantum amplifiers in the phase-space description are usually distinguished between *phase-insensitive amplifiers* (PIA), which upscale both quadratures at the cost of excess noise in both, and *phase-sensitive amplifiers* (PSA), which amplify one of the quadratures, while de-amplifying another one, a typical example of such process being quadrature squeezing. The PIA is therefore a non-degenerate optical parametric amplifier (OPA), which transforms the signal (S) and idler (I) modes with quadratures $\hat{x}_S, \hat{p}_S$ and $\hat{x}_I, \hat{p}_I$ as $\hat{x}_{S/I} \rightarrow \sqrt{g}\hat{x}_{S/I} + \sqrt{g-1}\hat{x}_{I/S}, \hat{p}_{S/I} \rightarrow \sqrt{g}\hat{p}_{S/I} - \sqrt{g-1}\hat{p}_{I/S}$, where $g > 1$ is the amplification gain. The idler mode is ideally in a vacuum state, or, more realistically, in a thermal state, which results in the excess noise added to the signal quadrature variances. The PSA, on the other hand, ideally results in the signal transformation of the form $\hat{x}_S \rightarrow \sqrt{g}\hat{x}_S$ and $\hat{p}_S \rightarrow \sqrt{1/g}\hat{p}_S$ so that the amplified quadrature $\hat{x}$ becomes more noisy and the de-amplified quadrature $\hat{p}$ becomes squeezed. It was shown that an optimal PSA can compensate for the practical imperfections (losses and noise) of a homodyne detector, while an optimal PIA compensates for the imperfections of a heterodyne deceiver (Fossier *et al.*, 2009a), which is valid even for practical noisy amplifiers, provided their noise is limited. Positive role of PSA in CV-QKD was recently demonstrated experimentally in (Liao *et al.*, 2025), where it improved the photodetector clearance, resulting in the homodyne detection efficiency of 96%.

The possibility of using PIA and PSA in coherent-state CV-QKD over multi-span links was recently studied in (Notarnicola *et al.*, 2024). It was shown that the key rate can be increased using multiple PSAs placed between the link segments if all the segments are considered untrusted, while both PIA and PSA can be helpful for only one untrusted link segment.

To avoid noise addition by the PIA, the post-selection can be used, resulting in the probabilistic *noiseless linear amplifier* (NLA) (Xiang *et al.*, 2010), which is ideally free from the idler-mode noise, and can distill continuous-variable entanglement, which a resource for CV-QKD. By considering NLA after the quantum channel and building an effective channel model, it was shown, that NLA can extend the secure distance of Gaussian CV-QKD or, equivalently, improve the robustness to noise at given channel attenuation (Blandino *et al.*, 2012). The operation should be optimized due to a trade-off between the probability of success and the amplification gain.

The main building block of an NLA is typically the so-called *quantum scissors* scheme (Pegg *et al.*, 1998), which is based on the input beam (coming from a multiport splitting of the signal entering the NLA) balanced coupling to a single-photon state, mixed with vacuum on a variable coupler, then the output of the variable coupler, conditioned on the click on the proper output of the balanced coupler, results in the scissors output. The outputs are then recombined with the other outputs from other parallel scissors schemes to produce the probabilistically noiselessly amplified signal (Dias *et al.*, 2020). The quantum scissors scheme in the receiving station of Gaussian CV-QKD was studied in (Ghalaii *et al.*, 2020b), incorporating the essentially non-Gaussian single-photon coupling and filtering operations into security analysis. The obtained bounds on the secret key rate demonstrate the improvement of the secret distances of the protocol in certain regimes of non-zero channel excess noise, suggesting the perspectives of using quantum scissors as a building block for CV quantum repeater schemes (Dias and Ralph, 2017) useful for CV-QKD. The result was extended to DM CV-QKD in (Ghalaii *et al.*, 2020a). The quantum scissors scheme can be generalized to N -photon Fock states (Winnel *et al.*, 2020), which was shown to be more efficient for NLA than multiple application of single-photon scissors, and can be further improved by optimizing the general interferometric coupling (Fiurášek, 2022a).

Another CV quantum repeater scheme, based on the non-Gaussian entanglement distillation (Fiurášek, 2010; Lund and Ralph, 2009) (enabled by the single-photon states and detections) with subsequent Gaussification (Campbell and Eisert, 2012), postponed to the end of the repeater protocol by means of non-Gaussian entanglement swapping, was proposed and analyzed for CV-QKD (Furrer and Munro, 2018), showing the possibility to improve rates and distances of the protocols. It was also shown, that losses can be noiselessly suppressed by combination of noiseless attenuation (heralded by single-photon detection on the residual port of an attenuating beam splitter) prior to transmission and noiseless amplification of the transmitted state (Mičuda *et al.*, 2012). As an alternative to the quantum scissors scheme, which has to be multiply implemented on the split signal, NLA can be efficiently realized using multiple single-photon additions and subtractions (Zavatta *et al.*, 2010) or two-

photon addition and subtraction (Neset *et al.*, 2024), by using weak measurements based on strongly nonlinear optical interactions (Menzies and Croke, 2009), or by combining Gaussian thermal noise and photon counting (Usuga *et al.*, 2010), which allows concentration of phase information of coherent states.

The practical implementation of NLA and other CV quantum repeater schemes, potentially useful for CV-QKD, is, however, very challenging as it requires single-photon (or N -photon) state generation and efficient photodetection or high optical nonlinearities. Nevertheless, the NLA scheme can be implemented in the form of post-selection, as we discuss in the next paragraph.

2. Post-selection

Classical post-selection in the sense of conditioning on a particular measurement outcome was first suggested for DR CV-QKD protocols to beat the 3 dB channel loss limit (Silberhorn *et al.*, 2002b) in the absence of channel noise. Alternatively, a quantum post-selection can be applied, which is equivalent to a physical operation on the state. NLA, virtually implemented in the form of Gaussian post-selection, was shown compatible with the Gaussian security proofs and helpful for CV-QKD in (Fiurášek and Cerf, 2012), especially if combined with the virtual noiseless attenuation on the sender side (even without the need of pre-selection on this stage). It was shown, that such virtual NLA (also referred to as measurement-based) can improve secure distance or tolerable channel noise of the protocols (Walk *et al.*, 2013) and restore the key rate in the EB realization of CV-QKD (Chrzanowski *et al.*, 2014). The quantum filtering, equivalent to NLA operation, should also be optimized due to a trade-off between the post-selection region and reduction of the raw key data. The filter implementation requires a cut-off on the data filter, which should be large enough to result to Gaussian statistics. In the finite-size regime, this cut-off has to be optimized to provide sufficient improvement of the effective transmittance and, simultaneously to preserve Gaussian statistics and not worsen the parameter estimation (Hosseinidehaj *et al.*, 2020). The equivalence between physical and virtual realizations of NLA was studied in detail in (Zhao *et al.*, 2017), showing the lower success rate of the measurement-based virtual realizations. Practical realizations of NLA using quantum scissors and single-photon catalysis (photon addition or subtraction operation, which can reportedly act as NLA (Zhang and Zhang, 2018)) were theoretically studied in (Notarnicola and Olivares, 2023), taking into account limited detection efficiency, and compared to ideal NLA analyzed in (Blandino *et al.*, 2012), resulting in the extended secure distance for both practical realizations.

Classical post-selection was analyzed and shown helpful for DM CV-QKD with phase-shift keying (Kanitschar and Pacher, 2022), where optimal post-selection strategies can improve the performance of the protocols with

fewer signal states and reduce the performance gap between the trusted and untrusted detector models.

3. Photonic integration

The development of quantum integrated photonics is a major challenge and key enabler across all quantum technologies as it paves the way to systems with reduced cost and complexity, and increased scalability, stability and reproducibility (Moody *et al.*, 2022). In particular for quantum communication and QKD, the use of photonic integrated circuits (PICs) will facilitate their deployment in practical infrastructures, notably in heavily constrained environments like data centers or satellite payloads. Significant progress has been achieved in the last years on all major PIC platforms, including silicon, III-V compound semiconductors, or lithium niobate (Aldama *et al.*, 2022). Many of these developments have focused on DV technology, which however faces the challenge of integrating single-photon detectors (Liu *et al.*, 2022b). Coherent detectors used in CV-QKD are more amenable to photonic integration, leading to several demonstrations in this direction, although the field is in general relatively young and more progress is expected in the following years. Most demonstrations leverage the silicon (Si) platform, which offers compatibility with mature manufacturing processes and low-loss components, but indium phosphide (InP) opens the prospect of monolithic integration as it allows for laser integration in addition to high-speed modulators and efficient photodiodes.

At the component level, early experiments focused on Si-integrated homodyne detectors. In (Raffaelli *et al.*, 2018), an electronic-to-shot-noise clearance of 11 dB at 150 MHz was achieved, while the device was also used to produce random numbers at 1.2 Gbit/s. The experiment in (Bruynsteen *et al.*, 2021) combined a Si optical front end and a custom integrated transimpedance amplifier designed in a 100 nm GaAs pHEMT technology, showing enhanced stability, bandwidth, and noise performance for the developed photonic-electronic balanced homodyne detector. The clearance was 28 dB and the shot-noise-limited bandwidth exceeded 20 GHz. In (Jia *et al.*, 2023), the silicon-on-insulator platform was used for a time-domain balanced homodyne detector, which features a common mode rejection ratio of 86.9 dB, a clearance of 19.42 dB, and a quantum efficiency of 38%. This performance enabled CV-QKD with a secret key generation rate of 0.01 bits/pulse at 50 km. Still on the detection side, (Milovančev *et al.*, 2021) showed first the use of commercially available die-level components for balanced homodyne detection, with a clearance exceeding 20 dB and a common mode rejection ratio of 50 dB at 1 GHz, and then, in (Milovančev and Vokić, 2024), a receiver combining Si and BiCMOS, featuring much lower noise than wire-bonded counterparts at equivalent bandwidth. This performance was compatible with a key rate of up to 30 Mbit/s at 10 km, considering CV-QKD with

Gaussian modulation and an untrusted receiver assumption.

In addition to the above developments at the component level, (Bian *et al.*, 2024a) demonstrated improved system stability reducing the standard deviation of the secret key rate by an order of magnitude using a biased Mach-Zehnder interferometer integrated on Si. The experiment showed a stable rate of 1.97 Mbit/s at 60 km with fluctuations on the order of 1%, assuming a finite size regime. Furthermore, (Li *et al.*, 2023) used an InP reflective semiconductor optical amplifier coupled to a low-loss silicon nitride cavity to develop on-chip low-linewidth lasers (with linewidth ranging from 1.6 to 3.2 kHz), hence addressing the laser integration issue inherent in the Si platform. These lasers were used as signal and LO sources in a CV-QKD experiment reaching a secret key generation rate of 0.75 Mbit/s at 50 km.

Operation of PIC-based CV-QKD subsystems, receivers or transmitters, has only been demonstrated recently. In (Hajomer *et al.*, 2024b), a Si-integrated photonic-electronic receiver implementing phase diverse heterodyne detection (with two balanced detectors), showed CV-QKD operation at a record-high 10 GBaud rate with advanced DSP techniques. A Si-integrated receiver with germanium photodiodes implementing RF heterodyne detection (with one balanced detector) was used in (Piétri *et al.*, 2024b), where the optimal coupling efficiency reached 26%, with a clearance of 10 dB at 150 MHz bandwidth, and an achieved secret key generation rate of 2.4 Mbit/s at 10 km and 220 kbit/s at 23 km, also with advanced DSP. The experiment of (Bian *et al.*, 2024b) used Si photonics for a receiver featuring a clearance of 7.42 dB at a bandwidth of 1.5 GHz, compatible with CV-QKD in a local LO configuration with a secret key generation rate of 1.38 Mbit/s or 0.24 Mbit/s at the asymptotic or finite-size regime, respectively, at 28.6 km with a trusted receiver. Progress has been achieved on the transmitter side as well, with a pulsed experiment with Gaussian modulation and pulse shaping, using an InP-integrated transmitter that includes an electrooptic modulator, an in-phase and quadrature (IQ) modulator equipped with thermo-optic and current-injection phase shifters, and a variable optical attenuator, featuring a 1 GHz bandwidth (Aldama *et al.*, 2023). The experiment achieved a rate of 2.3 Mbit/s in a back-to-back configuration or 0.4 Mbit/s at 11 km.

Full on-chip CV-QKD system operation still remains quite challenging. The very first PIC used for CV-QKD (Ziebell *et al.*, 2015) was in fact a transceiver including modulators based on carrier depletion, injection and thermal effects, and also germanium photodiodes in a homodyne detector. However, although this work demonstrated the possibility to integrate all key components, there was no performance assessment as a full system. More recently, (Zhang *et al.*, 2019) showed a Si-integrated system with both transmitter and receiver chips, including all key components. The system operated in a pulsed, transmitted LO configuration, with a

homodyne detector and Gaussian modulation. The laser was not integrated and the bandwidth was limited to 10 MHz due to the detector transimpedance amplifier. The detector featured a clearance of 5 dB and a quantum efficiency 49.8%, and the achieved secret key generation rate was 0.14 kbit/s over a simulated 100 km fiber.

With the increasing importance of photonic integration in several technological fields, a lot of progress is expected in the coming years, with a direct positive impact to quantum communication. Further advances will undoubtedly include advanced and efficient packaging techniques, optimized coupling methods, and co-integration of photonic and electronic chips. In particular for CV schemes, in addition to low-linewidth laser integration, a crucial challenge remains addressing the inherent trade-offs involved in high sensitivity, low noise and high bandwidth detection, in the presence of multiple photonic components on the same chip. This calls for precise control and optimization procedures in the entire chip and surrounding circuit that need to be validated in deployed quantum communication systems hence confirming the expected advantages of the use of integrated photonics.

4. Channel multiplexing and co-existence

Already in the first tests of CV-QKD, mode multiplexing was used to simultaneously transmit quantum signals and LO (Fossier *et al.*, 2009b; Lodewyck *et al.*, 2007). However, signal multiplexing can also be used to improve the performance of CV-QKD protocols. In particular, three-dimensional multiplexing (in wavelength, polarization, and orbital angular momentum) was shown to increase the rates of DM CV-QKD over free-space channels (Qu and Djordjevic, 2017). Multiplexed quantum teleportation was shown a promising tool for enhancing the quantum communication rates (Christ *et al.*, 2012). The possibility to upscale the secret key rate of Gaussian CV-QKD by means of mode multiplexing in the multi-mode fibers was demonstrated in (Sarmiento *et al.*, 2022). It was also shown theoretically and verified in the proof-of-principle test on a frequency-multiplexed source of entanglement in (Kovalenko *et al.*, 2021), revealing the negative role of the inter-mode cross talk, as well as suggesting cross talk removal by means of optimized data processing (equivalent to a passive linear-optical network to comply with Gaussian security proofs). Multiplexed CV-QKD over 194 channels with a total key secret rate of 172.6 Mbit/s over 25-km distance was reported in (Eriksson *et al.*, 2020), revealing the power of mode multiplexing for increasing the capacity of coherent-state protocol.

Quantum signals can also be multiplexed with classical communication channels, which is referred to as co-existence between QKD and classical communication and is essential for practical implementation of CV-QKD over existing fiber-optical networks. The possibility to perform CV-QKD over dense-wavelength-division multiplexing networks was experimentally studied in (Kumar

et al., 2015) in a 25-km long fiber link. It was shown, that Gaussian coherent-state CV-QKD, operating at 1500 nm, can coexist with the noise from up to 11.5 dBm classical channels at the same wavelength in the forward direction (9.7 dBm in the case of back-propagation). In the 75 km channel, the tolerable classical channel power was -3 and -9 dBm respectively. An experimental test of coherent-state CV-QKD jointly with 100 wavelength-division-multiplexed (WDM) channels with a total data rate of 18.3 Tbps in a 24-hour operation was reported in (Eriksson *et al.*, 2019b). Cross talk from the classical channels was studied in its impact on coherent-state CV-QKD in (Eriksson *et al.*, 2019a), showing that in-band cross talk from 30 WDM channels can stop the protocol, but by placing CV-QKD in wavelength not used by the classical channels the protocol can be realized even in the presence of amplified spontaneous emission noise. Impact of four-wave-mixing noise from dense WDM systems on EPR-based CV-QKD was studied in (Du *et al.*, 2020). Demonstration of CV-QKD in the existing telecommunication infrastructure was recently reported in (Jain *et al.*, 2024), combining CV-QKD channels with 100G optical transceivers operating at 1300 nm.

Further directions of ongoing development in CV-QKD include advancement of the detection schemes, particularly in a hybrid Gaussian CV-QKD protocol with photon-number resolving detectors, that can improve the secret key rate in the purely lossy channels and under the assumption that Eve employs homodyne detection (Cattaneo *et al.*, 2018). Recent results of the optimized state-discriminating receivers report extension of the security distance of CV-QKD in wiretap (noiseless) channels (Nortnicola *et al.*, 2023).

Protocol simplification by so-called *passive preparation* using splitting of a thermal state can reduce the cost and potentially remove some of the side channels in the preparing station, as suggested theoretically (Qi *et al.*, 2018) and recently studied experimentally (Qi *et al.*, 2020).

IV. CV QUANTUM COMMUNICATION BEYOND QKD

While QKD remains the most mature application of CV quantum communication, there are a few more protocols, that can be potentially realized using CV systems, as we discuss in the current section.

A. Quantum secure direct communication

CV-QSDC was proposed in (Pirandola *et al.*, 2008b) and consists of the two major phases: message mode and control mode, which relate to the message transmission and verification of its security, respectively.

The phase space is first discretized via a square lattice so that any pair of bits is specified by the parity of the phase-space coordinates of the respective lattice cell. In

the message phase, for each pair of message bits (u, u') the sender, Alice, computes the message amplitude $\alpha_{uu'}$, which points to the center of the lattice cell. Alice then adds a mask amplitude α_M to each of the message amplitudes so that the generated coherent signal states with amplitudes $\bar{\alpha} = \alpha_{uu'} + \alpha_M$ are continuously Gaussian-distributed across the phase space. Each signal state is measured by the remote receiving party, Bob, using a heterodyne detector, resulting in the outcome $\beta \simeq \bar{\alpha}$. The CV-QSDC setup is, therefore, conceptually very similar to the P&M CV-QKD scheme shown in Fig. 3. For each pair of bits, Alice classically communicates the mask α_M to Bob, who can then unmask the signal by computing $\beta - \alpha_M \simeq \bar{\alpha} - \alpha_M = \alpha_{uu'}$ and retrieve the message bits (u, u') through lattice decoding. Security analysis of the scheme relies on the assumption of individual attacks, in which it is optimal for an eavesdropper Eve to apply a universal Gaussian quantum cloner, which would unavoidably introduce noise to the signal. Therefore, in the control mode of the protocol, Alice only prepares the Gaussian-distributed signals $\bar{\alpha}$ and, after the transmission and detection, communicates their amplitudes to Bob, who extracts a test variable as $\beta - \bar{\alpha}$, from which the total channel noise can be inferred.

By setting a noise threshold value, the trusted parties can verify whether they should continue or abort the protocol. In principle, the threshold can even be set to zero noise, and the security of the scheme was analyzed in such a strict case (Pirandola *et al.*, 2008b). Trusted parties can optimize the lattice size and the fraction of control mode rounds of the protocol, which should be randomly switched to from the message mode, while Eve can optimize the added noise to obtain the maximum information on the message bits. Using the optimized settings, it was shown, that Alice can transmit 630 bits by using 2.2×10^4 systems, while Eve can steal 80 bits. The amount of leaking information can be decreased by increasing the fraction of the control mode runs (making the protocol less efficient) or by employing classical error correction codes, which make the decoding more sensitive to the presence of channel noise. In the above-mentioned model case, the optimal code allows decreasing the stolen bits to 10.

A CV-QSDC protocol based on Gaussian mapping of the classical data, encoded in the quadratures of TMSV states shared between Alice and Bob, was proposed and analyzed in (Cao *et al.*, 2021), building upon the previous theoretical works (Chai *et al.*, 2019; Srikara *et al.*, 2020). In this scheme, Alice prepares a TMSV state, randomly measures the quadratures of one of the modes, communicates the respective time slots and measurement outcomes to Bob, and sends both modes to Bob. Bob performs the same measurements on the other mode and verifies the nonseparability of the obtained TMSV. The trusted parties check the error rate between their data sets to be below a pre-agreed threshold and proceed to the Gaussian mapping stage once the condition is fulfilled. The secret message is divided into blocks and

mapped onto a sequence of Gaussian random values, G_1 . The values are used to modulate one of the quadrature observables of Alice's mode, another Gaussian sequence G_2 is used to modulate the complementary quadrature and the modulated mode is sent to Bob. Alice also classically communicates the sequence G_2 to Bob, who couples the modulated mode with the residual mode of TMSV and measures either of the quadratures on the two output modes. After that, the trusted parties perform the parameter estimation based on Bob using the measurement outcomes of the quadrature to which the sequence G_2 was encoded with the G_2 received from Alice. Alice and Bob perform the error correction on the data sequence G_1 (as modulated by Alice, and its version obtained by Bob after the channel). Finally, the trusted parties perform privacy amplification to eliminate the information introduced by the Gaussian mapping (which has to be optimized to account for the non-uniformity of the messages) as well as the information leaked from the quantum channel. The security of the scheme is analyzed against collective attacks following the techniques for Gaussian CV-QKD, strictly assuming that the second mode of TMSV, which is used by Bob in the detection stage, is not accessible to an eavesdropper (while being transmitted through the same quantum channel).

The CV-QSDC protocol using single-mode squeezed states was proposed and experimentally tested in (Paparelle *et al.*, 2025) assuming beam-splitting eavesdropping attacks. In the two-way quantum communication scheme, squeezing was considered on one side or on both sides of the channel (referred to as asymmetric and symmetric protocols respectively). By using an optical switch, Alice randomly chooses between the control and message states, received by Bob, measuring the former with a homodyne detector and storing the latter in a quantum memory or a delay line. By comparing the measurement outcomes to the amplitudes, classically communicated by Bob for the designated control states, and verifying sufficiently low amount of errors, Alice then encodes the message by controllably attenuating part of the message states (contrary to applying more technically demanding displacements as initially suggested in (Srikara *et al.*, 2020)) and sends them back to Bob along with non-attenuated decoy signal states, used to further bound the eavesdropping. It was shown that squeezing is advantageous for such CV-QSDC protocol already in the asymmetric configuration (Paparelle *et al.*, 2025).

B. Quantum dense coding

CV-QDC was first proposed in (Ban, 1999) and (Braunstein and Kimble, 2000) on the basis of highly entangled TMSV states, as shown in Fig. 9. One of the modes is modulated by the sender, Alice, who performs encoding of a message by applying quadrature displacement with an amplitude $\alpha_{in} = x_M + ip_M$. The displaced mode and the second mode of the TMSV are

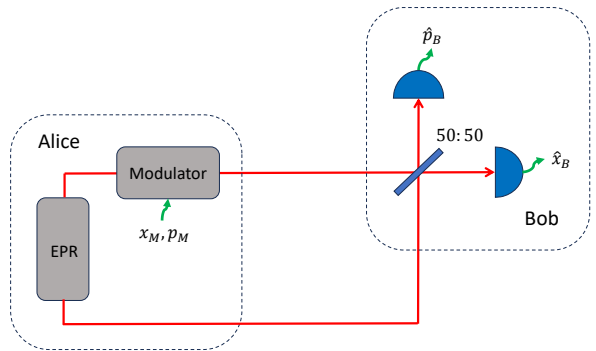


FIG. 9 Generic CV-QDC scheme. Alice generates a TMSV state (EPR), applies displacements x_M, p_M to one of the modes and sends both modes to Bob, who combines them on a balanced beam splitter and measures $\hat{x}_B$ and $\hat{p}_B$ quadratures on the output, to obtain the encoded message (encoding and decoding parts are not depicted and are explained in the text).

then sent to the receiver, Bob, who combines the modes on a balanced beam splitter and measures quadratures $\hat{x}_B$ and $\hat{p}_B$ on the outputs. The resulting outcomes are normalized and combined to obtain the output amplitude $\alpha_{out} = x_B + ip_B$, which constitutes the message received by Bob. In the limit of infinitely strong TMSV squeezing (or, equivalently, mean photon number $\bar{n} \rightarrow \infty$) $\alpha_{out} = \alpha_{in}$, meaning that the message is perfectly recovered. However, even upon limited squeezing (and, respectively, finite $\bar{n}$), CV entanglement of a TMSV state enables dense coding by achieving larger channel capacity than coherent- or squeezed-state communication with the same mean photon number. Indeed, the dense coding capacity of the CV-QDC scheme in the case of Gaussian-distributed signals α_{in} reads $C_{QDC} = \log(1 + \bar{n} + \bar{n}^2)$, which for the strong squeezing is approximated through the squeezing parameter as $4r$. On the other hand, P&M communication using coherent states can achieve $C_{coh} = \log(1 + \bar{n})$, which is always less than C_{QDC} , and using squeezed states the capacity of $C_{sq} = \log 1 + \bar{n}$ can be achieved, which is less than C_{QDC} for any $\bar{n} > 1$ (Braunstein and Kimble, 2000). Importantly, the CV-QDC protocol, operating at high parametric gains of the TMSV sources, allows for highly efficient deterministic transmission, contrary to the DV QDC protocols, which employ weak sources and perform probabilistically (Braunstein and Kimble, 2000). The analysis of CV-QDC was extended to lossy channels in (Ban, 2000), showing that CV-QDC remains advantageous at channel transmittance levels above approx. 0.63.

An experimental test of CV-QDC was reported in (Li *et al.*, 2002) with simultaneous sub-shot-noise measurements of signals encoded in the amplitude and phase quadratures, enabled by the CV entanglement produced using a non-degenerate OPA.

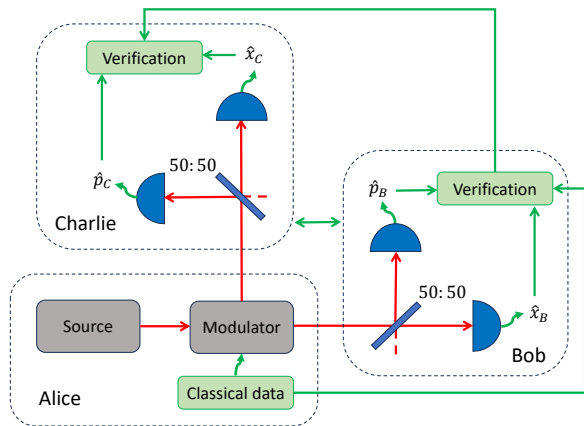


FIG. 10 CV-QDS scheme. Alice uses a laser Source and a quadrature Modulator to prepare the public key sequences of quantum states, and sends them to the remote parties Charlie and Bob, who perform heterodyne measurements of quadratures $\hat{x}_B, \hat{p}_B$ and $\hat{x}_C, \hat{p}_C$ respectively, feeding the outcomes to the verification procedures as well as exchanging the measurement settings and outcomes. Quantum links are given in red, classical links are given in green.

C. Quantum digital signatures

The QDS scheme using CV heterodyne measurements was suggested in (Croal *et al.*, 2016) and consists of two stages, namely the distribution stage, and the messaging stage. In the distribution stage, the sender, Alice, selects sequences of non-orthogonal quantum states for encoding a message bit, which forms the public keys. The classical information on the state sequences forms the private keys. Alice sends the public keys to two remote parties, Bob, and Charlie, over the respective quantum channels, as shown in Fig. 10. Bob and Charlie perform heterodyne measurements on the incoming quantum signals, hence obtaining the partial information on the public keys (eliminating the less probable quantum states according to the measurement results), which concludes the distribution stage. In the messaging stage, Alice sends a message to Bob or Charlie along with the corresponding private key. The message recipient checks if the private key sufficiently matches the previously obtained public key, which excludes the message forgery (when one of the remote parties fakes a message as originating from Alice). The protocol also enables message forwarding when the new recipient checks for mismatches with his measurement records and involves symmetrization to exclude repudiation by Alice (when Bob and Charlie disagree on the authenticity of a message), which relies on QKD established between the recipients. The mismatch threshold for acceptance of a forwarded message is then less strict compared to the direct messages received from Alice. Assuming collective attacks by dishonest parties and an otherwise authenticated quantum channel, the probabilities of the successful repudiation or forgery, as well as the probability of the protocol failure, can be

bounded from the protocol parameters. The probability of repudiation is bounded as

$$p_{\text{rep}} \leq 2 \exp \left[- (S_C - S_B)^2 \frac{L}{4} \right], \quad (50)$$

where S_C and S_B are Charlie's and Bob's acceptance thresholds, respectively. The probability of forgery is bounded as

$$p_{\text{forg}} \leq \exp \left[- (C_{\min} - S_C)^2 L \right], \quad (51)$$

where $C_{\min}$ is the minimum probability that an honest party will detect an error in an individual signature element coming from the forger. Finally, the probability of the protocol failure is bounded as

$$p_{\text{fail}} \leq 2 \exp \left(- \frac{g^2}{16} L \right). \quad (52)$$

where $g = C_{\min} - p_{\text{err}}$ with probability of error p_{err} being the probability for an honest recipient, properly following the protocol, to eliminate the state actually sent by Alice. The figure of merit for the CV-QDS protocol is the signature length $2L$, required to sign a one-bit message with a fixed probability of failure.

The above-described protocol was tested using sequences of four coherent states, $|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, | -i\alpha\rangle$ to encode single-bit messages, assuming authenticated quantum channels between Alice, Bob, and Charlie and achieving much larger signature lengths per quantum state compared to the DV QDS protocols (Croal *et al.*, 2016).

The CV-QDS scheme was extended to insecure quantum channels in (Thornton *et al.*, 2019), assuming collective attacks, modeled by an entangling cloner. The probability of failure in a purely lossy channel with transmittance T then reads $p_{\text{err}} = (1/2)\text{erfc}[\alpha\sqrt{T/2}]$. It was shown that the quantum encoding alphabet can be optimized in terms of the number of states and the displacement α . This allowed to assess the practical performance of the protocol, predicting the possibility of signing a single-bit message in the timescale of 1 millisecond at a distance of 20 km of standard telecom fiber, assuming a repetition rate of 100 MHz (Thornton *et al.*, 2019).

While the above-described protocols aim at iteratively signing single-bit messages, CV-QDS for multi-bit messages was developed in (Zhao *et al.*, 2021), also providing stronger security against the dishonest Bob. Furthermore, the security of multi-bit CV-QDS was extended to coherent attacks (Zhang *et al.*, 2024b) by employing one-time universal hashing and advanced DM CV-QKD security proofs (Matsuura *et al.*, 2021).

D. Quantum authentication

The protocol for CV-QA of the physical keys with the aim of entity authentication was proposed in (Nikolopoulos and Diamanti, 2017) based on probing the keys using

coherent states of light and their subsequent homodyne detection. The physical keys are represented by an optical multiple-scattering random medium and are supposed to be physically unclonable as their full characterization involves multiple degrees of freedom. The typical optical entity authentication is then done in two stages, namely enrolment and verification. In the *enrolment* stage, the authority, that distributes the keys, is characterizing the keys by interacting them with various probes (challenges) and recording responses to the challenges along with the parameters of respective probes. In the *verification* stage, the verifier checks the authenticity of the key by challenging the key with randomly chosen probes and comparing the obtained responses to the recorded ones. It was shown that by using quantum probes, the security of the scheme is considerably improved (Nielsen and Chuang, 2012), while CV realization offers advantageous homodyne detection technique (Nikolopoulos and Diamanti, 2017).

The key in the CV quantum entity authentication scheme is represented by a disordered multiple-scattering medium and the setup is largely based on the existing wavefront-shaping techniques for controlling the scattered light (Mosk *et al.*, 2012). The same setup is used to test the enrolment and the verification so that the authority generates a coherent state and uses its smaller fraction as a probe, which is shaped, directed to the key and, after scattering, is collected into a single-mode fiber. The stronger fraction of the initial coherent state is then used as an LO for the quadrature measurement of the collected scattered light on a homodyne detector. Provided that the verification setup is secure (hence, an attacker has no access to it), the protocol is reported to be collision resistant, meaning that it is able to distinguish between two randomly chosen keys, and is sensitive to cloning of the keys (which is assumed to be imperfect), hence being able to distinguish between a cloned key and the original (Nikolopoulos and Diamanti, 2017).

The CV protocol for quantum identity authentication was proposed in (Huang *et al.*, 2011) using Gaussian modulation of squeezed states and homodyne detection in the same setup as Gaussian P&M CV-QKD shown in Fig. 3. Furthermore, the proposed scheme can be combined with QKD to provide authentication and prevent man-in-the-middle attacks (Zeng and Zhang, 2000). The scheme starts with a pre-shared key (possibly a residual key from the previous QKD session), and Alice, acting as a certifying authority, modulates the squeezed signal states, thus encoding the key bits, and sends these to Bob. Bob measures the corresponding quadratures and publicly announces certain outcomes as defined by Alice, who evaluates the fidelity between her and Bob's data. Based on the fidelity, Alice verifies Bob's identity as well as the presence of an eavesdropper.

E. Quantum oblivious transfer

CV one-out-of-two randomized QOT protocol was suggested in the noisy storage model, assuming limited memory capacity of an attacker (Furrer *et al.*, 2018). In this protocol, Alice performs the bit-wise XOR operations $x_0 \oplus s_0$ and $x_1 \oplus s_1$ between the input strings x_0 and x_1 and independent and uniformly distributed outputs s_0 and s_1 , and send the results to Bob. Bob chooses a bit from $\{0, 1\}$, specifying the bit string to be learned, obtains the bit string $\tilde{s}$ and can learn the string x_t by adding $\tilde{s}$ to $x_t \oplus s_t$.

The protocol can be realized using Gaussian-modulated squeezed states of light measured by homodyne detectors in the same setup as shown in Fig. 3 (with $T_{\text{hetB}} \in \{0, 1\}$), but was studied and tested in the EB version as shown in Fig. 4 (with additionally $T_{\text{hetA}} \in \{0, 1\}$). Alice distributes n EPR states, each measured by Alice and Bob using homodyne detectors in one of two randomly chosen orthogonal quadratures. Both parties discretize the measurement outcomes (Bob performs scaling first to compensate for the channel losses), obtaining the n -bit strings Z and Y respectively. Then the parties wait for some pre-defined time to impose coherence requirement on Bob's memory in case he is malicious, and proceed to the classical post-processing, sifting the data (Bob stores the results obtained in compatible and incompatible bases independently) and splitting their strings to obtain correlated and anti-correlated sub-strings. The parties then perform one-way error correction and Bob, after applying the hash function as described by Alice, obtains the bit string $\tilde{s}$.

The correctness of the protocol, imposing uniform distribution of s_0 , s_1 , and the fact that Bob learns the desired string $s_t = \tilde{s}$, is analyzed in the composable security framework. The security of the scheme is shown for honest Bob against malicious Alice without any assumptions on the power of the latter. In the opposite scenario of dishonest Bob, the composable security of the protocol requires additional assumptions on the power of malicious Bob to store quantum states, which is limited in the time delay between the state distribution and the data post-processing. Bob's quantum memory is then modeled as the lossy channel. The security is obtained using the specially derived entropic uncertainty relations for the discretized quadrature observables, which limit Bob's knowledge on Alice's outcomes, and assuming general as well as Gaussian storage operations.

The protocol was tested using TMSV states produced by a balanced coupling of two orthogonally squeezed states generated by parametric down-conversion at 1550 nm and low-noise highly efficient homodyne detectors operating at 100 kHz. The signal and the LO were co-propagated through the variable attenuator simulating the quantum channel. Using optimized data processing and reconciliation, it was shown that in a highly transmitting quantum channel, the rate of the order of 0.1 bits per symbol can be achieved, while for stronger

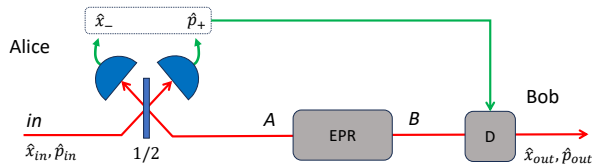


FIG. 11 Generic CV-QT scheme. Alice and Bob share an entangled state in modes A and B (ideally this is a CV EPR state with perfect quadrature correlations; in practice, this is a TMSV state). Alice couples the input state in mode in on a balanced beam splitter with transmittance $1/2$ to the mode A of the entangled state, the outputs $\hat{x}_-$ and $\hat{p}_+$ are measured and results are classically communicated to Bob, who accordingly performs displacement D on mode B of the entangled source to obtain the output state.

losses the results largely depend on the assumptions on the malicious Bob's storage (Furrer *et al.*, 2018).

F. Quantum teleportation

CV-QT was proposed in (Vaidman, 1994) using perfect EPR-type entanglement and extended to finite correlations in (Braunstein and Kimble, 1998), in order to avoid qubit Bell measurements, which are very challenging to implement (Lütkenhaus *et al.*, 1999). In the CV-QT scheme (Braunstein and Kimble, 1998), shown in Fig. 11, Alice and Bob share an entangled state in modes A and B , while the incoming state in mode in , characterized by the quadrature vector $\hat{\mathbf{r}}_{in} = \{\hat{x}_{in}, \hat{p}_{in}\}^T$, is to be teleported. Alice couples modes in and A on a balanced beam splitter and measures quadratures $\hat{x}_-$ and $\hat{p}_+$, performing a CV Bell measurement. The measurement outcomes are classically communicated to Bob, who performs displacement D on the mode B of the shared entangled state and obtains the output state with the quadrature vector $\hat{\mathbf{r}}_{out} = \{\hat{x}_{out}, \hat{p}_{out}\}^T$. In an infinitely strong CV EPR entangled state, the mode quadratures are fully correlated/anti-correlated: $\hat{x}_A = \hat{x}_B, \hat{p}_A = -\hat{p}_B$. Then, in a perfect implementation of the scheme, after values x_-, p_+ of the measured quadratures $\hat{x}_- = (\hat{x}_A - \hat{x}_{in})/\sqrt{2}$ and $\hat{p}_+ = (\hat{p}_A + \hat{p}_{in})/\sqrt{2}$ are sent to Bob, Bob's displacement is simply $\{-x_- \sqrt{2}, p_+ \sqrt{2}\}$ to obtain the output state $\hat{\mathbf{r}}_{out} \equiv \hat{\mathbf{r}}_{in}$, hence perform perfect teleportation with fidelity $F = 1$. Such a unit fidelity cannot be exactly reached in practice, since it would require infinite entanglement, or equivalently, infinite entropy at the local stations, therefore violating holographic bounds (Pirandola, 2024). Thus, finite entanglement resources and setup imperfections limit the quality of CV-QT. Nevertheless, the feasibility of CV Bell measurement allows CV-QT to be performed unconditionally.

In practice, the entangled resource state shared by the parties is a TMSV state. Then, Bob's displacements should be optimized by applying a gain factor to the measurement outcomes communicated by Alice. This helps compensate for the imperfect resource state, increasing

the teleportation fidelity in practical scenarios. Gain tuning was studied and optimized for coherent, vacuum, and single-photon inputs (Ide *et al.*, 2002), with further studies for DV input states under realistic experimental conditions (Takeda *et al.*, 2013). Limited fidelity of CV-QKD was shown to be equivalent to attenuation of the input signal (Hofmann *et al.*, 2000) and is related to information about the signal, obtained from Bell measurement, which should ideally be absent (Hofmann *et al.*, 2001).

Generally, in the case of a mixed input state, the fidelity can be obtained as $F = \text{Tr}(\sqrt{\hat{\rho}_{in}} \hat{\rho}_{out} \sqrt{\hat{\rho}_{in}})$ (Pirandola and Mancini, 2006), averaged over outcomes of the Bell measurement. The expression simplifies to $F = \langle \psi_{in} | \hat{\rho}_{out} | \psi_{in} \rangle$ for the pure input state $\hat{\rho}_{in} = |\psi_{in}\rangle \langle \psi_{in}|$. If the teleportation channel is a Gaussian state with a covariance matrix γ_{AB} of the form (16), and the input state is a pure single-mode Gaussian state with covariance matrix γ_{in} , the fidelity of teleportation with gain of $\sqrt{2}$ can be obtained as an overlap integral between input and output Wigner functions (Fiurášek, 2001):

$$F = 2\pi \int_{-\infty}^{\infty} W_{in}(x, p) W_{out}(x, p) dx dp, \quad (53)$$

which can be expressed as $F = 2/\sqrt{\det \Gamma}$, where the matrix Γ reads

$$\Gamma = 2\gamma_{in} + \gamma_B + \sigma_z \gamma_A \sigma_z - \sigma_z \sigma_{AB} - \sigma_{AB}^T \sigma_z. \quad (54)$$

For a coherent-state input and a TMSV resource state with squeezing r and unity gain, the fidelity is given by $F_{coh} = 1/[1 + \exp(-2r)]$ (Braunstein *et al.*, 2001). While in the case of infinitely strong entanglement $r \rightarrow \infty$ the fidelity approaches 1, in the absence of entanglement, $r = 0$, the fidelity is $F_{coh}^{r=0} = 1/2$, which gives the classical bound on the coherent-state fidelity. Alternatively, quantum cloning (also called quantum duplication) can achieve fidelity of $F = 2/3$, referred to as no-cloning limit (Grosshans and Grangier, 2001). Therefore, in order to not only show the advantage above the classical strategies but also to make sure that the teleported state is better than any cloned copy, QT should overcome the no-cloning limit. Beating the no-cloning limit also indicates that a quantum teleporter is able to preserve the nonclassicality (Wigner negativity) of the teleported states (Ban, 2004).

When the teleported state is a two-mode entangled state itself and the communicating parties do not initially share an entangled resource, but instead, each keeps a mode of their respective entangled mode pairs, while sending the two residual modes to a third party, who performs the Bell quadrature measurement and broadcasts the outputs, the QT scheme changes to CV entanglement swapping (van Loock and Braunstein, 1999; Tan, 1999). The state, shared between Alice and Bob and conditioned on the broadcast Bell measurement outcomes, is now entangled even though the entangled modes never physically interacted. Importantly for quantum communication, entanglement swapping can be a building block for

a CV quantum repeater (Dias and Ralph, 2017). It is also worth mentioning that CV entanglement swapping represents the EB version of the CV-MDI protocol, described in Sec. III.A. It is therefore an ideal setting to study the security of CV-MDI-QKD, similarly to the role that DV entanglement swapping plays in the security of DV-MDI-QKD (Braunstein and Pirandola, 2012).

While QT supposes the teleportation of a quantum state, its experimental test must also include verification, performed by a verifier (often referred to as a third party, Victor), who prepares and characterizes the input state and measures the output state, in order to assess the resulting fidelity. Experimental realization of unconditional CV-QT was first reported in (Furusawa *et al.*, 1998) using two-mode entanglement, produced by parametric down-conversion in an optical parametric oscillator (OPO). The experimental fidelity of coherent-state teleportation of 0.58 ± 0.02 was obtained, confirming the advantage of quantum teleportation over the classical benchmark. Fidelity of 0.61 ± 0.02 (or 0.62 after correcting for the efficiency of the verifying detector) was reported in (Zhang *et al.*, 2003). Teleportation of modulated coherent states was demonstrated in (Bowen *et al.*, 2003) in the experiment with entangled channel state, produced by coupling of two -4.8 dB squeezed states from two OPAs, showing the optimized fidelity of 0.64 ± 0.02 .

The benchmark of no-cloning limit was surpassed in (Takei *et al.*, 2005b), reporting the fidelity of 0.7 ± 0.02 and also demonstrating CV entanglement swapping, verified by confirming the sub-shot noise fluctuations of the quadrature differences of the two residual modes. The experimental scheme was based on two sources of entanglement (by coupling pairs of orthogonally squeezed states produced by four OPOs), measured by four homodyne detectors. Teleportation of a squeezed state with confirmed sub-shot-noise fluctuations on the output was reported in (Takei *et al.*, 2005a) with fidelity 0.85 ± 0.05 , which is above the classical limit for such states, experimentally verified as 0.73 ± 0.04 . Coherent-state teleportation fidelity of 0.83 ± 0.01 was reported in (Yukawa *et al.*, 2008) by using high degrees (-6 dB) of OPO squeezing to produce strong two-mode entanglement, also suggesting sequential teleportation towards advanced quantum information processing.

Teleportation of a nonclassical Schrödinger’s-cat state of superposed coherent states $|\alpha\rangle \pm |-\alpha\rangle$ was reported in (Lee *et al.*, 2011), confirmed by negativity of the Wigner function of the input and output states, characterized by state tomography. Similarly, noiseless teleportation of a single-photon state was confirmed by the Wigner function negativity, as reported in (Fuwa *et al.*, 2014), using loss suppression based on conditioning on the Bell quadrature measurements, resulting in 53% success rate. Long-distance teleportation of a coherent state over 6 km optical fiber was demonstrated in (Huo *et al.*, 2018), reaching fidelity of 0.62 ± 0.03 by means of OPO squeezing of approx. -5.3 dB. The milestone realizations of CV-QT are summarized in Table II.

Reference	Input	F	Prob.
(Furusawa <i>et al.</i> , 1998)	coherent	0.58	1
(Zhang <i>et al.</i> , 2003)	coherent	0.62	1
(Bowen <i>et al.</i> , 2003)	coherent	0.64	1
(Takei <i>et al.</i> , 2005a)	squeezed	0.85	1
(Takei <i>et al.</i> , 2005b)	coherent	0.7	1
(Yukawa <i>et al.</i> , 2008)	coherent	0.83	1
(Lee <i>et al.</i> , 2011)	cat	-	1
(Fuwa <i>et al.</i> , 2014)	single-photon	-	0.53
(Huo <i>et al.</i> , 2018)	coherent	0.62	1
(Zhao <i>et al.</i> , 2023)	coherent	0.92	10^{-5}

TABLE II Milestone bipartite CV-QT demonstrations (in chronological order), input states (coherent, squeezed, single-photon or Schrödinger’s-cat states), achieved fidelities F , and success probabilities (unity meaning unconditional, deterministic teleportation).

Several proposals were made for improving the fidelity of CV-QT with finite resources, such as, e.g., dividing the input state to multiple CV qubit teleporters and recombination of the outputs as suggested in (Andersen and Ralph, 2013). Equivalence between CV-QT with finite resources and single-mode phase-insensitive Gaussian channels was analyzed in (Liuzzo-Scorpo *et al.*, 2017) and used to theoretically optimize the teleportation of Gaussian-modulated coherent states. It was shown that optimal linear-optical operations on the signal and channel modes improve the fidelity and allow it to overcome the classical threshold at any degree of squeezing (Fiurásek, 2001). On the other hand, CV-QT can be used for efficient noiseless linear amplification of coherent states without the need for a single photon addition (Fiurásek, 2022b). Recently a heralded quantum teleporter with -6.5 dB of squeezing and measurement-based NLA was suggested in (Zhao *et al.*, 2023), demonstrating the fidelity of 92% at the cost of success rate of 10^{-5} . Limitations and possibilities of the NLA-based scheme were analyzed in (Fiurásek, 2024). Beyond the optical domain, CV-QT and entanglement swapping were extended to mechanical modes such as the vibrational modes of a mirror (Pirandola *et al.*, 2003, 2006).

Alternatively to employing measurement and feed-forward using respectively homodyne detectors and electro-optical modulators, CV-QT can be performed in all-optical setup using a PIA fed by an EPR state or properly pumped PSAs in an interferometric scheme (Ralph, 1999a), enabling multiplexed realizations of CV-QT (Liu *et al.*, 2020a, 2024) and entanglement swapping (Liu *et al.*, 2022c).

CV-QT was extended in yet other ways. An important multipartite extension was the theoretical development of CV quantum teleportation networks, as proposed by (van Loock and Braunstein, 2000) and experimentally tested in (Wu *et al.*, 2024; Yan *et al.*, 2024; Yonezawa *et al.*, 2004). Another interesting variant is port-based teleportation, originally developed for DV (Ishizaka and Hiroshima, 2008, 2009) and later extended to CV (Pereira

et al., 2023b). In this variant, the parties exploit a multi-copy entanglement source and a multi-system measurement at Alice's side. The scheme is built in a way that Bob does not need to apply any unitary correction but rather to choose a system (or port) for the output state.

As described in (Pirandola *et al.*, 2015a), one can consider four conditions to be met to have an ideal teleportation system: high efficiency (related to the practical success probability of Alice's detection), high average fidelity of the teleported states, distance of teleportation and, finally, the availability of a quantum memory (to store the teleported states). In this context, CV-QT with optical modes represents one of the best choices in terms of efficiency (100%) and fidelity ($> 80\%$). However, challenges remain in terms of extending distance and providing an efficient interface into a quantum memory.

G. GKP encoding

CV quantum states and coherent detection can be also used for encoding and manipulating DV states, hence allowing CV-based operations with DV quantum information. The Gottesman-Kitaev-Preskill (GKP) encoding, which encodes a qudit (state of a finite d -dimensional quantum system, qubit in the case of $d = 2$) into a state of an infinite-dimensional quantum oscillator, described by the field quadratures, was suggested in (Gottesman *et al.*, 2001). It was shown that such encoding, possible with the CV states with finite squeezing, enables efficient error correction, based on conversion of a photon loss by means of a PIA to a correctable Gaussian noise (Albert *et al.*, 2018). This makes the GKP codes particularly useful for fault-tolerant quantum computation.

In the context of quantum communication, the GKP codes were suggested as the basis for efficient quantum repeaters for qubit (Fukui *et al.*, 2021; Rozpędek *et al.*, 2021) and qudit states (Schmidt *et al.*, 2024), using either one- or two-way quantum communication and possibly combining CV and DV error correction codes. Particularly, it was shown that PSA is sufficient for converting losses to Gaussian noise in a two-way protocol and can be applied in the post-processing (Fukui *et al.*, 2021). Furthermore, it was shown that amplification is not needed for correcting channel losses with GKP codes and can be harmful in the relevant parameter regimes (Hastrup and Andersen, 2023).

Recently, GKP encoding was realized on the propagating light at the telecom wavelength (Konno *et al.*, 2024), which opens the pathway to implementation of GKP-based CV quantum repeaters for DV quantum communication.

V. SUMMARY AND OUTLOOK

This review covers the fascinating field of continuous-variable quantum communication, which develops and

studies methods for information transfer using quantum systems, defined on the infinite-dimensional phase space.

Using information encoding into the continuous quadrature observables and its efficient retrieval by means of coherent detection, continuous-variable quantum communication has developed into a widespread quantum technology, complementing discrete-variable methods with high efficiency at the cost of higher sensitivity to effects of the environment. Furthermore, the elegant covariance-matrix formalism, which is directly applicable to the large class of Gaussian states, typically produced in the quantum-optical laboratories, allows for efficient characterization of continuous-variable states and operations as well as their entropic properties, relevant for communication tasks. These features make continuous-variable quantum communication a great tool in numerous applications, starting with the well-known secure quantum key distribution. The review is largely focused on this area of quantum technology, presenting the major protocols, their security proofs, and methods of their practical realization and discussing security aspects of the implementations, which differ from the idealized theoretical models.

We summarize the quantum key distribution protocols based on continuous variables in Table III, covering state generation, modulation, and measurement techniques, equivalent EB representations for security analysis, and the best-known security proofs. Similarly, we summarize the milestone realizations of the protocols in Table IV, presenting the protocol types, security proofs, achieved key rates, system clock rates, and error correction efficiencies. The table illustrates advances in practical CV-QKD since its first experimental test in 2003, both in terms of achievable key rates and distances. The achieved key rates, normalized to the clock rates, are also plotted in Fig. 12 along with the fundamental PLOB bound (solid line), providing the secret-key capacity of the lossy channel, and the asymptotic key rates for GG02 in a perfect noiseless realization (dashed lines) and with finite post-processing efficiency, optimized modulation and the presence of small channel noise (dotted line). It is evident from the plot, that progress in the experimental techniques (particularly, high clock rates, providing large data ensembles, and high system stability and efficient data processing, resulting in lower excess noise levels) allows to strengthen the security assumptions (from asymptotic to composable finite-size security) without degrading the overall performance. However, there is still an evident gap between the practical performance of the protocols and the theoretical bounds, especially at strong channel loss levels, which requires experimental efforts toward even higher stability of the systems and efficient noise compensation methods as well as theoretical developments, particularly for the tight practical security of DM protocols. It is now clear, that the development of practical CV-QKD protocols will largely continue in the direction of discrete-modulation schemes, allowing for much higher repetition rates, while Gaussian-modulated

Protocol	Signal	Modulation	Bob's measurement	Equivalent Alice's preparation	Best known security proof(s)
Squeezed-state (Cerf <i>et al.</i> , 2001)	squeezed	Gaussian	homodyne	homodyne	composable (Furrer, 2014; Furrer <i>et al.</i> , 2012)
GG02 (Grosshans and Grangier, 2002)	coherent	Gaussian	homodyne	heterodyne	collective composable (Pirandola and Papanastasiou, 2024)
No-switching (Weedbrook <i>et al.</i> , 2004)	coherent	Gaussian	heterodyne	heterodyne	composable (Leverrier, 2015)
Thermal (Filip, 2008)	thermal	Gaussian	homodyne	heterodyne + noise	asymptotic collective (Filip, 2008) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
Two-way (Pirandola <i>et al.</i> , 2008c)	coherent/squeezed	Gaussian	homodyne/heterodyne	homodyne/heterodyne	asymptotic collective (Pirandola <i>et al.</i> , 2008c) composable (Ghorai <i>et al.</i> , 2019a)
(García-Patrón and Cerf, 2009)	squeezed	Gaussian	heterodyne	homodyne	asymptotic collective (García-Patrón and Cerf, 2009) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
DM (Leverrier and Grangier, 2011; Ralph, 1999b)	coherent	discrete	homodyne/heterodyne	heterodyne	collective composable (Kanitschar <i>et al.</i> , 2023) composable for QPSK+heterodyne (Bäuml <i>et al.</i> , 2024)
(Weedbrook <i>et al.</i> , 2012b)	thermal	Gaussian	heterodyne	heterodyne + noise	asymptotic collective (Weedbrook <i>et al.</i> , 2012b) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
(Madsen <i>et al.</i> , 2012)	squeezed	Gaussian	homodyne	homodyne modulation	asymptotic collective (Madsen <i>et al.</i> , 2012) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
(Fiurášek and Cerf, 2012)	coherent/squeezed	Gaussian	homodyne/heterodyne + Gaussian post-selection	homodyne/heterodyne	asymptotic collective (Fiurášek and Cerf, 2012) collective for coherent-state & heterodyne (Hosseinidehaj <i>et al.</i> , 2020)
Entanglement-in-the-middle (Weedbrook, 2013)	entangled	-	homodyne/heterodyne	-	finite-size (Guo <i>et al.</i> , 2019)
Unidimensional (Usenko and Grosshans, 2015)	coherent	Gaussian 1D	homodyne	heterodyne squeezing	asymptotic collective (Usenko and Grosshans, 2015) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
(Usenko, 2018)	squeezed	Gaussian 1D	homodyne	homodyne squeezing	asymptotic collective (Usenko, 2018) finite-size collective linear (Leverrier <i>et al.</i> , 2010)
Thermal DM (Papanastasiou and Pirandola, 2021)	thermal	discrete	heterodyne	heterodyne + noise	collective composable (Papanastasiou and Pirandola, 2021)

TABLE III Major trusted-device (non-MDI) CV-QKD protocols and their modifications (in chronological order), used signal states, modulation profiles, receiver (Bob's) measurements, equivalent sender (Alice's) state-preparing measurements in the EB representation plus additional operations on Bob's mode if needed, and the best known security proofs (asymptotic or finite-size unless specified, collective or general attacks unless specified, assumption of channel linearity, proof composability)

protocols with remain the important benchmarks as well as testbeds for advanced tools. Yet, the choice of the best practical CV-QKD protocol remains an open question, especially as its performance strongly depends on the practical security proofs and post-processing techniques, which are being developed (Milicevic *et al.*, 2018; Mountogiannakis *et al.*, 2022).

Despite the attention given to quantum key distribution, continuous-variable quantum communication goes well beyond this field and includes such specific quantum communication tasks as quantum direct communication, quantum super-dense coding, quantum digital signatures, quantum authentication, and quantum oblivious transfer. These tasks, although less mature than quantum key distribution, are only part of the plethora of novel communication methods offered by continuous-variable quantum technology. Many more tasks will likely be developed with the advances of quantum-optical technologies, while the existing ones will proceed to full-scale implementations, in-field tests, and possible further industrialization, similar to quantum key distribution. On the other hand, continuous-variable quantum teleportation, which has demonstrated impressive theoretical and experimental progress in the last 25 years, will benefit from long-distance implementation and hybrid integration with other systems capable of quantum storage, e.g., atomic ensembles (Sherson *et al.*, 2006).

In our review, we have limited the discussion to bipartite quantum communication (only including third parties by the protocol design, such as in the case of quantum digital signatures). However, continuous-variable quantum communication is being naturally developed toward quantum networking, e.g., with the recent results in multi-user quantum key distribution (Hajomer *et al.*, 2024a) and the generation of multipartite entanglement (Asavanant and Furusawa, 2024) for continuous variable teleportation networks. In parallel to this development, continuous-variable quantum communication will benefit from methods aimed at improving its efficiency, such as quantum repeaters or multiplexing, as well as from technological advances such as photonic integration, hybrid and satellite-based realizations, aimed at reducing the cost and making the technology more applicable and broadly available. Continuous-variable quantum communication remains an active field of research despite its immense progress in the past decades, and this review will hopefully encourage and stimulate this development.

Acknowledgments

The authors acknowledge insightful discussions with Radim Filip, Anthony Leverrier, Norbert Lütkenhaus, and Christoph Marquardt, and thank Jaromír Fiurášek, Cameron Foreman, Andrew Lance, Gui-Lu Long, Andrey Rakhubovsky, Lev Vaidman, and Qi Wu for the feedback on the manuscript. This project has received fund-

ing from the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, grant agreement No 101114043). V.C.U. acknowledges project 21-44815L of the Czech Science Foundation and project CZ.02.01.01/00/22_008/0004649 (QUEENTEC) of the Czech Ministry of Education, Youth and Sports (MEYS). A.A.E.H., T.G., and U.L.A. acknowledge projects CryptQ 0175-00018A and CyberQ 3200-00035A of Innovation Fund Denmark, projects bigQ and DNRF142 of DNRF, and project 0171-00055B of Danmarks Frie Forskningsfond. V.C.U., A.A.E.H., T.G., U.L.A., C.P., and F.K. acknowledge QuantERA project CVSTAR, which has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no. 731473, the Czech MEYS, project number 8C22002, Innovation Fund Denmark under Grant Agreement no. 101017733, and the Austrian Research Promotion Agency, project number FO999891361. E.D. and R.A. acknowledge the PEPR integrated project QCommTestbed (ANR-22-PETQ-0011), which is part of Plan France 2030. A.A. acknowledges support from the Government of Spain (Severo Ochoa CEX2019-000910-S, NextGenerationEU PRTR-C17.I1 and FUNQIP), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA program), the ERC AdG CERQUTE, and the AXA Chair in Quantum Information Science. S.P. acknowledges support from EPSRC and UKRI, via the grants EP/M013472/1, EP/T001011/1, and the "Integrated Quantum Networks Research Hub" (IQN, EP/Z533208/1).

References

- Abidin, A., and J.-Å. Larsson, 2012, in *Research in Cryptology: 4th Western European Workshop, WEWoRC 2011, Weimar, Germany, July 20-22, 2011, Revised Selected Papers 4* (Springer), pp. 99–108.
- Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, 2007, *Physical Review Letters* **98**(23), 230501.
- Adesso, G., S. Ragy, and A. R. Lee, 2014, *Open Systems & Information Dynamics* **21**(01n02), 1440001.
- Albert, V. V., K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang, 2018, *Physical Review A* **97**(3), 032346.
- Aldama, J., S. Sarmiento, S. Etcheverry, I. López Grande, L. Trigo Vidarte, L. Castelfvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri, 2023, in *Optical Fiber Communication Conference (OFC) 2023* (Optica Publishing Group), OFC, p. M1L.3.
- Aldama, J., S. Sarmiento, I. H. Lopez Grande, S. Signorini, L. T. Vidarte, and V. Pruneri, 2022, *Journal of Lightwave Technology* **40**(23), 7498.
- Andersen, U. L., T. Gehring, C. Marquardt, and G. Leuchs, 2016, *Physica Scripta* **91**(5), 053001.
- Andersen, U. L., and T. C. Ralph, 2013, *Physical Review Letters* **111**(5), 050504.
- Araki, H., and E. H. Lieb, 1970, *Communications in Mathematical Physics* **18**(2), 160.

Reference	Protocol	Security	Clock	Keyrate	Channel	β
1. (Grosshans <i>et al.</i> , 2003b)	GG02	individual, asymptotic	0.8 MHz	75 Kbps	- / 3 dB	-
2. (Lodewyck <i>et al.</i> , 2007)	GG02	collective, asymptotic	0.35 MHz	2 Kbps	25 km / 5 dB	90%
3. (Fossier <i>et al.</i> , 2009b)	GG02	collective, asymptotic	0.5 MHz	8 Kbps	15 km / 3 dB	90%
4. (Jouguet <i>et al.</i> , 2013b)	GG02	collective, finite-size	1 MHz	10 Kbps 2 Kbps 0.2 Kbps	25 km / 5 dB 53 km / 11 dB 80 km / 16 dB	95%
5. (Huang <i>et al.</i> , 2015a)	GG02+LLO	collective, finite-size	100 MHz	100 Kbps	25 km / 5 dB	97%
6. (Gehring <i>et al.</i> , 2015)	squeezed	coherent, composable, finite-size	100 kHz	10 Kbps	- / 0.8 dB	94.3%
7. (Huang <i>et al.</i> , 2015c)	GG02	collective, finite-size	50 MHz	1 Mbps	25 km / 5 dB	93%
8. (Huang <i>et al.</i> , 2016)	GG02	collective, finite-size	2 MHz	0.5 Kbps	100 km / 20 dB	95.6%
9. (Zhang <i>et al.</i> , 2020)	GG02	collective, finite-size	5 MHz	0.3 Kbps 6 bps	140 km / 23 dB 200 km / 32 dB	96% 98%
10. (Jain <i>et al.</i> , 2022)	GG02+LLO	collective, composable, finite-size	100 MHz	4.7 Mbps	20 km / 4 dB	94.3%
11. (Tian <i>et al.</i> , 2023)	DM+LLO	collective, asymptotic	2.5 GHz	49 Mbps 12 Mbps 2 Mbps	25 km / 5 dB 50 km / 10 dB 80 km / 16 dB	95%
12. (Hajomer <i>et al.</i> , 2024b)	DM+LLO	collective, asymptotic	10 GHz	0.7 Gbps 0.3 Gbps	5 km / 1 dB 10 km / 2 dB	95%
13. (Hajomer <i>et al.</i> , 2024c)	GG02+LLO	collective, finite-size	100 MHz	25 Kbps	100 km / 15 dB	92.5%
14. (Roumestan <i>et al.</i> , 2024)	DM	collective, finite-size	1 GHz	92 Mbps 24 Mbps	10 km / 2 dB 25 km / 5 dB	-
15. (Jaksch <i>et al.</i> , 2024)	DM	collective, composable, finite-size	25 MHz	375 Kbps	- / 3 dB	89%
16. (Hajomer <i>et al.</i> , 2025b)	DM+LLO	collective, composable, finite-size	125 MHz	1.3 Mbps	20 km / 5 dB	87.8%

TABLE IV Milestone trusted-device (non-MDI) CV-QKD tests and implementations (in chronological order), used protocols as referred to in Table III (LLO indicated where used), used security proofs, system clock rates, achieved key rates, channel distances in kilometers / loss levels in dB, and error correction efficiency β .

Araújo, M., M. Huber, M. Navascués, M. Pivoluska, and A. Tavakoli, 2023, *Quantum* **7**, 1019.
Asavanant, W., and A. Furusawa, 2024, *Physical Review A* **109**(4), 040101.
Aspect, A., P. Grangier, and G. Roger, 1982, *Physical Review Letters* **49**(2), 91.
Aymeric, R., Y. Jaouën, C. Ware, and R. Alléaume, 2022, in *Optical Fiber Communication Conference* (Optica Publishing Group), pp. W2A–37.
Ban, M., 1999, *Journal of Optics B: Quantum and Semiclassical Optics* **1**(6), L9.
Ban, M., 2000, *Physics Letters A* **276**(5–6), 213.
Ban, M., 2004, *Physical Review A* **69**(5), 054304.
Barnett, S. M., 2009, *Quantum information*, Oxford master series in atomic, optical and laser physics (Oxford Univ. Pr., Oxford [u.a.]), 1. publ. edition, ISBN 0198527624.
Barnum, H., C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, 2002, in *The 43rd Annual IEEE Symposium*

on Foundations of Computer Science, 2002. Proceedings. (IEEE Comput. Soc), SFCS-02.
Bäuml, S., C. Pascual-García, V. Wright, O. Fawzi, and A. Acín, 2024, *Quantum* **8**, 1418.
Beige, A., B. Englert, C. Kurtsiefer, and H. Weinfurter, 2002, *Acta Physica Polonica A* **101**(3), 357.
Ben-Or, M., M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, 2005, in *Theory of Cryptography*, edited by J. Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 386–406, ISBN 978-3-540-30576-7.
Ben-Or, M., and D. Mayers, 2004, arXiv:quant-ph/0409062 .
Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992a, *Journal of Cryptology* **5**(1), 3.
Bennett, C. H., and G. Brassard, 1984, in *Proceedings of International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore, India), volume 175, p. 9.
Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, *Physical Review Letters* **70**(13),

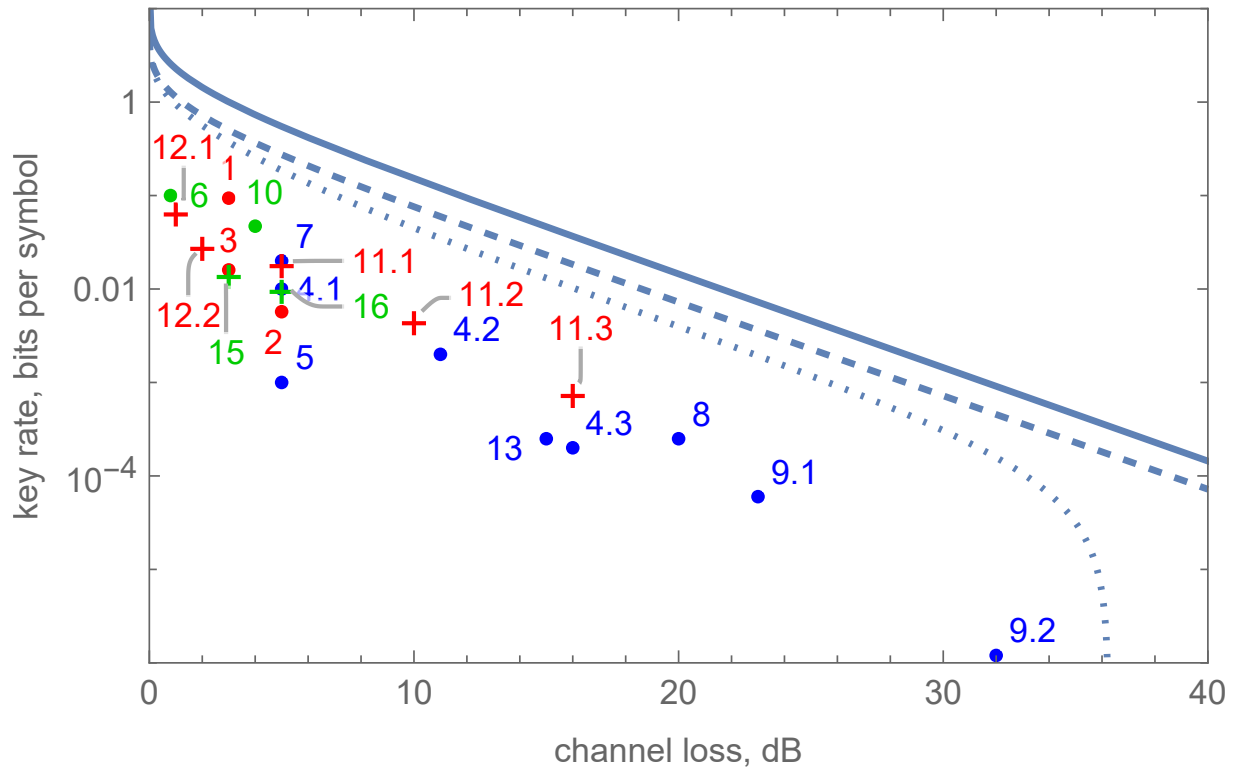


FIG. 12 Secret key rates in bits per symbol (bits per channel use) versus respective channel loss in dB, achieved in the milestone CV-QKD demonstrations as summarized in Table IV and numbered accordingly. Red points: asymptotic security; blue points: finite-size security; green points: composable finite-size security. Circles: Gaussian modulation, crosses with call-out labels: discrete modulation. Solid line: PLOB bound (Pirandola *et al.*, 2017); dashed line: key rate for GG02 protocol (Grosshans and Grangier, 2002) with perfect post-processing ($\beta = 1$) and strong modulation ($V_M = 10^3$ SNU) in a purely lossy (noiseless) channel; dotted line: GG02 protocol with practical error correction efficiency $\beta = 95\%$, optimized modulation (of the order of few SNU) and excess noise on the channel output $\nu_{\text{out}} = 10^{-5}$ SNU.

- 1895.
- Bennett, C. H., G. Brassard, C. Crépeau, and U. M. Maurer, 1995, *IEEE Transactions on Information theory* **41**(6), 1915.
- Bennett, C. H., G. Brassard, C. Crépeau, and M.-H. Skubiszewska, 1992b, *Practical Quantum Oblivious Transfer* (Springer Berlin Heidelberg), ISBN 9783540551881, pp. 351–366.
- Bennett, C. H., G. Brassard, and N. D. Mermin, 1992c, *Physical Review Letters* **68**(5), 557.
- Bennett, C. H., and S. J. Wiesner, 1992, *Physical Review Letters* **69**(20), 2881.
- Bian, Y., Y. Li, X. Xu, T. Zhang, Y. Pan, W. Huang, S. Yu, L. Zhang, Y. Zhang, and B. Xu, 2024a, *Optics Letters* **49**(9), 2521.
- Bian, Y., Y. Pan, X. Xu, L. Zhao, Y. Li, W. Huang, L. Zhang, S. Yu, Y. Zhang, and B. Xu, 2024b, *Applied Physics Letters* **124**(17), 174001.
- Blandino, R., A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Broui, 2012, *Physical Review A* **86**(1), 012327.
- Boschi, D., S. Branca, F. De Martini, L. Hardy, and S. Popescu, 1998, *Physical Review Letters* **80**(6), 1121.
- Boström, K., and T. Felbinger, 2002, *Physical Review Letters* **89**(18), 187902.
- Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, 1997, *Nature* **390**(6660), 575.
- Bowen, W. P., N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H.-A. Bachor, T. Symul, and P. K. Lam, 2003, *Physical Review A* **67**(3), 032302.
- Boyd, R. W., 2020, *Nonlinear Optics* (Elsevier), ISBN 9780128110027.
- Brádler, K., and C. Weedbrook, 2018, *Physical Review A* **97**(2), 022310.
- Branciard, C., E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, 2012, *Physical Review A* **85**(1), 010301.
- Brassard, G., N. Lütkenhaus, T. Mor, and B. C. Sanders, 2000, *Physical Review Letters* **85**(6), 1330.
- Braunstein, S. L., C. A. Fuchs, H. J. Kimble, and P. van Loock, 2001, *Physical Review A* **64**(2), 022321.
- Braunstein, S. L., and H. J. Kimble, 1998, *Physical Review Letters* **80**(4), 869.
- Braunstein, S. L., and H. J. Kimble, 2000, *Physical Review A* **61**(4), 042302.
- Braunstein, S. L., and S. Pirandola, 2012, *Physical Review Letters* **108**(13), 130502.
- Braunstein, S. L., and P. Van Loock, 2005, *Reviews of Modern Physics* **77**(2), 513.
- Brunner, H. H., S. Bettelli, C.-H. F. Fung, and M. Peev, 2020, in *2020 22nd International Conference on Transparent Optical Networks (ICTON)* (IEEE), pp. 1–4.

- Bruynsteen, C., M. Vanhovecke, J. Bauwelinck, and X. Yin, 2021, *Optica* **8**(9), 1146.
- Campbell, E. T., and J. Eisert, 2012, *Physical Review Letters* **108**(2), 020501.
- Canetti, R., 2000, *J. Cryptol.* **13**(1), 143.
- Canetti, R., 2001, in *FOCS* (IEEE Computer Society), pp. 136–145, ISBN 0-7695-1390-5.
- Cao, Z., L. Wang, K. Liang, G. Chai, and J. Peng, 2021, *Physical Review Applied* **16**(2), 024012.
- Cattaneo, M., M. G. A. Paris, and S. Olivares, 2018, *Physical Review A* **98**(1), 012333.
- Cerf, N. J., M. Levy, and G. Van Assche, 2001, *Physical Review A* **63**(5), 052311.
- Chai, G., Z. Cao, W. Liu, M. Zhang, K. Liang, and J. Peng, 2019, *Laser Physics Letters* **16**(9), 095207.
- Chai, G., P. Huang, Z. Cao, and G. Zeng, 2020, *New Journal of Physics* **22**(10), 103009.
- Chailloux, A., I. Kerenidis, and J. Sikora, 2010, arXiv:quant-ph/1007.1875 .
- Chen, Z., X. Wang, S. Yu, Z. Li, and H. Guo, 2023, *npj Quantum Information* **9**(1), 28.
- Chin, H., U. Andersen, and T. Gehring, 2024, *Optical Fiber Communication Conference (OFC) 2024, Technical Digest Series* (Optica Publishing Group, 2024) , M3H.4.
- Chin, H.-M., N. Jain, U. L. Andersen, D. Zibar, and T. Gehring, 2022, *Quantum Science and Technology* **7**(4), 045006.
- Chin, H.-M., N. Jain, D. Zibar, U. L. Andersen, and T. Gehring, 2021, *npj Quantum Information* **7**(1), 20.
- Christ, A., C. Lupo, and C. Silberhorn, 2012, *New Journal of Physics* **14**(8), 083007.
- Christandl, M., R. König, and R. Renner, 2009, *Physical Review Letters* **102**(2), 020504.
- Chrzanowski, H. M., N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, 2014, *Nature Photonics* **8**(4), 333.
- Clarke, P. J., R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, 2012, *Nature Communications* **3**(1), 1174.
- Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt, 1969, *Physical Review Letters* **23**(15), 880.
- Coles, P. J., E. M. Metodiev, and N. Lütkenhaus, 2016, *Nature Communications* **7**, 11712.
- Collins, R. J., R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, 2014, *Physical Review Letters* **113**(4), 040502.
- Crépeau, C., and L. Salvail, 1995, *Quantum Oblivious Mutual Identification* (Springer Berlin Heidelberg), ISBN 9783540492641, pp. 133–146.
- Croal, C., C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, 2016, *Physical Review Letters* **117**(10), 100503.
- Csiszár, I., and J. Körner, 1978, *Information Theory, IEEE Transactions on* **24**(3), 339.
- Curty, M., and D. J. Santos, 2001, *Physical Review A* **64**(6), 062309.
- Deng, F.-G., and G. L. Long, 2004, *Physical Review A* **69**(5), 052319.
- Deng, F.-G., G. L. Long, and X.-S. Liu, 2003, *Physical Review A* **68**(4), 042317.
- Denys, A., P. Brown, and A. Leverrier, 2021, *Quantum* **5**, 540.
- Dequal, D., L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, 2021, *npj Quantum Information* **7**(1), 3.
- Derkach, I., and V. C. Usenko, 2020, *Entropy* **23**(1), 55.
- Derkach, I., V. C. Usenko, and R. Filip, 2016, *Physical Review A* **93**(3), 032309.
- Derkach, I., V. C. Usenko, and R. Filip, 2017, *Physical Review A* **96**(6), 062309.
- Derkach, I., V. C. Usenko, and R. Filip, 2020, *New Journal of Physics* **22**(5), 053006.
- Devetak, I., and A. Winter, 2005, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* **461**(2053), 207.
- Diamanti, E., A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, and A. a. Yáñez, 2024, arXiv:2406.09110 .
- Diamanti, E., and A. Leverrier, 2015, *Entropy* **17**(9), 6072.
- Dias, J., and T. C. Ralph, 2017, *Physical Review A* **95**(2), 022312.
- Dias, J., M. S. Winnel, N. Hosseini, and T. C. Ralph, 2020, *Physical Review A* **102**(5), 052425.
- Dong, R., M. Lassen, J. Heersink, C. Marquardt, R. Filip, G. Leuchs, and U. L. Andersen, 2010, *Physical Review A* **82**(1), 012312.
- Dowling, J. P., and G. J. Milburn, 2003, *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **361**(1809), 1655.
- Du, S., Y. Tian, and Y. Li, 2020, *Physical Review Applied* **14**(2), 024013.
- Dunjko, V., P. Wallden, and E. Andersson, 2014, *Physical Review Letters* **112**(4), 040502.
- Dupuis, F., and O. Fawzi, 2019, *IEEE Transactions on Information Theory* **65**(11), 7596.
- Dupuis, F., O. Fawzi, and R. Renner, 2020, *Communications in Mathematical Physics* **379**(3), 867.
- Dušek, M., O. Haderka, M. Hendrych, and R. Myška, 1999, *Physical Review A* **60**(1), 149.
- Eberle, T., V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, and R. F. Werner, 2013, *New Journal of Physics* **15**(5), 053049.
- Eisert, J., S. Scheel, and M. B. Plenio, 2002, *Physical Review Letters* **89**(13), 137903.
- Ekert, A. K., 1991, *Physical Review Letters* **67**(6), 661.
- Eriksson, T. A., T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luis, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, 2019a, *Communications Physics* **2**(1), 9.
- Eriksson, T. A., R. S. Luis, B. J. Puttnam, G. Rademacher, M. Fujiwara, Y. Awaji, H. Furukawa, N. Wada, M. Takeoka, and M. Sasaki, 2020, *Journal of Lightwave Technology* **38**(8), 2214.
- Eriksson, T. A., B. J. Puttnam, G. Rademacher, R. S. Luis, M. Fujiwara, M. Takeoka, Y. Awaji, M. Sasaki, and N. Wada, 2019b, *IEEE Photonics Technology Letters* **31**(6), 467.
- Fan, L., Y. Bian, M. Wu, Y. Zhang, and S. Yu, 2023, *Physical Review Applied* **20**(2), 024073.
- Filip, R., 2008, *Physical Review A* **77**(2), 022310.
- Fiurášek, J., 2001, *Physical Review Letters* **86**(21), 4942.
- Fiurášek, J., 2002, *Physical Review Letters* **89**(13), 137904.
- Fiurášek, J., 2010, *Physical Review A* **82**(4), 042331.
- Fiurášek, J., 2022a, *Physical Review A* **105**(6), 062425.
- Fiurášek, J., 2022b, *Optics Express* **30**(2), 1466.
- Fiurášek, J., 2024, *Optics Express* **32**(2), 2527.
- Fiurášek, J., and N. J. Cerf, 2012, *Physical Review A* **86**(6), 060302.

- Fossier, S., E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, 2009a, *Journal of Physics B* **42**(11), 114014.
- Fossier, S., E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, 2009b, *New Journal of Physics* **11**(4), 045023.
- Frank, M., and P. Wolfe, 1956, *Nav. Res. Logist. Q.* **3**(1-2), 95.
- Fregona, G., C. De Lazzari, D. Giani, F. Chirici, F. Stocco, E. Signorini, G. Morgari, T. Occhipinti, A. Zavatta, and D. Bacco, 2024, *Authentication Methods for Quantum Key Distribution: Challenges and Perspectives* (IOS Press), ISBN 9781643684994.
- Fröhlich, B., J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, 2013, *Nature* **501**(7465), 69.
- Fukui, K., R. N. Alexander, and P. van Loock, 2021, *Physical Review Research* **3**(3), 033118.
- Furrer, F., 2014, *Phys. Rev. A* **90**(4), 042325.
- Furrer, F., T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, 2012, *Physical Review Letters* **109**(10), 100502.
- Furrer, F., T. Gehring, C. Schaffner, C. Pacher, R. Schnabel, and S. Wehner, 2018, *Nature Communications* **9**(1), 1450.
- Furrer, F., and W. J. Munro, 2018, *Physical Review A* **98**(3), 032335.
- Furusawa, A., J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, 1998, *Science* **282**(5389), 706.
- Fuwa, M., S. Toba, S. Takeda, P. Marek, L. Mišta, R. Filip, P. van Loock, J.-i. Yoshikawa, and A. Furusawa, 2014, *Physical Review Letters* **113**(22), 223602.
- García-Patrón, R., 2007, Ph.D. thesis (Université Libre de Bruxelles) .
- García-Patrón, R., and N. J. Cerf, 2006, *Physical Review Letters* **97**(19), 190503.
- García-Patrón, R., and N. J. Cerf, 2009, *Physical Review Letters* **102**(13), 130501.
- García-Patrón, R., S. Pirandola, S. Lloyd, and J. H. Shapiro, 2009, *Phys. Rev. Lett.* **102**, 210501.
- Gehring, T., V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, 2015, *Nature communications* **6**, 8795.
- Ghalaii, M., C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, 2020a, *IEEE Journal on Selected Areas in Communications* **38**(3), 506.
- Ghalaii, M., C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, 2020b, *IEEE Journal of Selected Topics in Quantum Electronics* **26**(3), 1.
- Ghalaii, M., P. Papanastasiou, and S. Pirandola, 2022, *npj Quantum Inf* **8**, 105.
- Ghalaii, M., and S. Pirandola, 2023, *Phys. Rev. A* **108**, 042621.
- Ghorai, S., E. Diamanti, and A. Leverrier, 2019a, *Physical Review A* **99**(1), 012311.
- Ghorai, S., P. Grangier, E. Diamanti, and A. Leverrier, 2019b, *Physical Review X* **9**(2), 021059.
- Gilbert, E. N., F. J. MacWilliams, and N. J. Sloane, 1974, *Bell System Technical Journal* **53**(3), 405.
- Gisin, N., S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, 2006, *Physical Review A* **73**(2), 022320.
- Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, *Reviews of Modern Physics* **74**(1), 145.
- Gisin, N., and R. Thew, 2007, *Nature Photonics* **1**(3), 165.
- Gottesman, D., and I. Chuang, 2001, *arXiv:quant-ph/0105032* .
- Gottesman, D., A. Kitaev, and J. Preskill, 2001, *Physical Review A* **64**(1), 012310.
- Gottesman, D., and J. Preskill, 2001, *Physical Review A* **63**(2), 022309.
- Grant, M., and S. Boyd, 2008, in *Recent Advances in Learning and Control*, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag Limited), Lecture Notes in Control and Information Sciences, pp. 95–110.
- Grant, M., and S. Boyd, 2014, CVX: Matlab software for disciplined convex programming, version 2.1, <http://cvxr.com/cvx>.
- Grosshans, F., 2005, *Physical Review Letters* **94**(2), 020504.
- Grosshans, F., N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, 2003a, *Quantum Info. Comput.* **3**(7), 535.
- Grosshans, F., and P. Grangier, 2001, *Physical Review A* **64**(1), 010301.
- Grosshans, F., and P. Grangier, 2002, *Physical Review Letters* **88**(5), 057902.
- Grosshans, F., G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, 2003b, *Nature* **421**(6920), 238.
- Guo, Y., Y. Su, J. Zhou, L. Zhang, and D. Huang, 2019, *Chinese Physics B* **28**(1), 010305.
- Hajomer, A. A., I. Derkach, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, 2024a, *Light: Science & Applications* **13**(1), 291.
- Hajomer, A. A., H. Q. Nguyen, and T. Gehring, 2022a, *arXiv:2210.07576* .
- Hajomer, A. A. E., U. L. Andersen, and T. Gehring, 2025a, *Quantum Science and Technology* **10**(2), 025032.
- Hajomer, A. A. E., C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, 2024b, *Optica* **11**(9), 1197.
- Hajomer, A. A. E., I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, 2024c, *Science Advances* **10**(1), eadi9474.
- Hajomer, A. A. E., N. Jain, H. Mani, H.-M. Chin, U. L. Andersen, and T. Gehring, 2022b, *npj Quantum Information* **8**, 136.
- Hajomer, A. A. E., F. Kanitschar, N. Jain, M. Hentschel, R. Zhang, N. Lütkenhaus, U. L. Andersen, C. Pacher, and T. Gehring, 2025b, *Light: Science & Applications* **14**(1).
- Häsel, H., T. Moroder, and N. Lütkenhaus, 2008, *Physical Review A* **77**(3), 032303.
- Hastrup, J., and U. L. Andersen, 2023, *Physical Review A* **108**(5), 052413.
- Hayashi, M., and T. Tsurumaru, 2016, *IEEE Transactions on Information Theory* **62**(4), 2213.
- Heid, M., and N. Lütkenhaus, 2006, *Physical Review A* **73**(5), 052316.
- Herrero-Collantes, M., and J. C. Garcia-Escartin, 2017, *Reviews of Modern Physics* **89**(1), 015004.
- Hillery, M., 2000, *Physical Review A* **61**(2), 022309.
- Hofmann, H., T. Ide, T. Kobayashi, and A. Furusawa, 2000, *Physical Review A* **62**(6), 062304.
- Hofmann, H. F., T. Ide, T. Kobayashi, and A. Furusawa, 2001, *Physical Review A* **64**(4), 040301.
- Hong, C. h., J. Heo, J. G. Jang, and D. Kwon, 2017, *Quantum Information Processing* **16**(10), 236.
- Hosseini-dehaj, N., A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, 2020, *Physical Review A* **101**(5), 052335.
- Hosseini-dehaj, N., N. Walk, and T. C. Ralph, 2021, *Physical Review A* **103**(1), 012605.
- Hu, J.-Y., B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q.

- Qin, and G.-L. Long, 2016, *Light: Science & Applications* **5**(9), e16144, ISSN 2047-7538.
- Hu, X.-M., Y. Guo, B.-H. Liu, C.-F. Li, and G.-C. Guo, 2023, *Nature Reviews Physics* **5**(6), 339.
- Huang, D., P. Huang, D. Lin, C. Wang, and G. Zeng, 2015a, *Optics Letters* **40**(16), 3695.
- Huang, D., P. Huang, D. Lin, C. Wang, and G. Zeng, 2015b, *Optics Letters* **40**(16), 3695.
- Huang, D., P. Huang, D. Lin, and G. Zeng, 2016, *Scientific reports* **6**, 19201.
- Huang, D., D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, 2015c, *Optics express* **23**(13), 17511.
- Huang, J.-Z., S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, 2014, *Physical Review A* **89**(3), 032304.
- Huang, J.-Z., C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, 2013, *Physical Review A* **87**(6), 062329.
- Huang, P., J. Zhu, Y. Lu, and G.-H. Zeng, 2011, *International Journal of Quantum Information* **09**(02), 701.
- Huo, M., J. Qin, J. Cheng, Z. Yan, Z. Qin, X. Su, X. Jia, C. Xie, and K. Peng, 2018, *Science Advances* **4**(10), eaas9401.
- Hwang, W.-Y., 2003, *Physical Review Letters* **91**(5), 057901.
- Ide, T., H. F. Hofmann, A. Furusawa, and T. Kobayashi, 2002, *Physical Review A* **65**(6), 062303.
- Ishizaka, S., and T. Hiroshima, 2008, *Phys. Rev. Lett.* **101**, 240501.
- Ishizaka, S., and T. Hiroshima, 2009, *Phys. Rev. A* **79**, 042306.
- Jacobsen, C. S., L. S. Madsen, V. C. Usenko, R. Filip, and U. L. Andersen, 2018, *npj Quantum Information* **4**(1), 32.
- Jain, N., H.-M. Chin, A. Hajomer, D. Null, H. Larfort, N. Nysom, E. Bidstrup, U. Andersen, and T. Gehring, 2024, *Optics Express* **32**, 43607.
- Jain, N., H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, *et al.*, 2022, *Nature Communications* **13**(1), 4740.
- Jain, N., I. Derkach, H.-M. Chin, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, 2021, *Quantum Science and Technology* **6**(4), 045001.
- Jaksch, K., T. Dirmeier, Y. Weiser, S. Richter, O. Bayraktar, B. Hacker, M. Rösler, I. Khan, S. Petscharning, T. Grafenauer, M. Hentschel, B. Ömer, *et al.*, 2024, arXiv:2410.12915.
- Jia, Y., X. Wang, X. Hu, X. Hua, Y. Zhang, X. Guo, S. Zhang, X. Xiao, S. Yu, J. Zou, and Y. Li, 2023, *New Journal of Physics* **25**(10), 103030.
- Johnson, S. J., A. M. Lance, L. Ong, M. Shirvanimoghaddam, T. C. Ralph, and T. Symul, 2017, *New Journal of Physics* **19**(2), 023003.
- Jouguet, P., D. Elkouss, and S. Kunz-Jacques, 2014, *Physical Review A* **90**(4), 042329.
- Jouguet, P., and S. Kunz-Jacques, 2014, *Quantum Information & Computation* **14**(3-4), 329.
- Jouguet, P., S. Kunz-Jacques, and E. Diamanti, 2013a, *Physical Review A* **87**(6), 062313.
- Jouguet, P., S. Kunz-Jacques, E. Diamanti, and A. Leverrier, 2012, *Physical Review A* **86**(3), 032309.
- Jouguet, P., S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, 2013b, *Nature Photonics* **7**(5), 378.
- Kanitschar, F., I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, 2023, *PRX Quantum* **4**, 040306.
- Kanitschar, F., and C. Pacher, 2022, *Phys. Rev. Appl.* **18**, 034073.
- Kanitschar, F., and C. Pacher, 2024, arXiv:2406.14610.
- Kanitschar, F. P., 2021, Master thesis (TU Wien) URL <https://repositum.tuwien.at/handle/20.500.12708/18394>.
- Kashiwazaki, T., T. Yamashima, K. Enbutsu, T. Kazama, A. Inoue, K. Fukui, M. Endo, T. Umeki, and A. Furusawa, 2023, *Applied Physics Letters* **122**(23), 234003.
- Kaur, E., S. Guha, and M. M. Wilde, 2021, *Physical Review A* **103**(1), 012412.
- Kiktenko, E. O., A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, and A. K. Fedorov, 2020, *IEEE Transactions on Information Theory* **66**(10), 6354.
- Kilian, J., 1988, in *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88* (ACM Press), STOC '88.
- Kleis, S., M. Rueckmann, and C. G. Schaeffer, 2017, *Optics Letters* **42**(8), 1588.
- Kleis, S., and C. G. Schaeffer, 2019, *Journal of Lightwave Technology* **37**(3), 722.
- König, R., R. Renner, A. Bariska, and U. Maurer, 2007, *Phys. Rev. Lett.* **98**, 140502.
- Konno, S., W. Asavanant, F. Hanamura, H. Nagayoshi, K. Fukui, A. Sakaguchi, R. Ide, F. China, M. Yabuno, S. Miki, H. Terai, K. Takase, *et al.*, 2024, *Science* **383**(6680), 289.
- Korzh, B., C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, 2015, *Nature Photonics* **9**(3), 163.
- Kovalenko, O., Y.-S. Ra, Y. Cai, V. C. Usenko, C. Fabre, N. Treps, and R. Filip, 2021, *Photonics Research* **9**(12), 2351.
- Kovalenko, O., K. Y. Spasibko, M. V. Chekhova, V. C. Usenko, and R. Filip, 2019, *Optics Express* **27**(25), 36154.
- Kumar, R., F. Mazzoncini, H. Qin, and R. Alléaume, 2021, *Scientific reports* **11**(1), 9564.
- Kumar, R., H. Qin, and R. Alléaume, 2015, *New Journal of Physics* **17**(4), 043027.
- Kumar, R., X. Tang, A. Wonfor, R. Pentty, and I. White, 2019, *Journal of the Optical Society of America B* **36**(3), B109.
- Kunz-Jacques, S., and P. Jouguet, 2015, *Physical Review A* **91**(2), 022307.
- Lasota, M., R. Filip, and V. C. Usenko, 2017, *Physical Review A* **95**(6), 062312.
- Lasota, M., O. Kovalenko, and V. C. Usenko, 2023, *New Journal of Physics* **25**(12), 123003.
- Laudenbach, F., C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, 2018, *Advanced Quantum Technologies* **1**(1), 1800011.
- Laudenbach, F., B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, 2019, *Quantum* **3**, 193.
- Lee, N., H. Benichi, Y. Takeda, S. Takeda, J. Webb, E. Huntington, and A. Furusawa, 2011, *Science* **332**(6027), 330.
- Leverrier, A., 2015, *Phys. Rev. Lett.* **114**, 070501.
- Leverrier, A., 2017, *Physical Review Letters* **118**(20), 200501.
- Leverrier, A., R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, 2008, *Physical Review A* **77**(4), 042325.
- Leverrier, A., and P. Grangier, 2009, *Physical Review Letters* **102**(18), 180504.
- Leverrier, A., and P. Grangier, 2011, *Physical Review A*

- 83**(4), 042312.
- Leverrier, A., F. Grosshans, and P. Grangier, 2010, *Physical Review A* **81**(6), 062343.
- Leverrier, A., E. Karpov, P. Grangier, and N. J. Cerf, 2009, *New Journal of Physics* **11**(11), 115009.
- Li, L., T. Wang, X. Li, P. Huang, Y. Guo, L. Lu, L. Zhou, and G. Zeng, 2023, *Photonics Research* **11**(4), 504.
- Li, X., Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, 2002, *Physical Review Letters* **88**(4), 047904.
- Liao, J., Z. Chen, J. Wang, H. Xiao, X. Guo, Z. Li, and D. Wang, 2025, *npj Quantum Information* **11**(1), 105.
- Liao, S.-K., W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, *et al.*, 2018, *Physical Review Letters* **120**(3), 030501.
- Lin, J., and N. Lütkenhaus, 2020, *Physical Review Applied* **14**(6), 064030.
- Lin, J., T. Upadhyaya, and N. Lütkenhaus, 2019, *Physical Review X* **9**(4), 041064.
- Liu, J., Y. Cao, P. Wang, S. Liu, Z. Lu, X. Wang, and Y. Li, 2022a, *Optics Express* **30**(15), 27912.
- Liu, Q., Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, 2022b, *Entropy* **24**(10), 1334.
- Liu, S., Y. Lou, Y. Chen, and J. Jing, 2022c, *Physical Review Letters* **128**(6), 060503.
- Liu, S., Y. Lou, and J. Jing, 2020a, *Nature Communications* **11**(1), 3875.
- Liu, S., Y. Lv, X. Wang, J. Wang, Y. Lou, and J. Jing, 2024, *Physical Review Letters* **132**(10), 100801.
- Liu, W., Y. Cao, X. Wang, and Y. Li, 2020b, *Physical Review A* **102**(3), 032625.
- Liu, W., X. Wang, N. Wang, S. Du, and Y. Li, 2017, *Physical Review A* **96**(4), 042312.
- Liu, W.-B., C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, 2021, *PRX Quantum* **2**(4), 040334.
- Liuzzo-Scorpo, P., A. Mari, V. Giovannetti, and G. Adesso, 2017, *Physical Review Letters* **119**(12), 120503.
- Lloyd, S., 1997, *Phys. Rev. A* **55**, 1613.
- Lo, H.-K., 1997, *Physical Review A* **56**(2), 1154.
- Lo, H.-K., and H. F. Chau, 1997, *Physical Review Letters* **78**(17), 3410.
- Lo, H.-K., M. Curty, and B. Qi, 2012, *Physical Review Letters* **108**(13), 130503.
- Lodewyck, J., M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, *et al.*, 2007, *Physical Review A* **76**(4), 042305.
- Long, G. L., and X. S. Liu, 2002, *Physical Review A* **65**(3), 032302.
- Long, N. K., R. Malaney, and K. J. Grant, 2023, *Information* **14**(10), 553.
- van Loock, P., and S. L. Braunstein, 1999, *Physical Review A* **61**(1), 010302.
- van Loock, P., and S. L. Braunstein, 2000, *Physical Review Letters* **84**(15), 3482.
- Lorente, A. G., P. V. Parellada, M. Castillo-Celeita, and M. Araújo, 2024, arXiv:2407.00152 .
- Lund, A. P., and T. C. Ralph, 2009, *Physical Review A* **80**(3), 032309.
- Luo, Y., X. Cheng, H.-K. Mao, and Q. Li, 2024, *Mathematics* **12**(14), 2243.
- Lupo, C., C. Ottaviani, P. Papanastasiou, and S. Pirandola, 2018, *Physical Review A* **97**(5), 052327.
- Lupo, C., and Y. Ouyang, 2022, *PRX Quantum* **3**(1), 010341.
- Lütkenhaus, N., J. Calsamiglia, and K.-A. Suominen, 1999, *Physical Review A* **59**(5), 3295.
- Lydersen, L., C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, 2010, *Nature Photonics* **4**(10), 686.
- Ma, X.-C., S.-H. Sun, M.-S. Jiang, M. Gui, Y.-L. Zhou, and L.-M. Liang, 2014, *Physical Review A* **89**(3), 032310.
- Ma, X.-C., S.-H. Sun, M.-S. Jiang, and L.-M. Liang, 2013a, *Physical Review A* **88**(2), 022339.
- Ma, X.-C., S.-H. Sun, M.-S. Jiang, and L.-M. Liang, 2013b, *Physical Review A* **87**(5), 052309.
- Madsen, L. S., V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, 2012, *Nature Communications* **3**, 1083.
- Mani, H., T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, 2021, *Physical Review A* **103**(6), 062419.
- Marie, A., and R. Alléaume, 2017, *Physical Review A* **95**(1), 012316.
- Marulanda Acosta, V., D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C. B. Lim, J.-M. Conan, and E. Diamanti, 2024, *New Journal of Physics* **26**(2), 023039.
- Matsuura, T., K. Maeda, T. Sasaki, and M. Koashi, 2021, *Nature Communications* **12**(1), 252.
- Maurer, U., 1993, *IEEE Transactions on Information Theory* **39**(3), 733.
- Mayers, D., 1997, *Physical Review Letters* **78**(17), 3414.
- Mayers, D., and A. Yao, 1998, in *Foundations of Computer Science, Palo Alto, 1998. Proceedings. 39th Annual Symposium on* (IEEE, Washington, DC), pp. 503–509.
- Mele, F. A., L. Lami, and V. Giovannetti, 2025, *Nature Photonics* **19**, 329.
- Menzies, D., and S. Croke, 2009, arXiv:0903.4181 .
- Metger, T., O. Fawzi, D. Sutter, and R. Renner, 2022, in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE), volume 2, pp. 844–850.
- Metger, T., and R. Renner, 2023, *Nature Communications* **14**(1), 5272.
- Mičuda, M., I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek, 2012, *Physical Review Letters* **109**(18), 180503.
- Milicevic, M., C. Feng, L. M. Zhang, and P. G. Gulak, 2018, *npj Quantum Information* **4**, 21.
- Milovančev, D., F. Honz, N. Vokić, F. Laudenbach, H. Hübel, and B. Schrenk, 2021, arXiv:2110.15228 .
- Milovančev, D., and N. Vokić, 2024, arXiv:2407.10517 .
- Moody, G., V. J. Sorger, D. J. Blumenthal, P. W. Juodawlakis, W. Loh, C. Sorace-Agaskar, A. E. Jones, K. C. Balram, J. C. F. Matthews, A. Laing, M. Davanco, L. Chang, *et al.*, 2022, *Journal of Physics: Photonics* **4**(1), 012501.
- Mosk, A. P., A. Lagendijk, G. Leroose, and M. Fink, 2012, *Nature Photonics* **6**(5), 283.
- Mountogiannakis, A. G., P. Papanastasiou, B. Braverman, and S. Pirandola, 2022, *Physical Review Research* **4**(1), 013099.
- Navascués, M., and A. Acín, 2005, *Physical Review Letters* **94**(2), 020505.
- Navascués, M., F. Grosshans, and A. Acín, 2006, *Physical Review Letters* **97**(19), 190502.
- Neset, M., J. Fadrný, M. Biela, J. Fiurášek, M. Ježek, and J. Bilek, 2024, arXiv:2412.13342 .
- Nielsen, M. A., and I. L. Chuang, 2012, *Quantum Computation and Quantum Information* (Cambridge University Press).

- Nikolopoulos, G. M., and E. Diamanti, 2017, Scientific Reports **7**(1), 46047.
- Notarnicola, M. N., F. Ciecich, and M. Jarzyna, 2024, New Journal of Physics **26**(4), 043015.
- Notarnicola, M. N., M. Jarzyna, S. Olivares, and K. Banaszek, 2023, New Journal of Physics **25**(10), 103014.
- Notarnicola, M. N., and S. Olivares, 2023, Physical Review A **108**(2), 022404.
- Oruganti, A. n., I. Derkach, R. Filip, and V. C. Usenko, 2025, Quantum Science and Technology **10**(2), 025023.
- Ottaviani, C., R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, 2016, Proc. SPIE 9996, 999609.
- Ottaviani, C., M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, 2020, IEEE Journal on Selected Areas in Communications **38**(3), 483.
- Pan, D., G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, 2024, IEEE Communications Surveys & Tutorials **26**(3), 1898.
- Papanastasiou, P., A. Mountogiannakis, and S. Pirandola, 2023, Scientific Reports **13**, 11636.
- Papanastasiou, P., C. Ottaviani, and S. Pirandola, 2017, Physical Review A **96**(4), 042332.
- Papanastasiou, P., C. Ottaviani, and S. Pirandola, 2018, Phys. Rev. A **98**, 032314.
- Papanastasiou, P., and S. Pirandola, 2021, Physical Review Research **3**(1), 013047.
- Paparelle, I., F. Mousavi, F. Scazza, A. Bassi, M. Paris, and A. Zavatta, 2025, Optics Express **33**(14), 28917.
- Paris, M. G. A., F. Illuminati, A. Serafini, and S. De Siena, 2003, Physical Review A **68**(1), 012314.
- Pascual-García, C., S. Bäuml, M. Araújo, R. Liss, and A. Acín, 2025, Physical Review A **111**(2), 022610.
- Pegg, D. T., L. S. Phillips, and S. M. Barnett, 1998, Physical Review Letters **81**(8), 1604.
- Pereira, D., A. N. Pinto, and N. A. Silva, 2023a, Journal of Lightwave Technology **41**(2), 432.
- Pereira, J., and S. Pirandola, 2018, Physical Review A **98**(6), 062319.
- Pereira, J. L., L. Banchi, and S. Pirandola, 2023b, Journal of Physics A: Mathematical and Theoretical **57**(1), 015305.
- Pfitzmann, B., and M. Waidner, 2001, in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*, pp. 184–200.
- Piétrì, Y., M. Schiavon, V. Marulanda Acosta, B. Gouraud, L. Trigo Vidarte, P. Grangier, A. Rhouni, and E. Diamanti, 2024a, Quantum **8**, 1575.
- Piétrì, Y., L. Trigo Vidarte, M. Schiavon, L. Vivien, P. Grangier, A. Rhouni, and E. Diamanti, 2024b, Optica Quantum **2**(6), 428.
- Pirandola, S., 2019, Communications Physics **2**, 51.
- Pirandola, S., 2021a, Physical Review Research **3**(4), 043014.
- Pirandola, S., 2021b, Physical Review Research **3**(1), 013279.
- Pirandola, S., 2024, Phys. Rev. Res. **6**, 013157.
- Pirandola, S., U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, *et al.*, 2020, Advances in Optics and Photonics **12**(4), 1012.
- Pirandola, S., S. L. Braunstein, and S. Lloyd, 2008a, Physical Review Letters **101**(20), 200504.
- Pirandola, S., S. L. Braunstein, S. Mancini, and S. Lloyd, 2008b, EPL (Europhysics Letters) **84**(2), 20013.
- Pirandola, S., J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, 2015a, Nature Photonics **9**(10), 641.
- Pirandola, S., R. García-Patrón, S. L. Braunstein, and S. Lloyd, 2009, Physical Review Letters **102**(5), 050503.
- Pirandola, S., R. Laurenza, C. Ottaviani, and L. Banchi, 2017, Nature Communications **8**(1), 15043.
- Pirandola, S., and S. Mancini, 2006, Laser Physics **16**(10), 1418.
- Pirandola, S., S. Mancini, S. Lloyd, and S. L. Braunstein, 2008c, Nature Physics **4**(9), 726.
- Pirandola, S., S. Mancini, D. Vitali, and P. Tombesi, 2003, Physical Review A **68**(6), 062317.
- Pirandola, S., C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, 2015b, Nature Photonics **9**(6), 397.
- Pirandola, S., and P. Papanastasiou, 2024, Phys. Rev. Res. **6**, 023321.
- Pirandola, S., D. Vitali, P. Tombesi, and S. Lloyd, 2006, Phys. Rev. Lett. **97**, 150403.
- Portmann, C., and R. Renner, 2022, Reviews of Modern Physics **94**(2), 025008.
- Primaatmaja, I. W., W. Y. Kon, and C. Lim, 2024, arXiv:2409.02630.
- Qi, B., P. G. Evans, and W. P. Grice, 2018, Physical Review A **97**(1), 012317.
- Qi, B., H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, and N. A. Peters, 2020, Physical Review Applied **13**(5), 054065.
- Qi, B., P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, 2015, Physical Review X **5**(4), 041009.
- Qin, H., R. Kumar, and R. Alléaume, 2016, Physical Review A **94**(1), 012325.
- Qin, H., R. Kumar, V. Makarov, and R. Alléaume, 2018, Physical Review A **98**(1), 012312.
- Qu, Z., and I. B. Djordjevic, 2017, Optics Express **25**(7), 7919.
- Raffaelli, F., G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, 2018, Quantum Science and Technology **3**(2), 025003.
- Ralph, T. C., 1999a, Optics Letters **24**(5), 348.
- Ralph, T. C., 1999b, Physical Review A **61**(1), 010303.
- Reid, M. D., 2000, Physical Review A **62**(6), 062308.
- Ren, S., R. Kumar, A. Wonfor, X. Tang, R. Pentty, and I. White, 2019, Journal of the Optical Society of America B **36**(3), B7.
- Renner, R., 2006, Ph.D. thesis (ETH Zurich).
- Renner, R., 2008, International Journal of Quantum Information **6**(01), 1.
- Renner, R., and J. I. Cirac, 2009, Physical Review Letters **102**(11), 110504.
- Rigas, J., 2006, Ph.D. thesis (University of Erlangen-Nuremberg).
- Rogaway, P., 1995, in *Annual International Cryptology Conference* (Springer), pp. 29–42.
- Roumestan, F., A. Ghazisaeidi, H. Mardoyan, J. Renaudier, E. Diamanti, and P. Grangier, 2022, in *Optical Fiber Communication Conference* (Optica Publishing Group), pp. Tu3I–4.
- Roumestan, F., A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, 2024, Journal of Lightwave Technology **42**(15), 5182.
- Rozpędek, F., K. Noh, Q. Xu, S. Guha, and L. Jiang, 2021, npj Quantum Information **7**(1), 102.
- Ruppert, L., C. Peuntinger, B. Heim, K. Günthner, V. C.

- Usenko, D. Elser, G. Leuchs, R. Filip, and C. Marquardt, 2019, *New Journal of Physics* **21**(12), 123036.
- Ruppert, L., V. C. Usenko, and R. Filip, 2014, *Physical Review A* **90**(6), 062310.
- Särkkä, S., 2013, *Bayesian Filtering and Smoothing* (Cambridge University Press), ISBN 9781107030657.
- Sarmiento, S., S. Etcheverry, J. Aldama, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M. J. Li, D. Loeber, and V. Pruneri, 2022, *New Journal of Physics* **24**(6), 063011.
- Scarani, V., A. Acín, G. Ribordy, and N. Gisin, 2004, *Physical Review Letters* **92**(5), 057901.
- Scarani, V., H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, 2009, *Reviews of Modern Physics* **81**(3), 1301.
- Scarani, V., and R. Renner, 2008, *Physical Review Letters* **100**(20), 200501.
- Schaetz, T., M. D. Barrett, D. Leibfried, J. Chiaverini, J. Britton, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland, 2004, *Physical Review Letters* **93**(4), 040505.
- Schmidt, F., D. Miller, and P. van Loock, 2024, *Physical Review A* **109**(4), 042427.
- Schumacher, B., and M. A. Nielsen, 1996, *Phys. Rev. A* **54**, 2629.
- Serafini, A., F. Illuminati, and S. De Siena, 2004, *Journal of Physics B* **37**(2), L21.
- Serafini, A., M. Paris, F. Illuminati, and S. De Siena, 2005, *Journal of Optics B: Quantum and Semiclassical Optics* **7**(4), R19.
- Shao, Y., Y. Pan, H. Wang, Y. Pi, Y. Li, L. Ma, Y. Zhang, W. Huang, and B. Xu, 2022, *Entropy* **24**(7), 992.
- Shen, S.-Y., M.-W. Dai, X.-T. Zheng, Q.-Y. Sun, G.-C. Guo, and Z.-F. Han, 2019, *Physical Review A* **100**(1), 012325.
- Sherson, J. F., H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, 2006, *Nature* **443**, 557.
- Shirokov, M. E., 2017, *Journal of Mathematical Physics* **58**(10), 102202.
- Shor, P. W., and J. Preskill, 2000, *Physical Review Letters* **85**(2), 441.
- Silberhorn, C., N. Korolkova, and G. Leuchs, 2002a, *Physical Review Letters* **88**(16), 167902.
- Silberhorn, C., T. C. Ralph, N. Lütkenhaus, and G. Leuchs, 2002b, *Physical Review Letters* **89**(16), 167901.
- Soh, D. B., C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, 2015, *Physical Review X* **5**(4), 041010.
- Srikara, S., K. Thapliyal, and A. Pathak, 2020, *Quantum Information Processing* **19**(4), 132.
- Stinson, D. R., 1996, *Congressus Numerantium* **114**, 7.
- Su, X., W. Wang, Y. Wang, X. Jia, C. Xie, and K. Peng, 2009, *Europhysics Letters* **87**(2), 20005.
- Su, Y., Y. Guo, and D. Huang, 2019, *Physics Letters A* **383**(20), 2394.
- Suleiman, I., J. Nielsen, X. Guo, N. Jain, J. Neergaard-Nielsen, T. Gehring, and U. L. Andersen, 2022, *Quantum Science and Technology* **4**, 045003.
- Sych, D., and G. Leuchs, 2010, *New Journal of Physics* **12**(5), 053019.
- Takahashi, R., Y. Tanizawa, and A. R. Dixon, 2016, in *6th Int. Conf. Quantum Cryptography*.
- Takeda, S., T. Mizuta, M. Fuwa, H. Yonezawa, P. van Loock, and A. Furusawa, 2013, *Physical Review A* **88**(4), 042327.
- Takei, N., T. Aoki, S. Koike, K.-i. Yoshino, K. Wakui, H. Yonezawa, T. Hiraoka, J. Mizuno, M. Takeoka, M. Ban, and A. Furusawa, 2005a, *Physical Review A* **72**(4), 042304.
- Takei, N., H. Yonezawa, T. Aoki, and A. Furusawa, 2005b, *Physical Review Letters* **94**(22), 220502.
- Takeoka, M., S. Guha, and M. M. Wilde, 2014, *Nat. Commun.* **5**, 5235.
- Tan, S. M., 1999, *Physical Review A* **60**(4), 2752.
- Tang, B.-Y., B. Liu, Y.-P. Zhai, C.-Q. Wu, and W.-R. Yu, 2019, *Scientific reports* **9**(1), 15733.
- Thornton, M., H. Scott, C. Croal, and N. Korolkova, 2019, *Physical Review A* **99**(3), 032341.
- Tian, Y., P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, 2022, *Optica* **9**(5), 492.
- Tian, Y., Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, 2023, *Optics Letters* **48**(11), 2953.
- Toh, K. C., M. J. Todd, and R. H. Tütüncü, 1999, *Optimization Methods and Software* **11**(1-4), 545.
- Tomamichel, M., R. Colbeck, and R. Renner, 2009, *IEEE Transactions on Information Theory* **55**(12), 5840.
- Tomamichel, M., C. C. W. Lim, N. Gisin, and R. Renner, 2012, *Nature Communications* **3**, 634.
- Tomamichel, M., C. Schaffner, A. Smith, and R. Renner, 2011, *IEEE Transactions on Information Theory* **57**(8), 5524.
- Tütüncü, R. H., K. C. Toh, and M. J. Todd, 2003, *Mathematical Programming* **95**(2), 189.
- Unruh, D., 2004, arXiv:quant-ph/0409125.
- Upadhyaya, T., 2021, Master thesis (University of Waterloo) URL <http://hdl.handle.net/10012/17209>.
- Upadhyaya, T., T. van Himbeek, J. Lin, and N. Lütkenhaus, 2021, *PRX Quantum* **2**(2), 020325.
- Ursin, R., F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, et al., 2007, *Nature Physics* **3**(7), 481.
- Usenko, V. C., 2018, *Physical Review A* **98**(3), 032321.
- Usenko, V. C., 2025, *Optics Express* **33**(11), 22643.
- Usenko, V. C., and R. Filip, 2010, *Physical Review A* **81**(2), 022318.
- Usenko, V. C., and R. Filip, 2011, *New Journal of Physics* **13**(11), 113007.
- Usenko, V. C., and R. Filip, 2016, *Entropy* **18**(1), 20.
- Usenko, V. C., and F. Grosshans, 2015, *Physical Review A* **92**(6), 062337.
- Usenko, V. C., B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, 2012, *New Journal of Physics* **14**(9), 093048.
- Usenko, V. C., C. Peuntinger, B. Heim, K. Günthner, I. Derkach, D. Elser, C. Marquardt, R. Filip, and G. Leuchs, 2018, *Optics Express* **26**(24), 31106.
- Usenko, V. C., L. Ruppert, and R. Filip, 2014, *Physical Review A* **90**(6), 062326.
- Usuga, M. A., C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, 2010, *Nature Physics* **6**(10), 767.
- Vahlbruch, H., M. Mehmet, K. Danzmann, and R. Schnabel, 2016, *Physical Review Letters* **117**(11), 110801.
- Vaidman, L., 1994, *Physical Review A* **49**(2), 1473.
- Van Assche, G., J. Cardinal, and N. J. Cerf, 2004, *IEEE Transactions on Information Theory* **50**(2), 394.
- Van Der Heide, S., J. Frazão, A. Albores-Mejía, and C. Okonkwo, 2023, in *Optical Fiber Communication Conference* (Optica Publishing Group), pp. W2A-37.
- Vasylyev, D., A. Semenov, and W. Vogel, 2016, *Physical Re-*

- view Letters **117**(9), 090501.
- Vazirani, U., and T. Vidick, 2014, Physical Review Letters **113**(14), 140501.
- Walk, N., S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, 2016, Optica **3**(6), 634.
- Walk, N., T. C. Ralph, T. Symul, and P. K. Lam, 2013, Physical Review A **87**(2), 020303.
- Wang, C., F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, 2005, Physical Review A **71**(4), 044305.
- Wang, L.-J., K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, *et al.*, 2021, npj quantum information **7**(1), 67.
- Wang, N., S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, 2018, Physical Review Applied **10**(6), 064028.
- Wang, P., Y. Zhang, Z. Lu, X. Wang, and Y. Li, 2023, New Journal of Physics **25**(2), 023019.
- Wang, T., Z. Zuo, L. Li, P. Huang, Y. Guo, and G. Zeng, 2022, Phys. Rev. Appl. **18**, 014064.
- Weedbrook, C., 2013, Physical Review A **87**(2), 022308.
- Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, 2004, Physical Review Letters **93**(17), 170504.
- Weedbrook, C., C. Ottaviani, and S. Pirandola, 2014, Physical Review A **89**(1), 012309.
- Weedbrook, C., S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, 2012a, Reviews of Modern Physics **84**(2), 621.
- Weedbrook, C., S. Pirandola, S. Lloyd, and T. C. Ralph, 2010, Physical Review Letters **105**(11), 110501.
- Weedbrook, C., S. Pirandola, and T. C. Ralph, 2012b, Physical Review A **86**(2), 022318.
- Weerasinghe, W., 2024, Ph.D. thesis (University of Cambridge) URL <https://www.repository.cam.ac.uk/handle/1810/375669>.
- Wegman, M. N., and J. L. Carter, 1981, Journal of computer and system sciences **22**(3), 265.
- Wehner, S., C. Schaffner, and B. M. Terhal, 2008, Physical Review Letters **100**(22), 220502.
- Williams, B. P., R. J. Sadlier, and T. S. Humble, 2017, Physical Review Letters **118**(5), 050501.
- Williamson, J., 1936, American Journal of Mathematics **58**(1), 141.
- Winick, A., N. Lütkenhaus, and P. J. Coles, 2018, Quantum **2**, 77.
- Winnel, M. S., N. Hosseini, and T. C. Ralph, 2020, Physical Review A **102**(6), 063715.
- Winter, A., 1999, IEEE Transactions on Information Theory **45**(7), 2481.
- Wolf, M. M., G. Giedke, and J. I. Cirac, 2006, Physical Review Letters **96**(8), 080502.
- Wootters, W. K., and W. H. Zurek, 1982, Nature **299**(5886), 802.
- Wu, L.-A., H. J. Kimble, J. L. Hall, and H. Wu, 1986, Physical Review Letters **57**(20), 2520.
- Wu, Y., L. Tian, W. Yao, S. Shi, X. Liu, B. Lu, Y. Wang, and Y. Zheng, 2024, Applied Physics Letters **124**(11), 114002.
- Xiang, G. Y., T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, 2010, Nature Photonics **4**(5), 316.
- Xing, Z., X. Li, X. Ruan, Y. Luo, and H. Zhang, 2022, Photonics **9**(7), 463.
- Xu, F., X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, 2020, Reviews of Modern Physics **92**(2), 025002.
- Xu, Y., T. Wang, X. Liao, Y. Zhou, P. Huang, and G. Zeng, 2024, Photonics Research **12**(11), 2549.
- Yamano, S., T. Matsuura, Y. Kuramochi, T. Sasaki, and M. Koashi, 2024, Physica Scripta **99**(2), 025115.
- Yan, B., Q. Li, H. Mao, and N. Chen, 2022, Quantum Information Processing **21**(4), 130.
- Yan, J., X. Zhou, Y. Qin, Z. Yan, X. Jia, C. Xie, and K. Peng, 2024, Physical Review Research **6**(3), 032062.
- Yang, S., Z. Yan, H. Yang, Q. Lu, Z. Lu, L. Cheng, X. Miao, and Y. Li, 2023, EPJ Quantum Technology **10**(1), 1.
- Yonezawa, H., T. Aoki, and A. Furusawa, 2004, Nature **431**(7007), 430.
- Yukawa, M., H. Benichi, and A. Furusawa, 2008, Physical Review A **77**(2), 022314.
- Zavatta, A., J. Fiurášek, and M. Bellini, 2010, Nature Photonics **5**(1), 52.
- Zeng, G., and W. Zhang, 2000, Physical Review A **61**(2), 022303.
- Zhang, G., J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, *et al.*, 2019, Nature Photonics **13**(12), 839.
- Zhang, H., Y. Luo, L. Zhang, X. Ruan, and D. Huang, 2022, IEEE Photonics Journal **14**(3), 1.
- Zhang, S., and X. Zhang, 2018, Physical Review A **97**(4), 043830.
- Zhang, T. C., K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, 2003, Physical Review A **67**(3), 033802.
- Zhang, W., D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, 2017, Physical Review Letters **118**(22), 220501.
- Zhang, Y., Y. Bian, Z. Li, S. Yu, and H. Guo, 2024a, Applied Physics Reviews **11**(1).
- Zhang, Y., Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, 2020, Physical Review Letters **125**(1), 010502.
- Zhang, Y.-F., W.-B. Liu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, 2024b, Physical Review A **110**(5), 052613.
- Zhao, J., J. Y. Haw, T. Symul, P. K. Lam, and S. M. Assad, 2017, Physical Review A **96**(1), 012319.
- Zhao, J., H. Jeng, L. O. Conlon, S. Tserkis, B. Shajilal, K. Liu, T. C. Ralph, S. M. Assad, and P. K. Lam, 2023, Nature Communications **14**(1), 4745.
- Zhao, W., R. Shi, and X. Ruan, 2021, Laser Physics Letters **18**(3), 035201.
- Zhao, Y., Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, 2018, Journal of Physics B **52**(1), 015501.
- Zhao, Y.-B., M. Heid, J. Rigas, and N. Lütkenhaus, 2009, Physical Review A **79**(1), 012307.
- Zheng, Y., P. Huang, A. Huang, J. Peng, and G. Zeng, 2019a, Physical Review A **100**(1), 012313.
- Zheng, Y., P. Huang, A. Huang, J. Peng, and G. Zeng, 2019b, Optics Express **27**(19), 27369.
- Ziebell, M., M. Persechini, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, 2015, in *2015 European Conference on Lasers and Electro-Optics* (Optica Publishing Group), European Quantum Electronics Conference, p. JSV_4_2.