Brazilian Journal of Physics (2026) 56:106
https://doi.org/10.1007/s13538-026-02023-9

Towards a Point-to-point CV-QKD System: Implementation Challenges and Perspectives

Davi Juvêncio Gomes de Sousa[1] · Nelson Alves Ferreira Neto[1] · Christiano M. S. Nascimento[1] · Lucas Q. Galvão[1] · Mauro Queiroz Nooblath Neto[1] · Micael Andrade Dias[1,2] · Cássio de Castro Silva[1] · Braian Pinheiro da Silva[1] · Alexandre B. Tacla[1] · Valéria Loureiro da Silva[1]

Received: 30 September 2025 / Accepted: 16 January 2026

Abstract

This article presents an analysis of the practical challenges and implementation perspectives of point-to-point continuous-variable quantum key distribution (CV-QKD) systems over optical fiber. The study addresses the physical layer, including the design of transmitters, quantum channels, and receivers, with emphasis on impairments such as attenuation, chromatic dispersion, polarization fluctuations, and coexistence with classical channels. We further examine the role of digital signal processing (DSP) as the bridge between quantum state transmission and classical post-processing, highlighting its impact on excess noise mitigation, covariance matrix estimation, and reconciliation efficiency. The post-processing pipeline is detailed with a focus on parameter estimation in the finite-size regime, information reconciliation using LDPC-based codes optimized for low-SNR conditions, and privacy amplification employing large-block universal hashing. From a hardware perspective, we discuss modular digital architectures that integrate dedicated accelerators with programmable processors, supported by a reference software framework (*CV-QKD-ModSim*) for algorithm validation and hardware co-design. Finally, we outline perspectives for the deployment of CV-QKD in Brazil, starting from metropolitan testbeds and extending toward hybrid fiber/FSO and space-based infrastructures. The work establishes the foundations for the first point-to-point CV-QKD system in Brazil, while providing a roadmap for scalable and interoperable quantum communication networks.

Keywords Quantum key distribution · Continuous variable · Optical fiber · Digital processing

✉ Davi Juvêncio Gomes de Sousa
davi.juvencio@fieb.org.br

Nelson Alves Ferreira Neto
nelson.neto@fieb.org.br

Christiano M. S. Nascimento
christiano.moreira@fieb.org.br

Lucas Q. Galvão
lqgalvao3@gmail.com

Mauro Queiroz Nooblath Neto
mauro.neto@fieb.org.br

Micael Andrade Dias
mandi@dtu.dk

Cássio de Castro Silva
cassio.castro@fbter.org.br

Braian Pinheiro da Silva
braian.silva@fieb.org.br

Alexandre B. Tacla
alexandre.tacla@fieb.org.br

Valéria Loureiro da Silva
valeria.dasilva@fieb.org.br

[1] QuIIN – Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845, Salvador 41650-010, BA, Brasil

[2] Department of Electrical and Photonics Engineering, Technical University of Denmark, Ørsteds Plads, Building 340, Lyngby 2800, Denmark

Published online: 03 March 2026

1 Introduction

A century has passed since the foundational works of quantum mechanics revolutionized our understanding of nature at its most fundamental level. Since then, our understanding of the quantum world has evolved from a purely physical perspective to an informational one. The emergence of quantum information science has led to the second quantum revolution, transforming our view of quantum mechanics from a purely physical theory to a powerful informational resource [1]. This paradigm shift has laid the groundwork for quantum technologies that are reshaping our modern world.

Today, as we commemorate these 100 years of quantum physics, Brazil finds itself at a pivotal moment in the quantum technology landscape, with quantum communication emerging as one of the most promising and strategically important applications of quantum mechanics. Recent large-scale initiatives in quantum communication and cryptography have been actively promoted by Brazil's Ministry of Science, Technology and Innovation (MCTI), resulting in the current development of quantum networks in Recife (PE), Rio de Janeiro (RJ), and São Carlos (SP) [2, 3]. Furthermore, the EMBRAPII CIMATEC Competence Center in Quantum Technologies, called Quantum Industrial Innovation (QuIIN), seeks to position Brazil at the forefront of scientific and technological development of quantum technologies.

Established in December 2023 through a partnership between SENAI CIMATEC, MCTI, and EMBRAPII (the Brazilian Company for Industrial Research and Innovation), QuIIN's mission is to advance quantum technologies in Brazil by fostering collaborative research and development partnerships with academia and industry, providing training and capacity building in quantum technologies (mainly in quantum communication and quantum computing), and supporting the creation and development of startups in the quantum sector. Despite being a young initiative, QuIIN already has a multidisciplinary team of over 80 researchers (staff and fellows), including physicists, mathematicians, computer scientists, and engineers. With a strong focus on continuous-variable quantum key distribution (CV-QKD), the research team is tackling a range of theoretical and experimental challenges, including hardware development, with the ambitious goal of implementing Brazil's first point-to-point CV-QKD system. Being the first initiative of this nature in the country adds a layer of complexity, as it requires not only overcoming the inherent technical difficulties of CV-QKD, but also building local expertise, establishing experimental infrastructure from the ground up, and navigating uncharted regulatory and integration pathways. In this pioneering effort, the team must simultaneously act as developers, educators, and ecosystem builders.

Quantum Key Distribution (QKD) is one of the first quantum technologies to achieve practical implementation at scale. Over the past two decades, the field has evolved from theoretical proposals to commercial solutions and advanced experimental demonstrations [4, 5]. Thanks to continuous progress in protocol design, rigorous security analyses, and technological development, large-scale testbed deployments are now operating worldwide, ranging from metropolitan networks [6–9] to intercontinental satellite-based quantum communication links [6, 10–14].

Although discrete-variable QKD (DV-QKD) protocols were the first to be developed [15] and achieve widespread adoption [4], in recent years CV-QKD systems have emerged as a competitive alternative, advancing rapidly in both theoretical understanding and experimental implementations [5]. The fundamental distinction between these approaches lies in the quantum states employed as information carriers and their corresponding measurement strategies. In a typical DV-QKD protocol, the transmitter (usually called Alice) encodes classical bits of information in discrete degrees of freedom of single photons (e.g., horizontal/vertical polarization) and transmits them through a quantum channel to the receiver (called Bob), who measures each photon to obtain binary outcomes. In most CV-QKD protocols, however, information is encoded in the quadratures of coherent states generated by laser sources; Alice transmits states modulated according to a predetermined encoding scheme, where different values of quadratures correspond to different information symbols. After receiving the CV state, Bob measures the quadratures by performing homodyne (or heterodyne) detection, thus obtaining continuous-valued measurement results.

Because classical optical communication systems also encode information in the quadrature amplitudes of laser light and recover it through coherent detection, CV-QKD protocols are fully compatible with the same fundamental components that form the backbone of modern telecommunication networks. This compatibility enables higher key generation rates over short and medium distances (of the order of Gbps for $\sim$10 km and Mbps for $\sim$100 km [16, 17]), facilitates integration into photonic platforms [18, 19] and existing fiber networks [20]. This approach thus provides a cost-effective alternative that eliminates the need for new infrastructure with specialized single-photon detection equipment, which is required by DV systems [5].

However, these advantages come at the cost of significantly increased complexity in post-processing and digital signal processing (DSP), which translates into increased hardware complexity compared to DV-QKD systems.

Unlike discrete-variable systems, where single photon detection events provide relatively clean binary outcomes, CV-QKD must extract cryptographic keys from continuous measurement data that are inherently dominated by quantum and classical noise. This fundamental challenge requires sophisticated DSP algorithms to distinguish and recover the highly attenuated quantum signal from background noise, demanding real-time computational capabilities with high precision analog-to-digital conversion and extensive digital filtering. Furthermore, the continuous nature of the measurement data necessitates parameter estimation procedures that can accurately characterize the quantum channel and assess security parameters. The post-processing pipeline must implement advanced error-correction codes specifically designed to operate at very low signal-to-noise ratios (SNRs) in continuous-variable systems. In practice, information reconciliation is typically performed using multi-edge low-density parity-check (LDPC) codes acting on blocks of at least 10^6 symbols to enable reliable decoding at low code rates. In contrast, parameter estimation and privacy amplification require significantly larger block sizes, ideally 10^8 symbols or more, in order to mitigate finite-size effects and approach the asymptotic secret key rate. In a point-to-point CV-QKD system, all these operations must be executed in real time, transforming what might initially seem like a simpler optical setup into a complex signal processing and systems engineering challenge. This high level of computational and algorithmic sophistication, combined with the need for robust and scalable hardware, makes the CV-QKD implementation a non-trivial task.

In the Brazilian context, these challenges are magnified by the absence of existing quantum communication infrastructure, which demands not only technological innovation but also the creation of a national knowledge base and ecosystem around quantum communication. Against this backdrop, this article explores the technical, infrastructural, and strategic challenges of developing Brazil's first point-to-point CV-QKD system, and outlines the perspectives that such an effort opens for the country's role in the global quantum technology landscape. To complement this practical perspective, another article in this special issue presents an introductory review of CV-QKD theory [21], covering fundamental concepts and key protocols in the field. For more comprehensive treatments of the subject, readers are referred to [4, 22–26]. Additionally, to support the training of a new generation of Brazilian researchers specializing in QKD, an accessible tutorial on quantum cryptography in Portuguese is presented in [27].

This article is organized as follows. In Section 2, we provide an overview of Quantum Key Distribution (QKD) protocols, with a focus on Continuous Variable QKD (CV-QKD) systems. In Section 3, we describe the physical layer of CV-QKD implementations, detailing the transmitter, channel, and receiver subsystems. In Section 4, we present the post-processing pipeline, including digital signal processing, parameter estimation, information reconciliation, and privacy amplification. Section 5 discusses the hardware development efforts required to enable real-time CV-QKD, including digital architectures and reference simulation frameworks. Finally, Section 6 presents perspectives for the deployment of quantum communication infrastructure in Brazil, with emphasis on ongoing initiatives and future scalability.

2 CV-QKD Systems Overview

A quantum key distribution (QKD) protocol is a quantum communication system designed to leverage unique properties of quantum systems to share classical random sequences secretly. The objective of a QKD protocol is to allow the two legitimate parties, Alice and Bob (the transmitter and receiver, respectively), to distribute (or generate) a classical random sequence that is kept secret from a potential eavesdropper, named Eve. This classical random sequence, the key, can then be used in further cryptographic protocols, such as one-time-pad (OTP) [28], the Advanced Encryption Standard (AES) [29], or key expansion protocols [30].

In a conceptual picture, a QKD protocol makes use of a noisy insecure quantum channel and a public authenticated classical channel, as depicted in Fig. 1. The quantum channel is used for the quantum communication stage and it is considered to be under Eve's control, meaning that she can interact with the quantum states sent by Alice to gain information on the shared key. As a security premise, the noise coming from the quantum channel is assumed to be the result of an eavesdropping attempt [31]. The classical channel, on the other hand, is used by Alice and Bob to exchange messages during the classical postprocessing of the raw key. By hypothesis, the classical channel is public, meaning that the classical messages are publicly available, but it is authenticated, so that Alice and Bob are certain that they are receiving messages from each other and not by the eavesdropper in disguise.

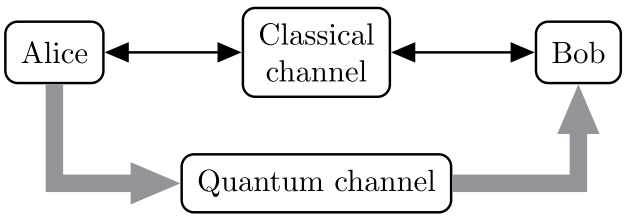

Fig. 1 Conceptual model of a QKD protocol

In a CV-QKD protocol, coherent states of light are typically used since they are easily generated in the laboratory by telecom-grade lasers, and information is encoded on conjugated quadratures of the electromagnetic field [26]. The quadratures may be modulated according to a pair of independent Gaussian random variables, or a discretized version with an appropriate choice of a discrete probability distribution on a set of points on the phase space (the complex plane) [32–36]. Protocols following the first strategy compose the class of Gaussian modulated coherent states (GMCS) protocols, whilst the second modulation strategy is known as discrete modulation of CV-QKD protocols. At the receiver, coherent measurement is employed by Bob, which can be either a homodyne detector, with a random choice of which quadrature is to be measured, or a heterodyne detector that measures both quadratures at once.

The operation of a typical CV-QKD protocol comes in general four major stages, (i) quantum communication, (ii) parameter estimation, (iii) information reconciliation, and (iv) privacy amplification. Below, we outline the important case of the GG02 protocol [32], which employs Gaussian-modulated coherent states with homodyne detection. A variant of this protocol with heterodyne (double homodyne) detection was later introduced by Weedbrook *et al.* in 2004 [33]. Both versions produce Gaussian random variables and can be analyzed using similar security frameworks [4], though they differ in their implementations and measurement noise characteristics. Heterodyne detection, which measures both quadratures simultaneously, has become more common in practice as it eliminates the need for a quantum random number generator (QRNG) at the receiver and the sifting stage. However, homodyne detection introduces less noise by measuring only one quadrature at a time, potentially enabling higher secret key rates.

1. **Quantum communication** - Comprises the "quantum part" of a CV-QKD protocol where quantum states are prepared, transmitted and measured. It consists of the following steps that are repeated L times:
    1. *State preparation* - Alice has access to a pair of independent and identically Gaussian random variables $Q, P \sim \mathcal{N}(0, \tilde{V}_m)$. At each round, Alice draws independent samples from P and Q, which she uses to prepare the coherent state $|\alpha\rangle = |q + ip\rangle$ by modulating the quadratures of a coherent pulse. The random samples of both Q and P are stored on the registers Q_L and P_L.
    2. *Quantum state transmission* - Alice transmits the modulated quantum signal through the insecure quantum channel, which is typically modeled by the transmittance parameter τ, accounting for the channel attenuation, and the excess noise ξ. Usually, implementations of CV-QKD protocols transmit the coherent states through optical fibers or free-space. During propagation, the quantum signals experience multiple distortion processes, which are discussed in detail in Section 3.
    3. *Measurement* - At reception, Bob must randomly chose to measure either the q or p quadrature at each round, and applies the homodyne measurement. The measurement results are stored in the L-sized register Y_L.
2. **Parameter estimation** - Alice and Bob have to estimate the channel parameters allowing them to compute the secret key rate (SKR). Before it takes place, Bob must inform Alice the random quadrature choices of the homodyne detection. Alice then discards the values corresponding to non-measured quadratures and form the random vector X_L. This procedure is called key sifting[1] and is only required in protocols with homodyne detection, where only one quadrature is measured. The pair X_L and Y_L is called the shared raw key. Now, Alice and Bob perform an estimation of the security parameters of the system by choosing a random subset of size $L' \lll L$ to be announced publicly and used by the estimators. The samples used for parameter estimation are discarded so that Alice and Bob keep the remaining $l = L - L'$ raw key elements. The estimated parameters are used to compute the SKR for the exchanged states. The protocol aborts if the SKR is negative, indicating that the channel conditions do not allow for secure key extraction. Otherwise, the protocol proceeds to the information reconciliation stage.
3. **Information reconciliation** - After parameter estimation, the sequences X_l and Y_l are correlated random variables that must be used to distill a pair of identical binary sequences. This process is accomplished with the use of an Information Reconciliation protocol, which will be discussed in detail in Section 4.3. The general idea is that, as X_l and Y_l are Gaussian vectors, a quantization operation[2] must take place so that the generated key takes binary values, followed by an error correction protocol to ensure that there are no differences between Alice and Bob's sequences. We denote by $Q(\cdot)$ the quantization operation. Alice and Bob may chose between performing direct reconciliation (DR) or reverse reconciliation (RR). In the DR scenario, the

[1] It is the CV analogous of the sifting procedure used in the BB84 DV-QKD protocol [15].

[2] Here, quantization refers to the representation of a continuous-valued variable with finite precision. Not to be confused with the quantization of the electromagnetic field.

reference frame is $U_A = Q(X_l)$ and Bob applies error correction to Y_l, obtaining a binary sequence U_B such that $U_A = U_B$ with high probability. In the RR, the roles are reversed and the reference frame is $U_l = Q(Y_l)$. Counterintuitively, RR is preferred as it allows key distribution beyond the 3 dB loss limit [37].

4. **Privacy amplification** - After information reconciliation, Alice and Bob share a pair of binary sequences (U_A, U_B) that are equal with high probability, but insecure in the sense that Eve acquired information during quantum state transmission and also from the reconciliation messages. To remove Eve's knowledge, Alice and Bob must reduce the size of the shared key by a fraction that is determined by the SKR calculation in the parameter estimation step. This reduction should enforce both randomness and secrecy, and is accomplished by using a suitable random mapping $f : \{0,1\}^l \mapsto \{0,1\}^m$, where *m* is the final key length given by security analysis. The mapping is randomly chosen from a family of 2-universal hash functions ensuring that $S = f(U_A) = f(U_B)$ with high probability, which is the final key, and that Eve has no information on *S*.

The above description provides a general outline of CV-QKD protocols. A few details deserve particular attention in practical implementations. The quantum channel parameters are unknown and must be estimated under the conservative assumption that the channel is controlled by an eavesdropper. Since information is encoded in coherent state quadratures, the channel naturally introduces attenuation and excess noise beyond the shot noise limit, making parameter estimation crucial for security analysis and SKR computation, as will be discussed in Section 4.2. Historically, parameter estimation was performed before error correction, but reversing this order has proven more efficient. This enables the use of nearly all exchanged data for both tasks, leading to more accurate channel estimation and effectively enlarging the dataset available for secret key distillation [17, 38, 39]. This is possible because information reconciliation depends on absolute SNR, which can be estimated without disclosing raw data, while specific security related channel parameters are only available though by data disclosure. A generalization to a protocol using heterodyne detection can be done with adjustments on the raw key length to be $2L$ and by dropping the sifting procedure [33]. Information reconciliation and privacy amplification should proceed equally in this case.

Another important aspect of CV-QKD protocols protocols is the reconciliation direction. In DR there is a fundamental 3 dB loss limit. Beyond this threshold, the channel attenuation is so severe that an eavesdropper on the channel would receive more information than Bob, making secure key distillation impossible. This occurs because, in a lossy channel, the eavesdropper can in principle capture the lost light, and beyond 3 dB loss (50% transmittance), more information is lost to the environment than reaches Bob. While techniques such as advantage distillation were proposed to overcome this limit [40], they lack compatibility with broader security proof frameworks. In contrast, RR does not face this limitation. Since Bob holds the reference frame, secure keys can theoretically be generated at any distance, with excess channel noise–rather than loss–becoming the primary limiting factor.

The above description of a CV-QKD protocol covers the major practical tasks that are are required by a theoretical security proof, meaning that it is, in some sense, a conceptual description. A practical implementation can result in several other aspects not foreseen in the theoretical model, which can impact the protocol performance by a significant increase on the overall noise levels, or even by introducing security loopholes due to specific system architectures or devices vulnerabilities [41, 42].

Due to the variety of practical implementation possibilities, several CV-QKD architectures have been proposed, with certain key innovations serving as major milestones in the development of the technique. The characteristics of transmitter and receiver setups will be detailed in the next sections. Notable advances include the transition from transmitted local oscillator (TLO) to local local oscillator (LLO) schemes. In TLO, Alice transmits her local oscillator alongside the quantum signal to Bob, while in LLO, Bob generates it locally and corrects the phase using a reference signal from Alice [43]. Additional key developments are the increasing use of digital signal processing [17, 44, 45] and the refinement of error correction codes (ECC), especially decoding implementations, as part of the information reconciliation protocol [46, 47].

The transition from TLO to LLO is due to security reasons. While using TLO is more practical in the sense that the transmitted local oscillator serves directly as the phase reference for coherent detection, it results in a security loophole as the eavesdropper can manipulate the reference signal and change Bob's measurements. The LLO implementation solves this security problem by avoiding the transmission of a strong reference field, while adding complexity to the receiver as it must synchronize both lasers (Alice and Bob's sides), typically through digital signal processing techniques. Digital signal processing has become imperative as it allows Bob to compensate for the optical channel effects dispersions and unavoidable devices imperfections. The efficient implementations of long- and low-rate decoders for ECC's, especially for LDPC codes, allows the system to operate at very low signal to noise region, meaning longer distances.

3 Physical Layer

QKD systems are primarily based on optical and photonic components. While information can be encoded in various optical degrees of freedom–such as polarization, time-bin, or spatial modes–CV-QKD encodes information in the field quadratures of light. This approach offers natural compatibility with conventional optical telecommunication technologies, making CV-QKD particularly suitable for integration into existing fiber-optic networks. In this section, we briefly describe the optical implementation of a typical CV-QKD systems, including the key components for state preparation, transmission, and detection.

3.1 Transmitter

Typical configurations of a CV-QKD optical system are depicted in Fig. 2: (a) with a TLO and (b) with a LLO. The system consists of three main parts: the transmitter (Alice), the quantum channel, and the receiver (Bob). As discussed in Section 2, Alice prepares and transmits a random coherent state to Bob in a typical prepare-and-measure CV-QKD protocol. Alice's transmitter is based on a standard commercial laser, which generates strong coherent states. These states are modulated using an in-phase and quadrature (IQ) electro-optic modulator to encode Gaussian-distributed random variables onto the field quadratures. A variable optical attenuator (VOA) then reduces the signal to the quantum regime, with a mean photon number on the order of one photon per pulse [5]. While coherent states remain the primary choice for practical CV-QKD systems, squeezed states of light have been theoretically shown to offer advantages such as enhanced secret key rates, improved resilience to excess noise, and better performance under imperfect information reconciliation [5, 48]. Despite these benefits, experimental implementations face significant technical challenges. Recent work has demonstrated the practical viability of squeezed-state CV-QKD over optical fiber channels, moving beyond earlier free-space demonstrations with emulated loss [49–51].

The choice of laser source is a critical design decision in CV-QKD systems, as the system's security and performance are directly affected by excess noise, with phase noise being a dominant contributor. Phase noise is determined by the

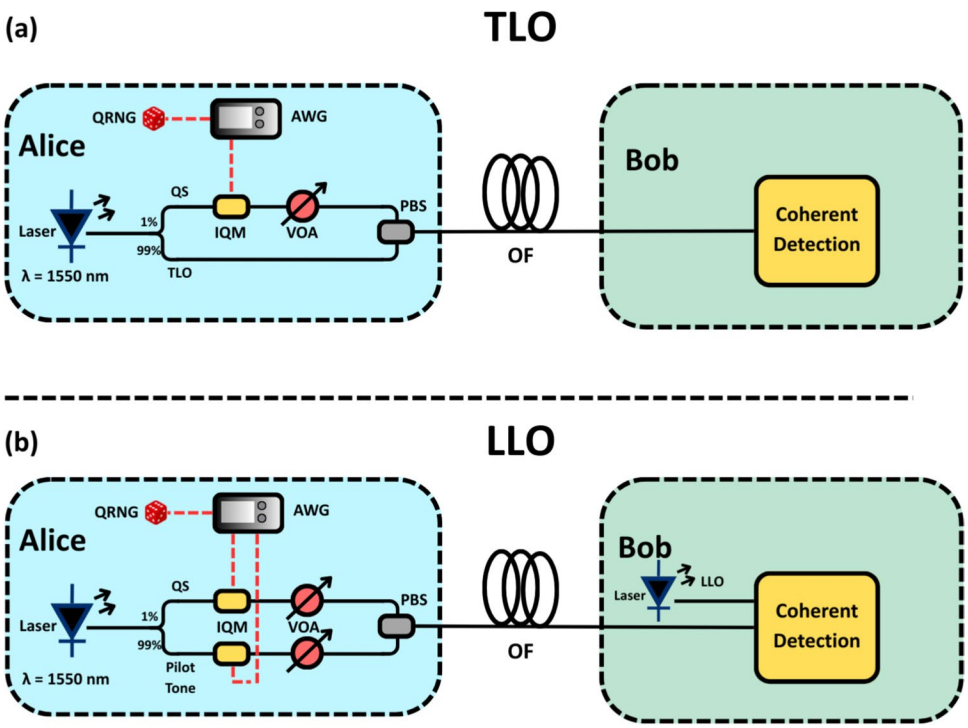

Fig. 2 Different transmission systems. (**a**) Transmitting Local Oscillator (TLO), in which the local oscillator is generated at Alice and co-propagates with the quantum signal through the optical fiber. A Telecom laser ($\lambda = 1550$nm) is split such that a fraction is called quantum signal (QS), which is modulated by an I/Q modulator (IQM) driven by an arbitrary waveform generator (AWG) seeded by a quantum random number generator (QRNG). The remaining optical power is transmitted to function as a local oscillator (TLO). A variable optical attenuator (VOA) sets the appropriate signal power before transmission, and a polarization beam splitter (PBS) is employed to multiplex the optical fields. At the receiver, Bob performs coherent detection, which will be explained in Sec. (**b**) Local-local Oscillator (LLO) configuration, where the quantum signal and a pilot tone are generated at Alice, while the local oscillator is independently generated at Bob. The pilot tone is transmitted along with the quantum signal to enable phase and frequency recovery at the receiver. At Bob, a local laser acts as the LLO and is combined with the received signal for coherent detection

laser's linewidth: a broader linewidth introduces larger phase fluctuations, degrading the SNR and reducing the achievable secret key rate. Although many demonstrations employ narrow linewidths (around 100 Hz [17, 20]) to mitigate these issues, such sources are costly. For scalable CV-QKD network deployment, this cost factor becomes a significant practical constraint. Consequently, the choice of laser is not merely a hardware consideration but a strategic design decision: selecting a laser with sufficiently low phase noise and with viable cost is paramount to ensuring both the system's performance and practical feasibility.

As mentioned, information is encoded in the quadratures of the laser field. This is commonly achieved using optical modulators, which exploit the Kerr effect to convert electrical signals into optical modulation. Although alternative encoding strategies exist, such as polarization encoding implemented with Pockels cells, these approaches are generally more complex to realize experimentally. Consequently, optical modulators remain the predominant solution. The first experimental implementation employed Gaussian modulation [52]. More recently, discrete modulation formats, such as QAM, have attracted increasing interest [5].

Furthermore, CV-QKD systems share similarities with coherent classical communication, as the quantum states must preserve both amplitude and phase information. As a result, the establishment of a reliable phase reference is essential. In early implementations, most protocols relied on TLO to the receiver. However, several attacks targeting this approach have been proposed [53, 54]. The two implementation strategies, TLO and LLO, are illustrated in Fig. 2.

3.2 Channels

Over the years, CV-QKD has been predominantly implemented using optical fiber (OFs) channels [55]. Optical fibers offer advantages compared to other transmission media, including high bandwidth, compact deployment, and immunity to electromagnetic interference. In addition, they can be modeled as a Gaussian channel, as discussed in Section 4. Nevertheless, optical fibers are subject to several impairments, and a proper understanding of these limitations is essential for the design of practical systems.

One of the primary impairments is fiber attenuation, which causes the signal transmittance to decrease exponentially with distance. While this loss is acceptable for metropolitan-scale links, it significantly constrains transmission over longer distances. At 1550 nm, which corresponds to a low-loss window, the attenuation of standard fibers is approximately 0.2 dB/km, thereby limiting the achievable secret key rate.

Another relevant limitation is chromatic dispersion, which leads to pulse broadening as a function of wavelength and directly affects the temporal profile of the quantum states. For standard single-mode fibers at 1550 nm, the dispersion coefficient is approximately 20 ps/(nm km) [56]. Although dispersion-shifted fibers can reduce this effect, they may introduce nonlinear phenomena such as four-wave mixing when multiple wavelength channels are employed [57]. Alternatively, digital-domain post-processing techniques, as discussed in Section 4, can partially compensate for dispersion.

Another relevant impairment is polarization fluctuation. Optical fibers are sensitive to environmental perturbations, such as temperature changes and mechanical vibrations, which cause random polarization drifts. These fluctuations impact both the quantum signal and the pilot tone when they are transmitted simultaneously via polarization multiplexing, typically implemented with a polarization beam splitter (PBS). As illustrated in Fig. 3, to transmit the quantum signal and the pilot tone simultaneously, we can use

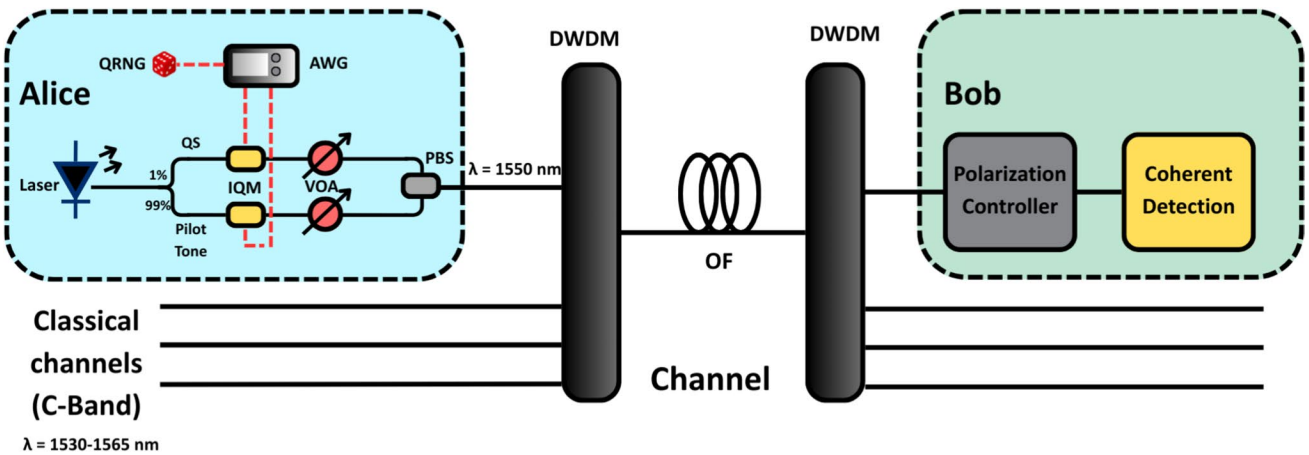

Fig. 3 Coexistence of the quantum signal with classical C-Band (λ = 1530-1565nm) channels. The signals are combined/separated with a dense wavelength-division multiplexer(DWDM). At the receiver, the quantum channel is demultiplexed from the classical traffic and coherently detected, with an active polarization control stage to compensate for polarization drifts induced by the optical fiber

polarization multiplexing by combining both signals with a PBS. During propagation, the fiber induces polarization changes in both signals, requiring the use of a polarization control system. Most implementations rely on active polarization controllers [58], which can introduce distortions into the optical setup. Alternatively, passive polarization controllers combined with Faraday mirrors have been employed to achieve long-term stabilization [59]. On the other hand, it is possible to have a polarization-diverse detection. Although there will be leakage of the pilot tone into the quantum signal, it can be recovered using an equalizer in the post-processing step [60].

Lastly, the coexistence with classical channels is another challenge [20]. With a larger quantity of classical channels, noises such as crosstalk and stimulated Raman scattering are more present. Crosstalk is the leakage of the classical channel into the quantum one. This leakage may originate from finite filter extinction ratios, non-ideal WDM components, or spectral broadening of classical signals due to modulation and fiber nonlinearities. As a consequence, crosstalk manifests as excess noise at the receiver, degrading the signal-to-noise ratio and potentially compromising the security of the quantum system. A possible solution for this problem is using spectral filters, such as a thinner Bragg grating, to diminish this leakage. Raman backscattering is a nonlinear effect of the fiber due to the interaction with two channels and the fiber structure, which generates phonons, therefore increasing the noise [22]. High-power classical channels can induce both spontaneous and stimulated Raman scattering, generating broadband noise photons that may spectrally overlap with the quantum channel. Raman noise is particularly detrimental due to its wide spectral distribution and its dependence on the relative wavelength spacing and launch power of the classical channels. While spectral filtering can partially mitigate this effect, a complementary approach is to use time multiplexing between classical and quantum channels, thereby preventing interaction between them. However, it will limit the rate of both channels.

A possible approach for QKD is to shift the quantum signal to the O-band, around a wavelength of 1310 nm [61, 62]. Operating in this band significantly reduces chromatic dispersion, crosstalk, and Raman scattering. However, fiber attenuation is higher in this wavelength range, typically around 0.3 dB/km [62]. Consequently, the optimal operating regime depends on the trade-off between these effects and the achievable key rate.

3.3 Receiver

To measure information encoded in the optical quadratures, coherent detection techniques can be employed [5, 22]. In this context, two variants of the protocol can be implemented, as illustrated in Fig. 4.

The first variant relies on homodyne detection, in which Bob randomly selects one quadrature to measure from the quantum state transmitted by Alice. This measurement is performed using a homodyne detector combined with a phase modulator driven by a random number generator, which determines the quadrature to be analyzed [5].

The second variant employs double homodyne detection, where Bob deterministically measures both quadratures of the incoming state. Although this approach enables simultaneous access to both quadratures, it incurs a penalty of 3 dB, corresponding to half of the original optical power, due to the use of an additional beam splitter to divide the signal [22].

For both detection schemes, a balanced detector is required to ensure common-mode noise rejection and to

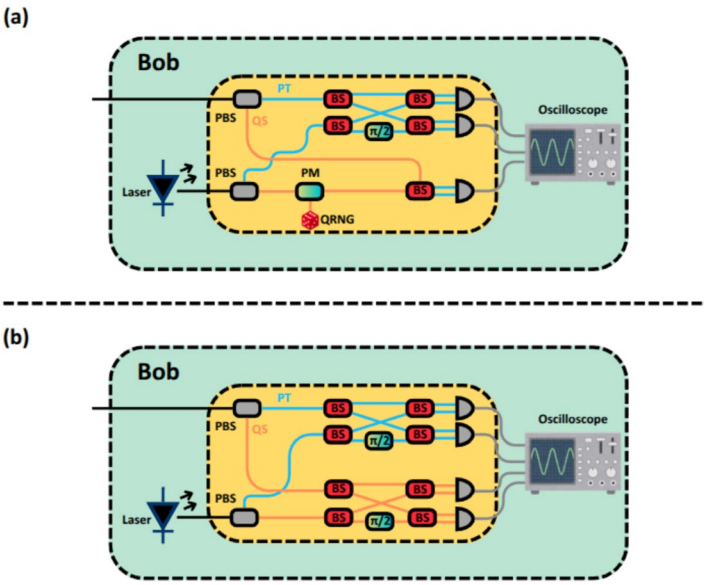

Fig. 4 Detection setups for CV-QKD. In both figures, the blue line represents the pilot tone, while the orange line corresponds to the quantum signal. The gray boxes indicate the balanced detectors. (**a**) Homodyne detection. The quantum signal is separated from the pilot tone. It is directed into a beamsplitter together with the local-local oscillator (LLO), whose phase is randomized by a phase modulator (PM) driven by a quantum random number generator (QRNG). The pilot tone, on the other hand, passes through an interferometer with the LLO, where one branch introduces a phase shift of $\pi/2$, allowing full reconstruction of both quadratures of the pilot tone. (**b**) Double homodyne/heterodyne. In this configuration, both the quantum signal and the pilot tone enter an interferometer with the LLO, where one branch imposes a phase difference of $\pi/2$, enabling the full measurement of both quadratures for each signal

isolate the quantum signal of interest [22, 24]. After optical detection, the resulting electrical signal is forwarded to the post-processing stage.

Regardless of the detection method, detection noise will be present, and, according to Laudenbach et. al. [22], it is the noise that mainly impacts CV-QKD systems. A balanced photodetector used for homodyne detection exhibits electronic noise from several internal components, including the photodiodes, transimpedance amplifier, and ADC. Each of these contributes with its own noise spectral density. Under this assumption, the total noise variance scales linearly with the detector bandwidth. Therefore, the increase in noise with bandwidth is not due to any specific detector parameter, but rather to the fact that a wider bandwidth integrates over a larger portion of the electronic noise spectrum. Therefore, if one chooses a detector with high electronic noise or insufficient bandwidth, it will significantly impact the secret key rate of the protocol.

Some studies demonstrate that we can treat detector noise as trusted, in which a portion of the observed noise is attributed to the detector itself rather than to a potential eavesdropper who cannot manipulate it. Incorporating this noise model enables more possibilities for analysis of the secure key rate in CV-QKD systems, accounting for imperfections inherent to the measurement devices. Despite its relevance, the detailed treatment of trusted detector noise is beyond the scope of this work. However, it has been reported in the following [36, 63].

4 Post-processing Pipeline

Post-processing in CV-QKD systems is an indispensable stage for transforming noisy and correlated measurements into secure secret keys. While the quantum channel is responsible for transmitting the modulated optical states, security against an adversary is effectively consolidated in the classical domain through posterior processing. During this stage, Alice and Bob apply protocols to reconcile the information with errors introduced by quantum noise, fiber attenuation, and excess noise, while simultaneously estimating and reducing the information potentially acquired by an eavesdropper. The efficiency of post-processing has a direct impact on both the final key generation rate and the maximum achievable distance, making it decisive for the feasibility of practical CV-QKD systems [5].

In general, the post-processing pipeline consists of a structured set of classical algorithms that follow the quantum transmission phase, typically including sifting, parameter estimation, information reconciliation, and privacy amplification [5]. Each stage plays a specific role in ensuring Alice and Bob derive identical and secret shared keys. However, sifting is not required when both quadratures are measured simultaneously using a no-switching protocol with dual quadrature homodyne or heterodyne detection, as all measurement results are retained for key generation [22, 33].

In this context, a central bridge between quantum optical physics and post-processing is the digital signal processing (DSP) stage, which prepares the signal at the transmitter and processes the raw measurements at the receiver. This stage directly determines the quality of the correlations shared by Alice and Bob. While in the CV-QKD literature the post-processing part of the protocol is commonly related to the classical operations applied to the raw key to distill identical secret sequences, the DSP stage is responsible for recovering the measured signal by mitigating distortions caused by the channel and optical/electronic imperfections, thereby reducing excess noise. That is, DSP generates the raw data for key distillation. At the transmitter side, DSP encodes information into the signal by mapping bits into quadratures, organizes frames, inserts pilots, and applies pulse shaping (e.g., root-raised cosine filtering). At the receiver side, it separates pilot and quantum signals, performs digital down-conversion, clock recovery, static equalization, IQ imbalance correction, S21 response compensation, and dynamic equalization (e.g., phase tracking and polarization rotation via MIMO (multiple input multiple output)), as well as matched filtering and frame synchronization. Its control stack also performs shot-noise unit calibration. The outcome is a set of normalized and time-aligned samples with minimized excess noise and reduced bias for parameter estimation [64]. In CV-QKD, this DSP chain — largely inherited from coherent communications — not only enables accurate LO stabilization and phase estimation, but also improves reconciliation efficiency β and secure transmission distance, as it produces a more accurate covariance matrix by mitigating noise from system impairment. Recent works further highlight that even linear DSP routines must be carefully calibrated, particularly regarding consistent shot-noise estimation, to ensure overall security of the protocol [65].

Figure 5 illustrates the complete end-to-end flow. For clarity, the terms highlighted in bold correspond directly to the functional blocks explicitly labeled in the figure. On Alice's side, the **QRNG** provides the raw key data, which are processed by the **DSP Transmitter**. This module maps the data onto optical quadratures by generating the baseband signal, inserting pilot symbols, and applying pulse shaping. The resulting digital samples are converted into electrical signals by the DAC and subsequently applied to the **Modulator**, which imprints them onto a continuous-wave laser. After appropriate attenuation, coherent states are generated and propagate through the quantum channel, as indicated by the transmission of quantum states region.

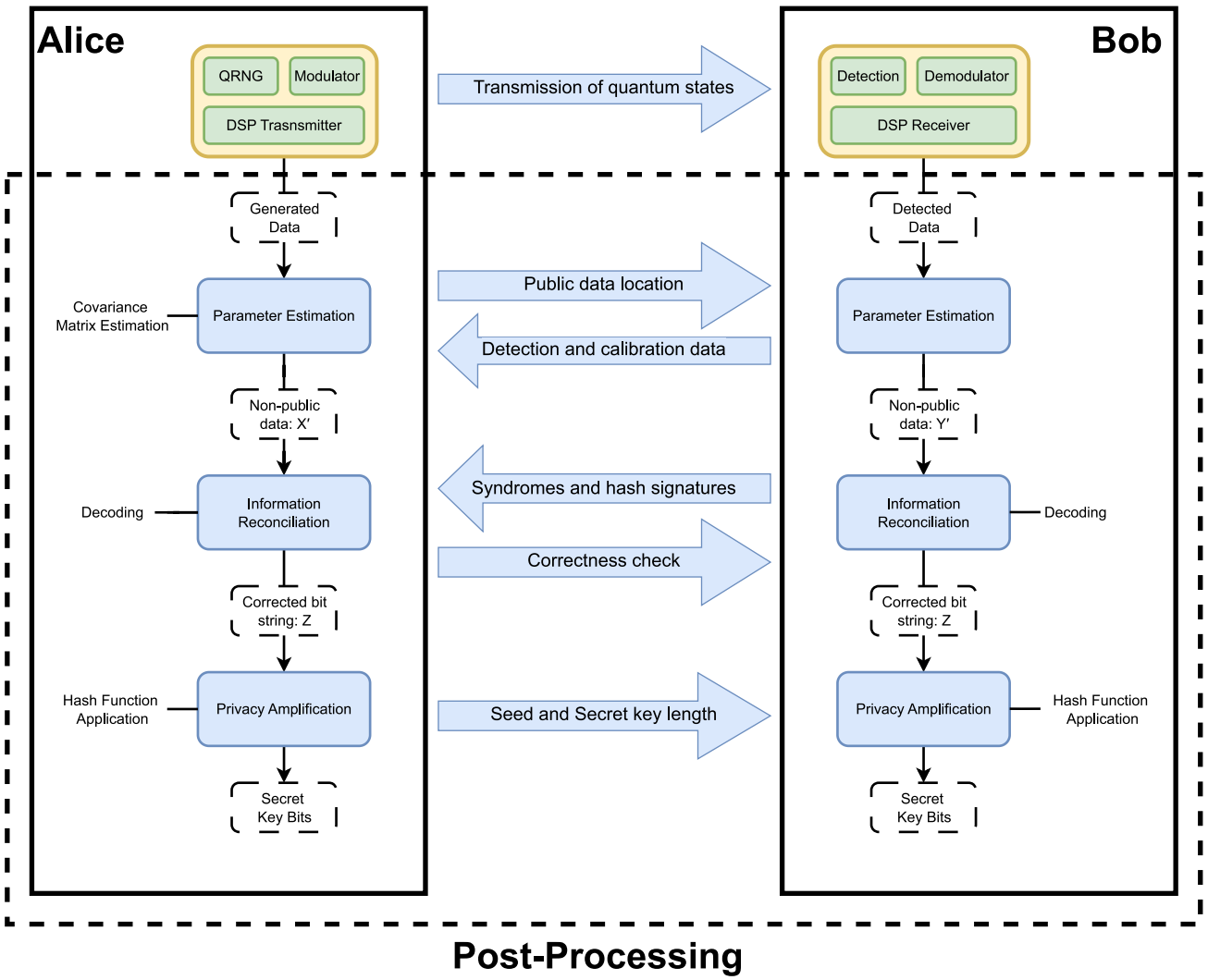

Fig. 5 End-to-end pipeline of a CV-QKD system, illustrating the generation, transmission, detection, and post-processing of quantum states for secret key extraction. The upper part depicts the quantum layer, from state preparation at Alice to quadrature measurement at Bob, while the lower part shows the classical and authenticated post-processing stages, including parameter estimation, information reconciliation, and privacy amplification. Public communications and private data are explicitly distinguished. Adapted from [5]

On Bob's side, the incoming optical states are measured by the **Detection** stage, operating in either homodyne or heterodyne configuration. The measurement outcomes are then processed by the **DSP Receiver**, which performs digital demodulation tasks including down-conversion, clock recovery, equalization, and shot-noise-unit normalization, yielding the digital **Detected Data**.

Subsequently, the **Post-Processing** stage takes place and is entirely classical and authenticated. Alice and Bob first perform **Parameter Estimation** using publicly disclosed random subsets of their data (X' and Y') in order to reconstruct the covariance matrix and assess the viability of secret key extraction. They then execute **Information Reconciliation** to correct discrepancies between their strings and obtain the aligned bit sequence Z. Finally, after publicly communicating the **Seed and Secret key length**, both parties apply **Privacy Amplification**, based on Toeplitz hash functions, to generate identical **Secret Key Bits**.

The figure further highlights the distinction between public communications, such as announcements, syndromes, and correctness checks, and private data, while clearly indicating that the transmission of quantum states is restricted to the segment between modulation and detection.

4.1 Digital Signal Processing for CV-QKD

Digital Signal Processing (DSP) emerges as a pivotal technology in the paradigm shift from classical optical communications to quantum-secure systems, most notably in CV-QKD. At its core, DSP acts as the fundamental bridge

between the quantum domain of information and the subsequent stages of classical post-processing, orchestrating the transformation of discrete sequences of quadrature values into a modulated optical signal at Alice's station and their subsequent reconstruction into digital form at Bob's station [66]. This capability is crucial not only for enabling data synchronization and mitigating signal impairments—such as chromatic dispersion, polarization-mode dispersion, and phase noise—in coherent optical communication systems, but also for enhancing the correlation between transmitted and received quantum states, thereby ensuring accurate key generation and the overall robustness of the CV-QKD system [65]. The adoption of DSP techniques originating from classical optical communications confers superior performance to CV-QKD in practical scenarios, where environmental factors and imperfections in optical components can degrade the quality of the quantum signal [65]. Moreover, DSP is indispensable for the implementation of a locally generated local oscillator (LO), enabling correction of frequency and phase offsets via frequency-multiplexed pilot tones transmitted by Alice [66].

The DSP pipeline in CV-QKD, shown in Fig. 6, represents the complete digital chain from quantum state preparation to key extraction. At the transmitter, the process begins with a QRNG, followed by distribution matching and constellation mapping, which determine the statistical properties of the encoded quadratures. The mapped symbols are pulse-shaped, typically with a root-raised cosine (RRC) filter, and digitally up-converted for optical modulation. Pilot tones and synchronization sequences are inserted to support frequency, phase, and timing recovery. At the receiver, the pipeline continues with high-speed analog-to-digital conversion (ADC), deskew, and static equalization. Chromatic dispersion compensation and adaptive equalization are then applied, followed by carrier frequency and phase recovery. Finally, decision and decoding modules convert the reconstructed quadratures into binary outputs that form the raw key material. This sequence highlights the role of DSP as the central element enabling reliable signal generation, synchronization, and impairment compensation in CV-QKD systems.

On the transmitter side, Alice's DSP executes a series of critical functions to prepare the quantum signal for transmission. Random symbols are first generated from a prescribed distribution; for instance, in the Gaussian Modulated Coherent State (GMCS) protocol, the mean quadrature values $\langle I \rangle$ and $\langle Q \rangle$ are randomly drawn from a Gaussian distribution with zero mean and variance V_A [66]. Probabilistic Constellation Shaping (PCS) applied to Quadrature Amplitude Modulation (QAM) formats is also employed to optimize mutual information and approach the Shannon channel capacity [68]. Subsequently, pulse shaping is carried out,

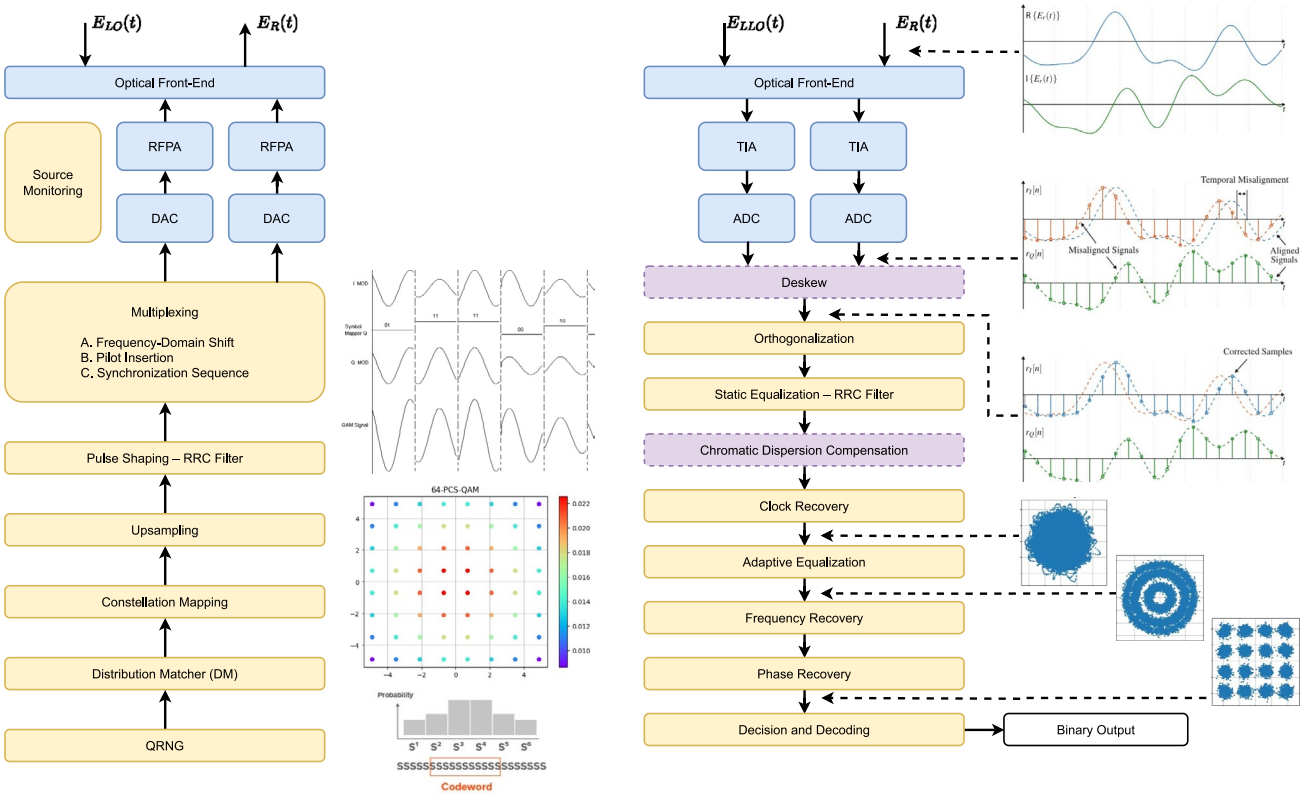

Fig. 6 DSP pipeline of a CV-QKD system, from quantum state transmission to recovered raw data keys. Adapted from [67]

which is essential for defining the temporal mode of the signal. While an ideal time-limited pulse would require infinite bandwidth for distortion-free detection, engineering practice relies on spectrally limited pulse shapes such as the root-raised cosine (RRC) filter [44]. The RRC filter, with an adjustable roll-off factor, minimizes inter-symbol interference (ISI) and distortions inherent to finite-bandwidth detectors [66]. In experimental settings, the roll-off factor is also a key parameter influencing the system's excess noise; therefore, it is typically optimized to values such as 0.4 or 0.2, depending on bandwidth constraints and overall performance requirements [44, 69]. After pulse shaping, the signal undergoes digital frequency up-conversion primarily to mitigate low-frequency electronic noise, which would otherwise degrade the signal-to-noise ratio in the quadrature measurements. Although up-conversion also enables RF heterodyne detection, such detection does not strictly require this step, as it can alternatively be achieved by employing slightly detuned local oscillators at Alice's and Bob's sides. In RF heterodyne detection, the quantum signal is mixed with a frequency-shifted local oscillator, allowing simultaneous retrieval of both quadratures with a single photodiode, as demonstrated in recent true-heterodyne receiver architectures for CV-QKD [44, 60]. To better reflect this context, references describing standard RF heterodyne implementations are more appropriate than those reporting phase-diverse detection schemes. Furthermore, frequency-multiplexed pilot tones are inserted into the quantum signal to provide robust references for clock and phase correction between Alice and Bob. A Zadoff-Chu or Constant Amplitude Zero Autocorrelation (CAZAC) sequence is appended at the beginning of each frame to facilitate synchronization and recovery of the time-multiplexed pilot sequence [5]. Strategies such as frequency and polarization multiplexing of the pilots with the quantum signal are employed to mitigate crosstalk and channel interference [70].

On the receiver side, Bob's DSP is more complex and indispensable for faithful reconstruction of the quantum signal. The received electrical signals are first digitized by an analog-to-digital converter (ADC) operating at sampling rates ranging from 5 GSa/s to 10 GSa/s [44, 71]. The quantum signals and frequency-multiplexed pilot tones are then digitally separated [5]. The quantum signal is subsequently down-converted to baseband, aligned with the frequency shift applied at the transmitter [5]. Digital clock recovery identifies optimal sampling instants, employing algorithms such as Gardner's method [72]. Static equalization then compensates for fixed imperfections, including I/Q imbalance and S21 mismatch, while the pulse is recovered through a matched RRC filter [5, 73]. Dynamic equalization is further applied to correct for variable phase and polarization drifts, frequently using Multiple-Input Multiple-Output (MIMO) algorithms [74]. This includes compensation of frequency offset, filtering and equalization, as well as pilot-aided phase recovery [75]. Frame synchronization is ensured through training sequences such as Zadoff-Chu or CAZAC [5], while fine data and clock synchronization are achieved via DSP-based routines [76].

Beyond its basic functions, DSP in CV-QKD incorporates advanced techniques to optimize performance. Chromatic dispersion (CD) compensation, typically carried out in the frequency domain, mitigates pulse broadening effects in long-haul fiber transmission [75]. Phase and LO correction are enhanced by employing multiple frequency-multiplexed pilot tones and advanced carrier frequency/phase estimation algorithms, including the M^{th}-power method for residual phase error removal [66, 68, 77]. To address polarization drifts and suppress noise, Kalman filters have shown effectiveness by adapting to slow variations in the polarization state [76]. A critical step is Shot Noise Unit (SNU) normalization, which provides a consistent and physically meaningful reference for quadrature measurements between Alice and Bob, rather than ensuring faithful quantum representation, and enables proper calibration of linear DSP outputs [42].

The impact of DSP on CV-QKD system performance is multifaceted and deeply intertwined with security metrics. DSP optimization directly improves the reconciliation efficiency (β), which is crucial for maximizing the secret key rate by enhancing the correlation between Alice's and Bob's data [65]. Excess noise (ξ) is a limiting factor for both the achievable transmission distance and the security threshold of the protocol. Its reduction does not increase the intrinsic security of CV-QKD but ensures that the noise level remains below the maximum tolerable bound required for secure key generation [65]. The fidelity of the covariance matrix, constructed from DSP-recovered data, is essential for accurately assessing protocol security, as it enables estimation of the information potentially accessible to an eavesdropper (Eve) [42]. Consequently, the overall security of the protocol is constrained by DSP's ability to maintain stable and accurate quadrature statistics while suppressing noise contributions that would otherwise compromise parameter estimation [65].

Future perspectives for DSP in CV-QKD are promising, driven by the pursuit of higher speed, longer reach, and deeper integration. The application of machine learning (ML) algorithms for nonlinear channel equalization is an active research frontier, with neural networks demonstrating the potential to surpass conventional DSP approaches [78, 79]. ML-based algorithms may also be applied to key sifting and excess noise reduction, enhancing system robustness in noisy environments [80], as well as to automatic modulation format recognition [81]. Integration

into Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) is fundamental for achieving real-time processing, as these platforms provide the parallel computational capabilities required by the intensive DSP operations, leading to significant increases in secret key rates and transmission distances [82]. The evolution toward system-on-chip (SoC) platforms, such as RFSoC-based architectures that integrate processors, programmable logic, and converters on a single chip, marks a decisive step in miniaturization and cost optimization, facilitating large-scale adoption of CV-QKD technology [81]. Achieving real-time operation — from quantum state preparation to final key extraction — constitutes the ultimate goal, making overall system speed a primary performance indicator for commercial deployments [82]. Thus, the continuous evolution of DSP is intrinsic to the advancement of CV-QKD, driving the field toward increasingly efficient, secure, and adaptable quantum communication networks.

4.2 Parameter Estimation and Calibration

A fundamental security assumption for QKD protocols is that the quantum channel is insecure, meaning that the eavesdropper controls it and all information lost to the environment ultimately goes to the eavesdropper. In a practical scenario, this means that Eve controls the channel parameters, making precise parameter estimation a pivotal step in a QKD protocol operating in a non-asymptotic regime. Thus, Alice and Bob must use their random variables, X and Y, respectively, to compute the worst-case-scenario parameters and construct their covariance matrix in order to compute the amount of information leaked to an eavesdropper (E) using the Holevo bound $\chi(Y;E)$ [5, 25, 26].

The channel parameters must be estimated using a portion of the signals, denoted as L', where L is the total number of quadrature measurements after sifting (as introduced in Section 2). The remaining $l = L - L'$ samples are reserved for raw key generation. In principle, they need to estimate the transmittance T, the excess noise ξ, Alice's variance V_A, quantum efficiency of the detectors η_{eff} and the electronic noise ν_{el}. However, the main problem of parameter estimation is reduced to estimate T and ξ, since one can reasonably assume that the other parameters are relatively well known: [83]. In fact, η_{eff} is calibrated beforehand from the receiver's known efficiency and losses, and V_A is a fixed parameter set and verified locally by the transmitter. In contrast, the excess noise has the most significant impact on the secret-key rate [84, 85].

The Gaussian channel parameters can be estimated considering the linear model

$$Y = tX + Z\,, \tag{1}$$

where $t = \sqrt{T}$, X is a random variable related to the transmitted signal, Z is a random variable related to the noise channel, and Y is a random variable related to the received signal [22].

In general, these variables are normalized in a shot-noise units (SNU) for both, Alice and Bob, have a reference unit for security analysis [5]. In this way, the variance of the quantum fluctuation in phase space is usually defined as this reference unit, represented by the SNU. In practical implementations, its estimation is made by measuring the vacuum, which is recorded in the receiver setup as electronic signals [86]. During the detection, the electronic noise is accounted to the shot-noise, such that Bob needs to make a calibration.

The calibration of shot noise can be performed using various methodologies [86–91]. Here, we outline the primary strategies commonly employed in the literature:

1. **Two-time with pre-calibration** [87]: In this calibration, the electronic noise is measured (see Fig. 7). First, with the LO beam blocked at the optical input ports and the homodyne detector powered on, the measured variance corresponds to the raw electronic noise. Subsequently, the total system noise is measured with the LO illuminated. The shot-noise unit (SNU) is then obtained by calculating the difference between these two variance measurements.
2. **Two-time in real-time** [88, 89]: in this calibration, the pre-calibration is also performed at first. This enables

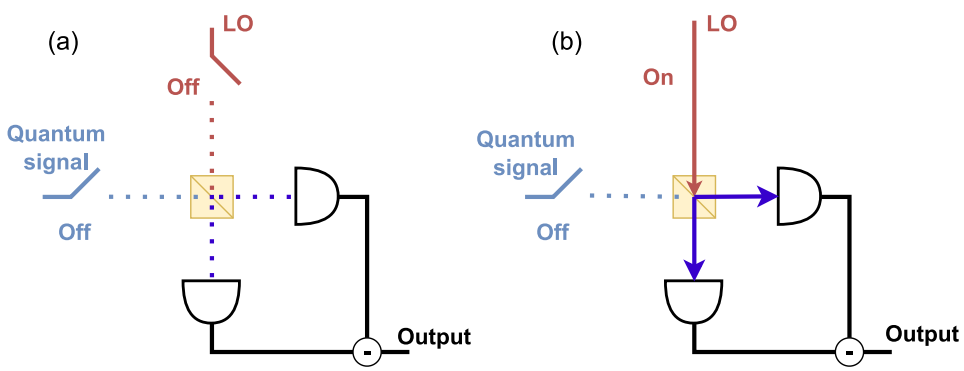

Fig. 7 Calibrating a balanced homodyne detector. (**a**) Electronic noise level, measured by blocking both the signal and local oscillator (LO) inputs. (**b**) Total system noise, measured with the local oscillator (LO) beam applied

Bob to compute a linear relation between the optical power and the SNU. Then, a small portion of the LO is separated and constantly measured. Then, based on the computation made after pre-calibration, the SNU is adjusted in real-time.

3. **One-time** [90, 91]: In this method, the SNU is calibrated by measuring the total noise. Then, the signals are normalized considering this measure, such that the electronic noise can be represented using another vacuum state for security analisys. However, the performance of this protocol is slightly inferior to that of the traditional method because electronic noise is not estimated in this process. As a result, the electronic noise is considered untrusted, meaning the associated loss is also deemed untrusted.

Following calibration, the signals are normalized, and their quadratures are distributed as $X \sim \mathcal{N}(0, V_A), Z \sim \mathcal{N}(0, \sigma^2)$, and $Y \sim \mathcal{N}(0, t^2 V_A + \sigma^2)$, where $\sigma^2 = 1 + t^2\xi$ [83]. In this expression, the unit variance (1) originates from the shot-noise normalization inherent to homodyne detection. For heterodyne detection, this value becomes 2, as the signal is split on a balanced beam splitter to enable simultaneous measurement of both conjugate quadratures [63]. The parameters t and σ^2 are then estimated from the data, with the resulting estimators denoted as $\hat{t}$ and $\hat{\sigma}^2$.

An estimator is a function of samples of a random variable[3], being a random variable itself, and the estimator $\hat{\theta}$ of a parameter θ is said to be unbiased if $\mathbb{E}[\hat{\theta}] = \theta$. However, in general, the variance of the estimator is a non-zero value which is inversely proportional to the number of samples provided to the estimator, meaning that the estimated value may differ from the true parameter value in a finite statistics setting. In a CV-QKD scenario, one needs unbiased estimators for the channel parameters ($\mathbb{E}[\hat{t}] = t$ and $\mathbb{E}[\hat{\sigma}^2] = \sigma^2$), and provide that the achievable secret-key rate will not be overestimated [63]. This can be done by computing the estimator's confidence intervals and using the worst case boundaries of such intervals as practical values to compute the secret key rate. In other words, one ensures that, with high probability, the parameter estimation satisfy $\hat{t}_{\min} \leq t$ and $\hat{\sigma}^2_{\max} \geq \sigma^2$, where $\hat{t}_{\min}$ and $\hat{\sigma}^2_{\max}$ are the upper and lower bounds of the confidence intervals for the transmittance and excess noise [83], respectively, given by

$$t_{\min} \approx \hat{t} - z_{\epsilon_{PE}/2}\mathrm{SD} \tag{2}$$

and

$$\sigma^2_{\max} \approx \hat{\sigma}^2 + z_{\epsilon_{PE}/2}\mathrm{SD}, \tag{3}$$

where $z_{\epsilon_{PE}/2} = \mathrm{erf}^{-1}(1 - \epsilon_{PE}/2)$ and $\mathrm{erf}(x)$ is the error function [92]. Here, SD is the standard deviation.

The primary challenge in practical implementations is to achieve highly precise parameter estimation using a limited subset of m signals, as these are subsequently discarded because their information is announced over the authenticated classical channel [93]. Within the literature, Maximum Likelihood Estimation (MLE) is widely recognized as the standard method in the field [94–96]. This prominence is largely due to the first comprehensive security proof against Gaussian collective attacks in the finite-size regime being established using an MLE-based framework [83]. Subsequently, alternative methods have been proposed to achieve improved performance, such as yielding tighter confidence intervals and thus higher secret key rates [94, 97, 98].

4.3 Information Reconciliation

The objective of the Information Reconciliation (IR) process is to enable Alice and Bob to share a set of completely consistent key bits, even in the presence of inevitable discrepancies introduced during quantum transmission, whether caused by the physical characteristics of the channel or by eavesdropping attempts from third parties. To achieve this goal, classical error-correcting codes (EECs) are employed, allowing the identification and correction of discrepancies between the bit sequences initially obtained by each party. In this way, IR serves as a fundamental step to ensure the reliability of the final keys, reducing inconsistencies and guaranteeing the secure sharing of common keys [5].

However, the IR of CV-QKD is particularly challenging due to its operation in low SNR regimes over long distances. In addition to the incorporation of a digital signal processing (DSP) stage, the effective application of ECCs requires the development of novel design, optimized code designs that generate LDPC matrices suitable for real-time hardware implementation, with reduced latency and high throughput. Under low-SNR conditions, LDPC codes demand a high degree of redundancy to reliably correct errors and enhance the key parameters used to evaluate IR performance namely: reconciliation efficiency (β), frame error rate (FER) and throughput (T). The first is used to characterize the efficiency of the error correction and expressed by a factor $\beta \in [0, 1]$, the second indicates the probability of IR failure (with lower values being preferable), and the third is directly associated with process performance, measuring the number of raw key bits processed per unit of time. In CV-QKD, given the transmission distance, higher reconciliation efficiency enables higher key rate [41].

Reconciliation can be implemented in two distinct forms with different performance characteristics: direct reconciliation (DR) or reverse reconciliation (RR). In DR, Alice sends

[3] More formally, the samples are a sequence of independent and identically distributed random variables.

the redundant information required for error correction to Bob, who uses it to correct the errors in his data and obtain a bit string identical to Alice's. In RR, Bob's raw keys serve as the reference, and he sends the necessary error correction information to Alice enabling her to adjust her bit string to match his. RR can significantly extend the transmission distance and enable the generation of secure keys over longer ranges, making it the dominant approach.

The raw keys in CV-QKD are Gaussian variables, and several schemes have been proposed for their reconciliation. The most well-known are slice reconciliation, multidimensional reconciliation and signal reconciliation.

- **Slice Reconciliation** - Suitable for relatively high SNR (greater than 0dB), typically in short transmission distances. In RR, Bob applies a quantization function $\mathcal{Q} : \mathbb{R} \to \{0,1\}^m$ to transform each Gaussian variable Y_i into an m-bit label $\{B_j(Y_i)\}$, $j = 1, ..., m$. Bob then employs a multi-level encoder, which encodes each bit level of the label independently as the syndromes of an ECC with coding rate R_j $(1 \leq j \leq m$. To recover Bob's m-bit label B_j. Alice uses a multi-stage decoder, leveraging her own correlated varaible X as side information. As a result, both parties ultimately share identical keys.
- **Multidimensional Reconciliation** - Suitable for low SNR (from -20dB to 0dB), typically occurring in long-distance CV-QKD. In this scenarios the raw keys of Alice and Bob are correlated Gaussian variables and the SNR will be very low for long transmission distances. In this case, the raw keys have a small absolute value and are distributed around 0. Thus, it is difficult to discriminate the sign and realize the encoding and decoding. The multidimensional reconciliation algorithm provides a powerful encoding scheme for low SNR scenario and thus effectively extend the key distribution distance. The channel between Alice and Bob is converted into a virtual biary input additive white Gaussian noise (AWGN) channel and therefore efficient binary codes can be employed.
- **Sign Reconciliation** - Direct encoding the continuous random variable to a key bit by using sign. The sign reconciliation has the feature of simplicity and low complexity, however the performance is low, due to some states are very close to each other, making discrimination difficult.

The Fig. 8 shows the four possibles states that Bob needs to discriminate [99]. Consider that Alice and Bob share a set of correlated Gaussian variables X and Y and x_1 e x_2 belong to **x**.

Multidimensional reconciliation has emerged as the most effective approach for low SNR regimes [99], such as those encountered in long-distance CV-QKD. As previously discussed, this technique enables the use of efficient binary codes, such as LDPC, thereby reducing the error rate and enhancing the SKR.

Since CV-QKD systems typically operate over Gaussian channels with very low SNRs, approximately below 0 dB, the initial bit error rate is consequently very high. To mitigate this, ECCs with strong decoding performance are required to detect and correct errors introduced during transmission, thereby improving reliability. Most notably, LDPC codes, defined by sparse parity-check matrices H of size $(n-k) \times n$, with code rate $R_{code} = \frac{k}{n}$. As mentioned earlier, in low-SNR regimes, very high redundancy is required to achieve reliable reconciliation, leading to large matrix dimensions (on the order of 10^6) and significant computational burden during decoding. This complexity negatively impacts the performance of the decoding algorithm named

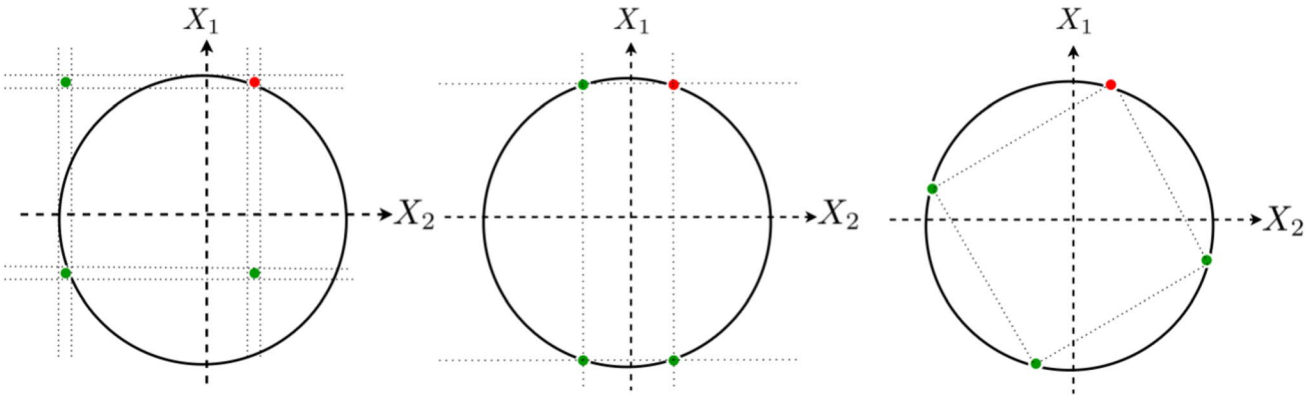

Fig. 8 Figures (**a**), (**b**), and (**c**) illustrate the four possible states that Bob must discriminate after Alice sends side information through the authenticated classical channel. In (**a**), corresponding to slice reconciliation, the four states are well separated, but the Gaussian symmetry is broken. In (**b**), representing sign reconciliation, the problem's symmetry is preserved, but some states are very close to each other, making discrimination difficult. In (**c**), corresponding to multidimensional reconciliation, a clever rotation is applied: the symmetry of the problem is preserved and the states become well to discriminate

as Belief Propagation (BP) and limits the real-time SKR, posing major challenge to the scalability of CV-QKD systems. Consequently, the design of LDPC code structures optimized for low-SNR and efficient hardware implementation is essential for advancing practical CV-QKD deployments [41].

LDPC codes are among the most promising strategies for application in the IR stage, as they enable performance close to the Shannon limit and are extensively employed in noisy communication systems. The parity-check matrix H can be represented by a bipartite Tanner graph, denoted as $\mathcal{G}$, composed of two sets of nodes: the variable nodes V_j, associated with the columns of H, and the check nodes C_i, corresponding to its rows [100]. A connection between a variable node j and a check node i is established when $H(i,j) = 1$, indicating an edge between the nodes. The number of edges incident to a vertex of $\mathcal{G}$ is referred to as its degree, and the degree distribution is defined by two polynomials, $\lambda(x) = \sum_i \lambda_i x^i$ and $\rho(x) = \sum_i \rho_i x^i$, where λ_i and ρ_i denote the fraction of variable and check nodes of degree i, respectively [100].

Alternative design approaches, for these codes are required in IR. In this context, Multi-Edge Type LDPC (MET-LDPC) proposed in [101], generalize both irregular and irregular LDPC codes by introducing multiple edges types in the Tanner graph, allowing greater flexibility in defining the degree distribution of the nodes. This unified structure enables efficient modeling of codes with both uniform and non-uniform distributions, adapting them to varying channel conditions. A key advantage of MET-LDPC codes over conventional LDPC codes is their ability to achieve performance close to Shannon limit, particularly in low-rate regimes such as IR in CV-QKD systems, where they operate robustly even under extremely low SNR conditions. In addition, the LDPC Quasi-cyclic codes (QC-LDPC) represents a structure LDPC code class, in which the parity-check matrix H is built from circulate blocks permutations of identity matrix. This structure allows a compact representation, facilitating efficient hardware implementations and significantly reducing the computational cost of encoding and decoding, which is essential for CV-QKD systems with large block sizes [46, 102]. These combined techniques can serve as a foundation for constructing codes applicable to various practical scenarios, including the optimization of IR in CV-QKD systems operating at very low SNRs, thereby extending the range and efficiency of QKD on long-distance optical communications.

4.4 Privacy Amplification

Privacy amplification (PA) is integrated into the post-processing flow of CV-QKD systems, acting as the mechanism that converts the reconciled key into a final key uniformly random and entirely independent of any quantum system E accessible to an eavesdropper [5, 103]. After the phases of *sifting* (for discrete-variable protocols) or the conversion of continuous variables into binary bits (for CV-QKD), and the information reconciliation stage, Alice and Bob share a bit sequence that, although corrected, may still contain information potentially accessible to an eavesdropper (Eve) [104]. The primary goal of PA is to compress the corrected sequence using a universal hash function into a significantly shorter sequence, thereby reducing Eve's knowledge of the final key to an arbitrarily small level. This process is essential, since any residual base error rate is indistinguishable from eavesdropping, requiring that Eve's information be either removed or rendered useless. The derivation of the final secure key length is extensively discussed in security analyses that take into account correctness and secrecy requirements [44, 103, 105].

The computational challenges in implementing PA are multifaceted and critical to the practical feasibility of high-speed CV-QKD systems. The complexity of universal hash algorithms is a limiting factor: while direct matrix multiplication has a computational complexity of $O(N^2)$, techniques such as Toeplitz matrices, optimized by number-theoretic transforms (NTT) or fast Fourier transforms (FFT), can reduce this complexity to $O(N \log N)$ [103]. However, these techniques produce uniform distributions only at the asymptotic regime, such that finite size effects of the order $O(n^{-1} \log_2(1/\epsilon_h))$ must be taken into account, where ϵ_h is the hashing parameter [106]. To mitigate these effects, which inevitably reduce the secure key rate, the PA block size (input length, N) should be as large as possible, ideally 10^8 bits or more (e.g., $10^9, 10^{10}$), to effectively counter finite-size effects, improve the secure key rate, and approach asymptotic performance [5, 104, 107]. The need for processing rates on the order of gigabits per second (Gbps) is driven by the increasing repetition rates of CV-QKD systems and the adoption of wavelength-division multiplexing (WDM), which boosts raw key rates to unprecedented levels [104].

Given the large block sizes and stringent throughput requirements, real-time execution of privacy amplification demands dedicated hardware support. Conventional software-based approaches are unable to maintain the data rates required when operating on blocks approaching hundreds of millions of bits. Section 5.1 provides a detailed examination of the hardware trade-offs and architectural strategies necessary to support PA alongside information reconciliation and digital signal processing.

The impact of finite-size effects on the final secure key rate is a significant theoretical and practical concern [107]. The security of CV-QKD is often analyzed in the asymptotic regime (infinite key length), but in practical scenarios,

the key length is finite, leading to a reduction in the actual secure key rate. This reduction becomes more pronounced as part of the data must be allocated to parameter estimation, and statistical fluctuations grow with smaller block sizes. To mitigate these effects, it is essential to maximize the block length used for key generation, which in turn requires PA algorithms capable of processing extremely large data blocks. Simulations indicate that the improvement in secure key rate due to large-scale PA is particularly pronounced in CV-QKD systems, where finite-size effects are more critical than in DV-QKD [104].

5 Hardware Development

The practical viability of CV-QKD systems, which can operate in real-time and over long distances, fundamentally depends on overcoming significant computational challenges. The DSP and post-processing stages, which ensure the key's security, require handling enormous volumes of data under low SNR conditions. To meet this demand, the development of dedicated hardware is necessary, as off-the-shelf solutions like CPUs and GPUs do not offer the required combination of performance, low power consumption, and latency to enable compact and integrable CV-QKD devices capable of generating keys in real-time on existing network infrastructures and being mass-produced.

5.1 Digital Hardware Architecture

The need for a dedicated, programmable, and flexible accelerator hardware architecture is a prerequisite for building CV-QKD systems that can evolve with research. The main objective is to enable real-time key generation and the efficient processing of large data volumes, overcoming the computational bottlenecks imposed by processing long transmission frames, a direct consequence of low SNR in the quantum regime and long-distance communications. A well-defined architecture is essential not only to achieve the necessary performance but also to ensure that the system can adapt to the continuous theoretical and algorithmic innovations that characterize the field of quantum communication.

In contrast to the concise reference in Section 4.4, which addressed privacy amplification in isolation, the assessment presented here encompasses the complete digital processing chain of CV-QKD systems. This broader scope is essential to evaluate the architectural requirements for real-time operation under practical deployment conditions.

The computational demands of a CV-QKD system are extraordinarily high. Both the DSP modules, responsible for signal encoding and recovery, and the post-processing stages — parameter estimation, IR, and PA — require massive processing power. To ensure security and efficiency in noisy channels, it is necessary to process data blocks that can exceed 10^9 symbols [4, 69, 90]. Information reconciliation, for example, uses complex error correction codes (e.g., MET-LDPC) that operate on blocks of hundreds of millions of bits [46, 69], while privacy amplification performs hash operations on matrices of equally massive dimensions, making real-time processing a major challenge [5].

Off-the-shelf hardware solutions, such as CPUs and GPUs, are often insufficient to meet the stringent requirements of commercial CV-QKD systems, particularly for embedded or high-speed deployment [108–110]. Although GPUs provide substantial parallelism and have been successfully employed in experimental demonstrations [46, 111], their power consumption and latency characteristics limit their suitability for compact or energy-constrained applications. CPUs, in turn, lack the parallel processing capability needed to handle the data throughput in real-time. FPGAs emerge as a promising platform, combining low power consumption with the ability to efficiently manage both system control and computation, thereby facilitating integration with optical and electronic components [103, 104]. Nonetheless, on-chip memory availability remains a critical constraint for FPGA-based implementations operating on very large code blocks. External memory interfaces, such as DDR, may be employed to extend capacity, but careful architectural planning is required to avoid throughput degradation. Furthermore, a hybrid architecture can be a good approach to address this need while accommodating the evolution of algorithms. In such an approach, computationally intensive and stable operations, including LDPC decoding and hashing, are implemented as dedicated hardware accelerators, while algorithmically evolving components, such as DSP functions and parameter estimation, execute on programmable processors. Application-Specific Instruction-set Processors (ASIPs), typically based on RISC-V extensions [110, 112, 113], provide flexibility with a customized instruction set that accelerates key quantum-communication tasks without demanding hardware redesign.

Modularity is also an essential principle for an architectural concept. As CV-QKD theory continues to advance, DSP and post-processing algorithms are constantly being improved. A modular architecture allows individual system components to be updated or replaced independently. This partitioning strategy facilitates system maintenance and evolution, ensuring that the hardware platform can adapt to future generations of CV-QKD protocols.

The path for developing and implementing the digital hardware architecture should go through two distinct phases: prototyping and production. FPGAs are highly suitable for prototyping, validation, and integrated testing, owing to their reconfigurable nature and straightforward interface

with optoelectronic subsystems [81, 114]. After validating the concept on an FPGA, the final solution points towards the fabrication of an ASIC in the form of a SoC. This SoC would integrate the ASIPs and dedicated accelerators on a single chip, ensuring performance, low power consumption, and reduced unit cost necessary for mass production and the widespread adoption of CV-QKD technology.

5.2 Software Framework

The development of such complex and specialized hardware requires, as an indispensable prerequisite, a robust and validated reference model. To this end, the creation of a comprehensive software framework is fundamental. This framework, named CV-QKD-ModSim, has been designed to model, simulate, and validate the entire digital information processing chain of a CV-QKD system, serving as a solid foundation and a blueprint for the hardware microarchitecture design. It allows exploring the design space and optimizing algorithms before committing resources to physical implementation.

The framework executes all digital processing steps, from the transmitter to the receiver. It simulates the DSP algorithms in Alice, such as pulse shaping and pilot tone multiplexing, and in Bob, such as clock recovery, equalization, and phase recovery. Furthermore, it models the signal propagation through the quantum channel, incorporating realistic effects like attenuation and excess noise from various sources, including laser phase noise and electronics imperfections. The framework implements the entire post-processing pipeline, including shot-noise unit (SNU) calibration and normalization, parameter estimation [64], information reconciliation (e.g., LDPC codes), and privacy amplification to ensure the security of the keys.

One of the most critical functions of CV-QKD-ModSim is to serve as a reference for transitioning algorithms from a floating-point model to a fixed-point model. The analysis of the required bit resolution for the numerical representation of each variable in the system is a determining step for hardware design. Insufficient precision can compromise security and performance, while excessive precision leads to a waste of logic resources, memory, and power in the FPGA or ASIC. The framework enables bit-true simulation, measures the impact of quantization, and determines the lowest binary word resolution that still guarantees secure key generation, thereby optimizing the efficiency of the final implementation.

The complexity of CV-QKD systems lies in the interdependence of multiple configuration parameters that need to be optimized simultaneously to maximize the secret key rate. The software framework provides a controlled environment to perform this optimization. Through computationally efficient simulations, it is possible to conduct a broad search in the parameter space, such as modulation variance, transmission frame size (e.g., blocks of 10^8 up to 10^9 symbols), and pilot tone strategies, to identify the optimal configuration for different channel conditions and distance scenarios. This fine-tuning process in software accelerates research and development, avoiding the cost and time associated with experimental tests implemented directly in hardware [115, 116].

The CV-QKD-ModSim software framework, being developed within the QuIIN research group, constitutes a core element of our hardware-oriented design methodology. It supports algorithm exploration and optimization, provides a validated digital reference model, and allows quantitative assessment of accuracy and resource requirements before deployment on FPGA or ASIC devices.

The current version is an internal prototype under continuous refinement, with its DSP and post-processing modules being validated through theoretical consistency checks and comparison with offline key-generation experiments performed on optical testbeds. As the framework reaches maturity, a public release under an open-source license is planned, along with a dedicated publication presenting its architecture, validation methodology, and benchmarking results. This roadmap ensures a reliable reference model for hardware design while maintaining alignment with practical system constraints.

6 Perspectives

6.1 QuIIN's Perspectives

QuIIN's development plan for CV-QKD systems follows a staged approach toward practical deployment in real-world metropolitan networks. Our implementation will employ Gaussian modulation with heterodyne (dual-quadrature homodyne) detection. As a proof of concept, we will initially perform offline key extraction with GPU-accelerated processing, leveraging the frameworks discussed in Section 5.2. The second phase involves prototyping a digital hardware FPGA/ASIC accelerator (see Section 5.2) for real-time secret key generation. Following laboratory validation, we plan to conduct field tests on an operational metropolitan quantum network in partnership with the Rio Quantum Network (RQN), a quantum communication network under deployment in Rio de Janeiro [2, 3]. The RQN infrastructure connects major research institutions through both fiber-optic and free-space optical (FSO) channels, providing an ideal testbed for comprehensive evaluation of CV-QKD performance under realistic metropolitan conditions.

The validation phase on the RQN will evaluate our CV-QKD system under realistic metropolitan network conditions. The RQN's heterogeneous topology presents significant engineering challenges that must be addressed for practical implementation. Fiber links introduce chromatic dispersion and polarization mode dispersion that require compensation, while FSO segments face atmospheric attenuation, turbulence-induced beam wander, and pointing stability issues. Additionally, maintaining synchronization across the heterogeneous network poses a fundamental challenge. Characterizing system performance under these variable conditions is essential for validating the technology's readiness for broader deployment.

Following the RQN validation, our efforts will focus on optimizing FSO link performance to enable scaling beyond metropolitan networks. Key objectives include improving link margin, reducing beam divergence, and enhancing tracking accuracy through refined adaptive optics systems and robust modulation techniques that mitigate atmospheric effects. These improvements are necessary steps toward establishing reliable long-distance quantum channels that can support a future national quantum network infrastructure in Brazil, transitioning from isolated metropolitan deployments to integrated wide-area quantum communications.

Looking beyond the RQN validation phase, our research roadmap includes the investigation of CV-QKD applications in more challenging scenarios. Mobile platforms such as unmanned aerial vehicles (UAVs) represent an intermediate step toward space-based quantum communication, introducing engineering challenges including precision tracking of moving nodes, vibration compensation, and terminal miniaturization. Similarly, satellite-to-ground quantum links would enable global-scale secure communications but require significant advances in adaptive optics and link acquisition. These directions represent natural extensions of our FSO optimization efforts, though they remain subjects for future investigation as terrestrial CV-QKD technology reaches maturity.

6.2 Scalability of Quantum Network

The transition from isolated metropolitan quantum networks to a fully integrated national quantum infrastructure represents the next critical frontier for quantum communication in Brazil. While metropolitan networks in Rio de Janeiro, Recife, and São Carlos demonstrate QKD viability on a local scale, their interconnection across Brazil's vast and geographically diverse territory presents significant challenges due to distance limitations and exponential signal attenuation in optical fibers. Achieving national scalability requires moving beyond terrestrial fiber optics toward a multi-layer hybrid network architecture that integrates optical fibers, FSO links–including those enabled by drone-mounted or high-altitude platform station (HAPS) systems–and satellite-based quantum communication.

Long-haul FSO links represent the foundational step for national scalability, bridging intermediate distances between metropolitan areas or reaching regions where trenching fiber is impractical or prohibitively expensive. The partnership between QuIIN and the RQN, which plans to test a CV-QKD system over an 800-meter channel combining fiber and FSO, serves as a pilot for assessing CV-QKD performance under real-world FSO conditions characterized by atmospheric turbulence, scintillation, and variable attenuation [117].

For distances beyond a few hundred kilometers and coverage of remote regions, UAVs and HAPS offer dynamic and flexible solutions. Drone-based optical terminals can act as mobile trusted nodes, creating reconfigurable aerial mesh networks. The mobility of drones mitigates the challenge of maintaining line-of-sight for ground FSO by adapting to changing conditions. This layer can provide, for instance, rapid deployment for emergency communications and extend coverage to rural areas.

Ultimately, satellite-based QKD provides the enabling layer for continental-scale coverage. As demonstrated by satellites such as Micius and Jinan-1, space-based links are the only viable technology for distributing keys over thousands of kilometers, connecting nodes across the entire national territory without requiring numerous intermediate trusted nodes [118]. For Brazil, the choice between Low Earth Orbit (LEO) and Geostationary Orbit (GEO) satellites involves critical trade-offs. LEO satellites offer lower transmission losses but require complex tracking systems and handover protocols, which can introduce disruptions to the key stream [119, 120]. Conversely, GEO satellites provide stable, persistent links over vast geographic areas, which is highly advantageous for the prolonged interactive exchanges required by CV-QKD post-processing algorithms [121]. However, this stability comes at the cost of significantly higher channel losses, demanding highly optimized systems with ultra-low noise detection [122]. CV-QKD's coherent detection mechanism offers advantages in this space environment, as its narrow-band local oscillator inherently rejects broad-spectrum background radiation, enabling robust daytime operation and under strong stray light conditions [123].

Realizing a scalable national quantum network requires a coordinated, multi-phase approach. This includes consolidating and standardizing existing metropolitan networks to ensure interoperability through common protocols and hardware interfaces. A strategic hybrid backbone must integrate fixed FSO links for inter-city connections alongside drone and HAPS-based networks for flexible coverage.

Concurrently, developing the space segment through national satellite capabilities or international partnerships is essential to secure space-based QKD resources. Thus, it requires determining the optimal orbital configuration, balancing LEO and GEO options, based on a thorough analysis of Brazil's specific needs for coverage, key rates, and latency requirements.

Finally, intelligent network management through sophisticated control plane software will dynamically route quantum key traffic across the hybrid ecosystem, continuously evaluating real-time channel conditions, weather data, and security requirements to select the most efficient and secure transmission path available among fiber, FSO, drone, and satellite links.

7 Conclusion

A century after quantum mechanics revolutionized our understanding of nature, we witness its transformation from theoretical framework to technological infrastructure. The second quantum revolution has matured from conceptual promise to engineering challenge. CV-QKD exemplifies this evolution, bridging quantum principles with classical telecommunication systems to deliver practical quantum security.

Realizing practical CV-QKD systems requires navigating substantial technical challenges across multiple layers. In this article, we have addressed these challenges comprehensively, from physical layer implementations to post-processing algorithms and hardware platforms. At the physical layer, the optical system must maintain phase stability while operating at extremely low SNR, where quantum effects dominate. Digital signal processing becomes critical for mitigating impairments in fiber links: chromatic dispersion and the ubiquitous phase noise that threatens coherent detection. Moving from offline GPU-accelerated post-processing to real-time FPGA-based key extraction demands not only computational power but algorithmic optimization that preserves security while maximizing throughput.

QuIIN's roadmap for developing Brazil's first CV-QKD system—from laboratory validation to field deployment on the RQN metropolitan infrastructure—directly confronts the gap between controlled environments and operational networks. Testing over real fiber infrastructure with unknown conditions will provide essential validation of CV-QKD's practical viability. Building a robust quantum technology ecosystem, however, requires more than infrastructure investment—it demands cultivating expertise that spans quantum fundamentals and engineering practice. Brazil's quantum future depends on professionals capable of navigating both domains: understanding the physics that governs secret key rates while engineering systems that operate reliably within practical and economic constraints.

As CV-QKD systems progress from research demonstrations to operational deployments, the challenges shift from "can it work?" to "can it scale?" The integration of quantum and classical systems, the coexistence with conventional data traffic, and the development of network protocols for quantum key management all require solutions grounded in both quantum theory and telecommunications engineering. As we mark this centennial of quantum mechanics, Brazil faces a defining choice in quantum technology development. The networks being deployed, the systems being engineered, and the professionals being trained today will determine whether Brazil contributes to or merely adopts quantum-secured communications infrastructure.

Acknowledgements This work was partially funded by the projects: *Non-conventional Receivers for CV-QKD, HW DSP: Development and Prototyping of Multicore SoC with Dedicated Accelerators and RISC-V DSP, Offline Demonstration for CV-QKD systems and LDPC Code Design for Information Reconciliation in CV-QKD Optimized for Hardware Implementation* supported by QuIIN – Quantum Industrial Innovation, the EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Industry 4.0 of the MCTI, grant number 053/2023, signed with EMBRAPII. MAD thanks financing from the European Union (HORIZON-MSCA-2023 Postdoctoral Fellowship, 101153602 - COCoVaQ).

Author Contributions A.B.T. and D.J.G.de.S. wrote the Introduction. M.A.D. prepared the Overview on CV-QKD Systems. C.M.S.N. wrote the Physical Layer section. D.J.G.de.S., N.A.F.N., L.Q.G., and M.Q.N.N. prepared the Post-processing Pipeline. D.J.G.de.S. and N.A.F.N. developed the Hardware Development section. B.P.da.S. and C.C.S. wrote QuIIN's Perspectives. Conceptualization was carried out by A.B.T., D.J.G.de.S. and V.L.da.S. All authors reviewed and approved the final version of the manuscript.

Funding The Article Processing Charge (APC) for the publication of this research was funded by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) (ROR identifier: 00x0ma614). This work was partially funded by the projects, HW DSP: Development and Prototyping of Multicore SoC with Dedicated Accelerators and RISC-V DSP, Offline Demonstration for CV-QKD systems and LDPC Code Design for Information Reconciliation in CV-QKD Optimized for Hardware Implementation supported by QuIIN – Quantum Industrial Innovation, the EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Industry 4.0 of the MCTI, grant number 053/2023, signed with EMBRAPII. MD thanks financing from the European Union (HORIZON-MSCA-2023 Postdoctoral Fellowship, 101153602 - COCoVaQ).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

1. I.H. Deutsch, Harnessing the power of the second quantum revolution. PRX Quantum. **1**, 020101 (2020). https://doi.org/10.1103/PRXQuantum.1.020101
2. Brazil's first quantum cryptography network is expected to connect five research institutions (2024). https://revistapesquisa.fapesp.br/en/brazils-first-quantum-cryptography-network-is-expected-to-connect-five-research-institutions/. This story was published with the title "Qubits in Guanabara" in Revista Pesquisa FAPESP, issue 342
3. G. Temporão, F. Melo, A. Khoury, The rio quantum network: a reconfigurable hybrid multi-user metropolitan quantum key distribution network. In: Anais do I Workshop de Redes Quânticas, pp. 19–24. SBC, Porto Alegre, RS, Brasil (2024). https://doi.org/10.5753/wqunets.2024.2872
4. S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J.L. Pereira, M. Razavi, J.S. Shaari, M. Tomamichel, V.C. Usenko, G. Vallone, P. Villoresi, P. Wallden, Advances in quantum cryptography. Adv. Opt. Photon. **12**(4), 1012–1236 (2020). https://doi.org/10.1364/AOP.361502
5. Y. Zhang, Y. Bian, Z. Li, S. Yu, H. Guo, Continuous-variable quantum key distribution system: Past, present, and future. Appl. Phys. Rev. **11**(1) (2024)
6. H.-Z. Chen, M.-H. Li, Y.Z. Wang, Z.-G. Zhao, C. Ye, F.L. Li, Z. Chen, S.-L. Han, B. Tang, Y.J. Miao, et al., Implementation of carrier-grade quantum communication networks over 10000 km. NPJ Quantum Information **11**(1), 137 (2025)
7. Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.X. Ng, L. Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Commun. Surv. Tutor. **24**(2), 839–894 (2022). https://doi.org/10.1109/COMST.2022.3144219
8. S.-H. Wei, B. Jing, X.-Y. Zhang, J.-Y. Liao, C.-Z. Yuan, B.-Y. Fan, C. Lyu, D.-L. Zhou, Y. Wang, G.-W. Deng et al., Towards real-world quantum networks: a review. Laser & Photon. Rev. **16**(3), 2100219 (2022)
9. J. Liu, T. Le, T. Ji, R. Yu, D. Farfurnik, G. Byrd, D. Stancil, The road to quantum internet: Progress in quantum network testbeds and major demonstrations. Prog. Quantum Electron. **99**, 100551 (2025)
10. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Satellite-to-ground quantum key distribution. Nature **549**(7670), 43–47 (2017). https://doi.org/10.1038/nature23655
11. J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Satellite-based entanglement distribution over 1200 kilometers. Science **356**(6343), 1140–1144 (2017). https://doi.org/10.1126/science.aan3211
12. J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Ground-to-satellite quantum teleportation. Nature **549**(7670), 70–73 (2017). https://doi.org/10.1038/nature23675
13. Li, Y. Cai, W.-Q. Ren, J.-G. Wang, C.-Z. Yang, M. Zhang, L. Wu, H.-Y. Chang, L. Wu, J.-C. Jin, B. et al., Microsatellite-based real-time quantum key distribution. Nature 47–54 (2025)
14. Bedington, R. Arrazola, J.M. Ling, A. Progress in satellite quantum key distribution. NPJ Quantum Inf. **3**(1) (2017). https://doi.org/10.1038/s41534-017-0031-5
15. C.H. Bennett, G.Brassard, Quantum cryptography: Public key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, pp. 175–179 (1984)
16. H. Wang, Y. Li, T. Ye, L. Ma, Y. Pan, M. Wu, J. Li, Y. Bian, Y. Pi, Y. Shao, J. Yang, J. Liu, A. Sun, W. Huang, S. Pirandola, Y. Zhang, B. Xu, High-rate continuous-variable quantum key distribution over 100 km fiber with composable security (2025). arXiv:2503.14843
17. A.A.E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U.L. Andersen, T. Gehring, Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. Sci. Adv. **10**(1), 9474 (2024). https://doi.org/10.1126/sciadv.adi9474
18. A.A.E. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U.L. Andersen, X. Yin, T. Gehring, Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver **11**(9), 1197. https://doi.org/10.1364/OPTICA.530080
19. A.A.E. Hajomer, A. Bomhals, C. Bruynsteen, A. Sidhique, I. Derkach, U.L. Andersen, X. Yin, T. Gehring, Chip-Based 16 GBaud Continuous-Variable Quantum Key Distribution (2025). arXiv:2504.09308
20. A.A.E. Hajomer, I. Derkach, V.C. Usenko, U.L. Andersen, T. Gehring, Coexistence of continuous-variable quantum key distribution and classical data over 120-km fiber (2025). arXiv:2502.17388
21. M.F. Anka, J.A.M. Rodríguez, D.F. Pinto, L.Q. Galvão, M.A. Dias, A.B. Tacla, An introductory review of the theory of continuous-variable quantum key distribution: Fundamentals, protocols, and security (2025). arXiv:2512.01758
22. F. Laudenbach, C. Pacher, C.-H.F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel, Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations. Adv. Quantum Technol. **1**(1), 1800011 (2018)
23. I.B. Djordjevic, Physical-Layer Security and Quantum Key Distribution, 1st edn. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27565-5
24. C. Weedbrook, S. Pirandola, R. García-Patrón, N.J. Cerf, T.C. Ralph, J.H. Shapiro, S. Lloyd, Gaussian quantum information. Rev. Mod. Phys. **84**(2), 621–669 (2012)
25. V.C. Usenko, A. Acín, R. Alléaume, U.L. Andersen, E. Diamanti, T. Gehring, A.A.E. Hajomer, F. Kanitschar, C. Pacher, S. Pirandola, V. Pruneri, Continuous-variable quantum communication (2025). arXiv:2501.12801

26. E. Diamanti, A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations. Entropy **17**(9), 6072–6092 (2015). https://doi.org/10.3390/e17096072
27. V.L. Sena, F. Melo, M.A. Dias, A.B. Tacla, R. Chaves, Um tutorial sobre distribuição quântica de chaves: dos fundamentos às tecnologias modernas. Revista Brasileira de Ensino de Física **47**, 20250373 (2025)
28. C.E. Shannon, Communication Theory of Secrecy Systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
29. M. Manimozhi, R.K. Mugelan, Post-quantum AES encryption using ECC points derived from BB84 sifted keys. EPJ Quantum Technol. **12**(1), 109 (2025). https://doi.org/10.1140/epjqt/s40507-025-00411-9
30. Q. Zhang, H. Lai, J. Pieprzyk, Quantum-key-expansion protocol based on number-state-entanglement-preserving tensor network with compression. Phys. Rev. A **105**(3), 032439 (2022). https://doi.org/10.1103/PhysRevA.105.032439
31. V. Usenko, R. Filip, Trusted Noise in Continuous-Variable Quantum Key Distribution A Threat and a Defense. Entropy **18**(1), 20 (2016). https://doi.org/10.3390/e18010020
32. F. Grosshans, P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett. **88**(5), 57902 (2002). https://doi.org/10.1103/PhysRevLett.88.057902
33. C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, P.K. Lam, Quantum cryptography without switching. Phys. Rev. Lett. **93**, 170504 (2004). https://doi.org/10.1103/PhysRevLett.93.170504
34. S. Ghorai, P. Grangier, E. Diamanti, A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. Phys. Rev. X **9**(2), 021059 (2019). https://doi.org/10.1103/PhysRevX.9.021059
35. I.B. Djordjevic, Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols. IEEE Photonics J. **11**(4), 1–10 (2019). https://doi.org/10.1109/JPHOT.2019.2921521
36. A. Denys, P. Brown, A. Leverrier, Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum **5**, 540 (2021). https://doi.org/10.22331/q-2021-09-13-540
37. G.V. Assche, J. Cardinal, N.J. Cerf, Reconciliation of a quantum-distributed Gaussian key. IEEE TIT **50**(2), 394–400 (2004). https://doi.org/10.1109/tit.2003.822618
38. N. Jain, 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, U.L. Andersen, Practical continuous-variable quantum key distribution with composable security. Nat. Commun. **13**(1) (2022). https://doi.org/10.1038/s41467-022-32161-y
39. A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states. Phys. Rev. Lett. **114**(7) (2015). https://doi.org/10.1103/physrevlett.114.070501
40. Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus, G. Leuchs, Continuous variable quantum cryptography beating the 3 dB loss limit. Phys. Rev. Lett. **89**(16), 167901 (2002). https://doi.org/10.1103/PhysRevLett.89.167901
41. S. Yang, Z. Yan, H. Yang, et al., Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications. EPJ Quantum Technol. **10**, 40 (2023). https://doi.org/10.1140/epjqt/s40507-023-00197-8
42. Z. Chen, X. Wang, S. Yu, Z. Li, H. Guo, Continuous-mode quantum key distribution with digital signal processing. NPJ Quantum Inf. **9**(1), 28 (2023)
43. D.B.S. Soh, C. Brif, P.J. Coles, N. Lütkenhaus, R.M. Camacho, J. Urayama, M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. Phys. Rev. X **5**(4) (2015). https://doi.org/10.1103/physrevx.5.041010
44. F. Roumestan, A. Ghazisaeidi, J. Renaudier, L.T. Vidarte, E. Diamanti, P. Grangier, High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In: 2021 European Conference on Optical Communication (ECOC), pp. 1–4 (2021). IEEE
45. D. Pereira, M. Almeida, M. Facão, A.N. Pinto, N.A. Silva, Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres. Opt. Lett. **47**(15), 3948 (2022). https://doi.org/10.1364/OL.456333
46. M. Milicevic, C. Feng, L.M. Zhang et al., Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography. NPJ Quantum Inf. **4**, 21 (2018). https://doi.org/10.1038/s41534-018-0070-6
47. Z. Bai, S. Yang, Y. Li, High-efficiency reconciliation for continuous variable quantum key distribution. Jpn. J. Appl. Phys. **56**(4), 44401 (2017). https://doi.org/10.7567/jjap.56.044401
48. V.C. Usenko, Unidimensional continuous-variable quantum key distribution using squeezed states. Phys. Rev. A **98**(3), 032321 (2018)
49. H.Q. Nguyen, I. Derkach, H.-M. Chin, A.A.E. Hajomer, A. Oruganti, R. Filip, U.L. Andersen, V.C. Usenko, T. Gehring, Practical continuous-variable quantum key distribution with squeezed light (2025). arXiv:2506.19438
50. H.Q. Nguyen, Practical continuous variable quantum key distribution with squeezed light. Ph.d. dissertation, Technical University of Denmark, Lyngby, Denmark (2025)
51. A. Oruganti, I. Derkach, R. Filip, V.C. Usenko, Continuous-variable quantum key distribution with noisy squeezed states. Quantum Sci. Technol. **10**(2), 025023 (2025)
52. F. Grosshans, P. Grangier, Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**, 057902 (2002). https://doi.org/10.1103/PhysRevLett.88.057902
53. B. Qi, P. Lougovski, R. Pooser, W. Grice, M. Bobrek, Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X **5**(4), 041009 (2015)
54. P. Jouguet, S. Kunz-Jacques, E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A-Atomic, Mol. Opt. Phys. **87**(6), 062313 (2013)
55. M. Ghalaii, S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution in free-space channels. Phys. Rev. A **108**(4), 042621 (2023)
56. I.B. Djordjevic, Physical-layer security, quantum key distribution, and post-quantum cryptography, 2nd edn. Springer (2025). https://doi.org/10.1007/978-3-031-88372-9
57. A. Redyuk, O. Sidelnikov, M. Fedoruk, Compensation of nonlinear signal distortions in optical fiber communication systems. Opt. Commun. **578**, 131418 (2025)
58. J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, H. Zeng, Stable quantum key distribution with active polarization control based on time-division multiplexing. New J. Phys. **11**(6), 065004 (2009)
59. C.H. Park, M.K. Woo, B.K. Park, Y.-S. Kim, H. Baek, S.-W. Lee, H.-T. Lim, S.-W. Jeon, H. Jung, S. Kim et al., 2× n twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing. NPJ Quantum Inf. **8**(1), 48 (2022)
60. D. Pereira, A.N. Pinto, N.A. Silva, Polarization diverse true heterodyne receiver architecture for continuous variable quantum key distribution. J. Lightwave Technol. **41**(2), 432–439 (2023). https://doi.org/10.1109/JLT.2022.3216754
61. P. Gavignet, E. Pincemin, F. Herviou, Y. Loussouarn, F. Mondain, A. Grant, L. Johnson, R.I. Woodward, J.F. Dynes, B. Summers et al., Co-propagation of qkd & 6 tb/s (60 × 100g) dwdm channels with 17 dbm total wdm power in single and multi-spanconfigurations. J. Lightwave Technol. 42(4), 1321–1327 (2023)

62. L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen et al., Long-distance copropagation of quantum key distribution and terabit classical optical data channels. Phys. Rev. A **95**(1), 012301 (2017)
63. S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. Phys. Rev. Res. **3**, 043014 (2021). https://doi.org/10.1103/PhysRevResearch.3.043014
64. L.Q. Galvão, D.J.G. Sousa, M.A. Dias, N.A.F. Neto, Neural network for excess noise estimation in continuous-variable quantum key distribution under composable finite-size security (2025). arXiv:2507.23117
65. V.L. Silva, M.A. Dias, N.A.F. Neto, A.B. Tacla, From coherent communications to quantum security: Modern techniques in cv-qkd. In: 2024 SBFoton International Optics and Photonics Conference (SBFoton IOPC), pp. 1–5 (2024). https://doi.org/10.1109/SBFotonIOPC62248.2024.10813518
66. M. Schiavon, Y. Piétri, L.T. Vidarte, D. Fruleux, M. Huguenot, B. Gouraud, A. Rhouni, P. Grangier, E. Diamanti, High-speed continuous-variable quantum key distribution with advanced digital signal processing. In: 2023 23rd International Conference on Transparent Optical Networks (ICTON), pp. 1–6 (2023). IEEE
67. D.A. Arruda Mello, F.A. Barbosa, Digital Coherent Optical Systems: Architecture and Algorithms, 1st edn. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-66541-8
68. F. Roumestan, A. Ghazisaeidi, J. Renaudier, L.T. Vidarte, A. Leverrier, E. Diamanti, P. Grangier, Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation. J. Lightwave Technol. **42**(15), 5182–5189 (2024)
69. A.A. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U.L. Andersen, X. Yin, T. Gehring, Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver. Optica **11**(9), 1197–1204 (2024)
70. D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, B. Schrenk, High rate cv-qkd secured mobile wdm fronthaul for dense 5g radio networks. J. Lightwave Technol. **39**(11), 3445–3457 (2021)
71. Y. Pan, H. Wang, Y. Shao, Y. Pi, T. Ye, S. Zhang, Y. Li, W. Huang, B. Xu, Simple and fast polarization tracking algorithm for continuous-variable quantum key distribution system using orthogonal pilot tone. J. Lightwave Technol. **41**(19), 6169–6175 (2023)
72. K. Xu, J. Song, Y. Li, J. Chen, J. Qiu, X. Hong, H. Guo, Z. Yang, J. Wu, Real-time low-complexity diversity combining algorithm for free space coherent optical communication systems over atmospheric turbulence channel. Opt. Express **31**(24), 40705–40716 (2023)
73. Y. Pan, M. Wu, H. Wang, Y. Shao, J. Liu, Y. Li, Y. Zhang, W. Huang, B. Xu, 100 km discrete-modulated continuous-variable quantum key distribution using probabilistic shaped 16qam. In: 2024 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC), pp. 1–5 (2024). IEEE
74. M. Qiao, Y. Wang, Z. Li, Y. Xiao, Y. Chen, Z. Li, D. Wang, Novel dispersion and timing estimation for weakly-coupled oam fiber transmission systems. IEEE Photonics Technol. Lett. **36**(14), 913–916 (2024)
75. J. Reis Frazão, V. Vliet, S. Heide, M. Hout, K. Gümüş A. Albores-Mejia, B. Okonkwo, C. Škorić, Real-time cv-qkd reception resilient to urban atmospheric turbulence. In: CLEO: Applications and Technology, pp. 3–1 (2024). Optica Publishing Group
76. T. Shen, X. Wang, Z. Chen, H. Tian, S. Yu, H. Guo, Experimental demonstration of llo continuous-variable quantum key distribution with polarization loss compensation. IEEE Photonics J. **15**(2), 1–9 (2023)
77. H.-M. Chin, N. Jain, U.L. Andersen, D. Zibar, T. Gehring, Digital synchronization for continuous-variable quantum key distribution. Quantum Sci. Technol. **7**(4), 045006 (2022)
78. P.J. Freire, A. Napoli, B. Spinnler, N. Costa, S.K. Turitsyn, J.E. Prilepsky, Neural networks-based equalizers for coherent optical transmission: Caveats and pitfalls. IEEE J. Sel. Topics Quantum Electron. **28**(4: Mach. Learn. in Photon. Commun. and Meas. Syst.), 1–23 (2022)
79. N. Alshaer, T. Ismail, H. Mahmoud, Enhancing performance of continuous-variable quantum key distribution (cv-qkd) and gaussian modulation of coherent states (gmcs) in free-space channels under individual attacks with phase-sensitive amplifier (psa) and homodyne detection (hd). Sensors **24**(16), 5201 (2024)
80. D. Jin, Y. Guo, Y. Wang, Y. Li, D. Huang, Key-sifting algorithms for continuous-variable quantum key distribution. Phys. Rev. A **104**(1), 012616 (2021)
81. G. Anjos, M. Almeida, J. Martins, N.A. Silva, N.J. Muga, A.N. Pinto, An fpga-based physical layer approach for a cv-qkd transmitter. In: 2023 23rd International Conference on Transparent Optical Networks (ICTON), pp. 1–4 (2023). IEEE
82. M. Iqbal, A. Villegas, M.S. Moreolo, L. Nadal, R. Muñoz, P. Adillon, S. Sarmiento, J. Tabares, S. Etcheverry, Sdn-enabled continuous-variable qkd in coexistence with 8× 200 gb/s 16-qam classical channels. In: 2024 International Conference on Optical Network Design and Modeling (ONDM), pp. 1–3 (2024). IEEE
83. A. Leverrier, F. Grosshans, P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution. Phys. Rev. A **81**, 062343 (2010). https://doi.org/10.1103/PhysRevA.81.062343
84. A.A.E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U.L. Andersen, T. Gehring, Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. Sci. Adv. **10**(1), 9474 (2024). https://doi.org/10.1126/sciadv.adi9474
85. D. Huang, P. Huang, D. Lin, G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci. Rep. **6**(1), 19201 (2016). https://doi.org/10.1038/srep19201
86. X.-Y. Wang, X.-B. Guo, Y.-X. Jia, Y. Zhang, Z.-G. Lu, J.-Q. Liu, Y.-M. Li, Accurate shot-noise-limited calibration of a time-domain balanced homodyne detector for continuous-variable quantum key distribution. J. Lightwave Technol. **41**(17), 5518–5528 (2023). https://doi.org/10.1109/JLT.2023.3264234
87. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, P. Grangier, Field test of a continuous-variable quantum key distribution prototype. New J. Phys. **11**(4), 045023 (2009). https://doi.org/10.1088/1367-2630/11/4/045023
88. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photonics **7**(5), 378–381 (2013). https://doi.org/10.1038/nphoton.2013.63
89. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, P. Painchault, Field test of classical symmetric encryption with continuous variables quantum key distribution. Opt. Express **20**(13), 14030–14041 (2012). https://doi.org/10.1364/OE.20.014030
90. Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, H. Guo, Continuous-variable qkd over 50 km commercial fiber. Quantum Sci. Technol. **4**(3), 035006 (2019). https://doi.org/10.1088/2058-9565/ab19d1
91. Y. Zhang, Y. Huang, Z. Chen, Z. Li, S. Yu, H. Guo, One-time shot-noise unit calibration method for continuous-variable quantum key distribution. Phys. Rev. Appl. **13**, 024058 (2020). https://doi.org/10.1103/PhysRevApplied.13.024058

92. G. Casella, R.W. Berger, Statistical Inference, 2nd edn. CRC Texts in Statistical Science. CRC Press, Boca Raton (2024). https://doi.org/10.1201/9781003456285
93. R.Y.Q. Cai, V. Scarani, Finite-key analysis for practical implementations of quantum key distribution. New J. Phys. **11**(4), 045024 (2009). https://doi.org/10.1088/1367-2630/11/4/045024
94. O. Thearle, S.M. Assad, T. Symul, Estimation of output-channel noise for continuous-variable quantum key distribution. Phys. Rev. A **93**, 042343 (2016). https://doi.org/10.1103/PhysRevA.93.042343
95. S. Pirandola, P. Papanastasiou, Improved composable key rates for cv-qkd. Phys. Rev. Res. **6**, 023321 (2024). https://doi.org/10.1103/PhysRevResearch.6.023321
96. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys. Rev. Lett. **125**, 010502 (2020). https://doi.org/10.1103/PhysRevLett.125.010502
97. W. Liu, P. Huang, J. Peng, J. Fan, G. Zeng, Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution. Phys. Rev. A **97**, 022316 (2018). https://doi.org/10.1103/PhysRevA.97.022316
98. H. Luo, Y.-J. Wang, W. Ye, H. Zhong, Y.-Y. Mao, Y. Guo, Parameter estimation of continuous variable quantum key distribution system via artificial neural networks. Chin. Phys. B **31**(2), 020306 (2022). https://doi.org/10.1088/1674-1056/ac2807
99. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, P. Grangier, Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. A **77**(4) (2008). https://doi.org/10.1103/physreva.77.042325
100. T.K. Moon, Error Correction Coding: Mathematical Methods and Algorithms, 1st edn. Wiley-Interscience, Hoboken, NJ (2005). https://doi.org/10.1002/0471739219
101. T. Richardson, R. Urbanke, Multi-edge type ldpc codes. ISIT talk (2002)
102. Y. Li, X. Zhang, Y. Li, B. Xu, L. Ma, J. Yang, W. Huang, High-throughput gpu layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems. Sci. Rep. **10**(1), 14561 (2020)
103. H. Li, A. Wonfor, A. Weerasinghe, M. Alhussein, Y. Gong, R. Penty, Quantum key distribution post-processing: A heterogeneous computing perspective. In: 2022 IEEE 35th International System-on-Chip Conference (SOCC), pp. 1–6 (2022). IEEE
104. B.-Z. Yan, Q. Li, H.-K. Mao, H.-W. Xu, A.A. Abd El-Latif, Large-scale and high-speed fpga-based privacy amplification for quantum key distribution. J. Lightwave Technol. **41**(1), 169–175 (2022)
105. F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, R.F. Werner, Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. Phys. Rev. Lett. **109**(10), 100502 (2012)
106. R. Konig, R. Renner, C. Schaffner, The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory **55**(9), 4337–4347 (2009). https://doi.org/10.1109/TIT.2009.2025545
107. S.-S. Yang, Z.-G. Lu, Y.-M. Li, High-speed post-processing in continuous-variable quantum key distribution based on fpga implementation. J. Lightwave Technol. **38**(15), 3935–3941 (2020)
108. S.-S. Yang, Z.-G. Lu, Y.-M. Li, High-speed post-processing in continuous-variable quantum key distribution based on fpga implementation. J. Lightwave Technol. **38**(15), 3935–3941 (2020). https://doi.org/10.1109/JLT.2020.2985408
109. J. Sun, H. Cheng, Z. Jin, Y. Chen, G. Chen, L. Ren, X. Jiang, A high-speed fpga implementation of the multidimensional reconciliation for continuous variables quantum key distribution. In: 2024 9th International Conference on Communication, Image and Signal Processing (CCISP), pp. 170–174 (2024). https://doi.org/10.1109/CCISP63826.2024.10765578
110. S.Q. Ng, F. Kanitschar, G. Zhang, C. Wang, Gigabit-rate Quantum Key Distribution on Integrated Photonic Chips (2025). arXiv:2504.08298
111. A. Weerasinghe, M. Alhussein, A. Alderton, A. Wonfor, R. Penty, Practical, high-speed Gaussian coherent state continuous variable quantum key distribution with real-time parameter monitoring, optimised slicing, and post-processed key distillation. Sci. Rep. **13**(1), 21543 (2023). https://doi.org/10.1038/s41598-023-47517-7
112. A. Waterman, Design of the risc-v instruction set architecture. PhD thesis, EECS Department, University of California, Berkeley (2016). http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-1.html
113. A. Dörflinger, M. Albers, B. Kleinbeck, Y. Guan, H. Michalik, R. Klink, C. Blochwitz, A. Nechi, M. Berekovic, A comparative survey of open-source application-class risc-v processor implementations. In: Proceedings of the 18th ACM International Conference on Computing Frontiers. CF '21, pp. 12–20. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3457388.3458657
114. G. Zhang, 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, A.Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat. Photonics **13**(12), 839–842 (2019). https://doi.org/10.1038/s41566-019-0504-5
115. Y. Piétri, M. Schiavon, V.M. Acosta, B. Gouraud, L.T. Vidarte, P. Grangier, A. Rhouni, E. Diamanti, Qosst: A highly modular open source platform for continuous variable quantum key distribution applications. In: Quantum 2.0 Conference and Exhibition, Technical Digest Series. Optica Publishing Group, Rotterdam, Netherlands (2024). https://doi.org/10.1364/QUANTUM.2024.QTh4B.4
116. S. Kreinberg, I. Koltchanov, P. Novik, S. Alreesh, F. Laudenbach, C. Pacher, H. Hübel, A. Richter, Modelling weak-coherent cv-qkd systems using a classical simulation framework. In: 2019 21st International Conference on Transparent Optical Networks (ICTON), pp. 1–4 (2019). https://doi.org/10.1109/ICTON.2019.8840253
117. S. Mantey, M. Fernandes, G. Fernandes, N. Silva, F. Guiomar, P. Monteiro, A. Pinto, N. Muga, On the coexistence of quantum and classical signal transmission over turbulent fso channels. J. Lightwave Technol. **43**(3), 1043–1050 (2025)
118. Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen et al., An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature **589**(7841), 214–219 (2021)
119. A. Alvaro, L. Pascual, A. Abad, P. Pinto, A. Alvarez-Herrero, T. Belenguer, C. Miravet, P. Campo, L.F. Rodriguez, M. Reyes, et al.: Caramuel: The future of space quantum key distribution in geo. In: 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS), pp. 57–65 (2022). IEEE
120. Y. Gao, G. Song, T. Zhu, Optimizing global quantum communication via satellite constellations (2024). arXiv:2501.00280
121. J. Cheng, Y. Chen, A. Liu, X. Sun, J. Guo, B. Yang, P. Yin, W. Liu, L. Chen, C. Dong, Feasibility and parameter optimization of ground-to-satellite uplink continuous-variable quantum key distribution. New J. Phys. **27**(2), 023011 (2025)
122. D. Orsucci, P. Kleinpaß, J.D. Meister, I. Marco, S. Häusler, T. Strang, N. Walenta, F. Moll, Assessment of practical satellite quantum key distribution architectures for current and near-future missions. Int. J. Satell. Commun. Network. **43**(3), 164–192 (2025)
123. I. Derkach, V.C. Usenko, Applicability of squeezed-and coherent-state continuous-variable quantum key distribution over satellite links. Entropy **23**(1), 55 (2020)