ACADEMIA QUANTUM

Research Article
Published: 2025-08-14
https://doi.org/10.20935/AcadQuant7844

Robust simulation of continuous-variable quantum key distribution in Matlab and Simulink

Shashank Gupta[1,2,*], Abhishek Mani Shukla[1], Arijit Roy[3], Sruthi Chennuri[1], Vijayalaxmi Mogligidda[1], Rajesh Kumar Krishnan[1], Dilip Singh[1]

Academic Editors: Salem Hegazy

Abstract

Continuous-variable quantum key distribution with coherent detection is widely acknowledged for its compatibility with contemporary optical communication technologies. However, the robustness of various modulation formats and detection procedures against high excess noise remains uncertain, posing a significant barrier to the widespread implementation of quantum key distribution networks. This paper introduces a Matlab and Simulink-based experimental simulator designed to analyze different modulation formats (Gaussian and discrete) and coherent detection techniques (homodyne, heterodyne, and intradyne). Our findings suggest that polarization-multiplexed quantum signals with discrete modulation and pilot tones exhibit greater resilience to experimental imperfections. Enhanced robustness can be achieved through post-selection. Furthermore, under conditions of trusted detector noise, intradyne detection proves more effective in mitigating various offsets between the two nodes, thereby resulting in an increased secret key rate. The secure key rate is determined using the Gaussian extremity theorem for Gaussian modulation and a strict numerical technique against collective attacks in the asymptotic regime for discrete modulation. The results demonstrate that the protocol enables key distribution over distances approaching intercity scales, thereby supporting the advancement of cost-effective quantum-secure communication networks.

Keywords: *quantum cryptography, quantum key distribution, quantum simulation, continuous-variable quantum system*

Citation: Gupta S, Shukla AM, Roy A, Chennuri S, Mogligidda V, Krishnan RK, et al. Robust simulation of continuous-variable quantum key distribution in Matlab and Simulink. *Academia Quantum* 2025;2. https://doi.org/10.20935/AcadQuant7844

1. Introduction

Secure communication is a cornerstone of modern society, with applications spanning civilian and military domains. Traditional encryption methods rely on the computational complexity of mathematical problems, such as factoring large integers [1]. However, the rise of quantum computing, coupled with algorithms like Shor's [2] and Grover's [3, 4], poses a significant threat to the security of classical cryptographic protocols. Quantum communication offers a transformative solution, providing security guarantees rooted in the fundamental principles of quantum mechanics. Among quantum communication protocols, the continuous-variable quantum key distribution (CV-QKD) [5–11] has emerged as a leading candidate for practical quantum cryptography. CV-QKD leverages the quadratures of coherent states to encode information, enabling higher key rates and seamless integration with existing telecommunication infrastructure. This compatibility positions CV-QKD as a promising approach for scalable and secure quantum communication networks [12–15].

Information is encoded into the quadrature components of weak coherent states to create the initial key in CV-QKD. Retrieval of information depends on coherent detection, which involves combining a strong local oscillator (LO) in a balanced beamsplitter with the weak quantum channel. The resulting optical power difference at the outputs corresponds to the quadrature (I or Q), determined by the LO's phase. PIN diodes, capable of power measurements at rates of up to 10 GHz, are employed for their cost efficiency and high detection rates, offering significant advantages over the lower-rate, less efficient avalanche photodiodes used in discrete-variable QKD. Coherent detection in CV-QKD operates in three configurations: homodyne ($f_T = f_{LO}$), intradyne ($|f_T - f_{LO}| < R_{sym}$), and heterodyne ($|f_T - f_{LO}| > R_{sym}$). Here, R_{sym} is the rate at which symbols are encoded on the quadratures of light. The signal and LO must have a steady frequency and phase relationship for all three configurations to work. The 'in-line LO' approach, using a shared laser source for both the signal and LO, ensures this stability and was pivotal in early CV-QKD implementations [16, 17]. However, joint transmission of the LO with the quantum signal introduces challenges, including LO power limitations due to channel loss, interference with dense wavelength-division multiplexing (DWDM) channels, and vulnerability to side-channel attacks on the LO [18–24].

To enable secure key exchange and ensure compatibility with telecom fibers, a locally generated local oscillator (LLO) is employed at the receiver for coherent detection. This approach utilizes independent signal and LO lasers, requiring precise phase and frequency synchronization. In classical communication, carrier-phase recovery typically relies on post-measurement adjustments to align data with reference phases, often derived directly from the data itself, as in quadrature amplitude modulation (QAM). Howe-

[1]QuNu Labs Pvt. Ltd., M. G. Road, Bengaluru, Karnataka, India.
[2]Okinawa Institute of Science and Technology Graduate University, Okinawa, Japan.
[3]Institute for Advancing Intelligence, TCG CREST, Kolkata, West Bengal, India.
*email: shashank@qnulabs.com

ver, in CV-QKD, the quantum signals are inherently weak, necessitating a distinct strategy. Here, Alice transmits a strong secondary signal containing phase information, enabling Bob to estimate and correct discrepancies between the independent lasers [25–32]. This reference signal facilitates continuous monitoring and compensation of phase drifts, ensuring robust detection. CV-QKD can be implemented in various configurations, including different quantum signal modulation formats and coherent detection schemes (heterodyne, intradyne, or homodyne). Experimentally or commercially analyzing these alternatives is resource-intensive. To address this, quantum communication simulation toolkits have emerged as a cost-effective solution, with several initiatives already advancing QKD research [33–38]. The modeling and simulation package we previously developed for our Armos QKD and quantum secure direct communication (QSDC) systems was based on Matlab. This simulation kit facilitates experimental simulations of real systems and evaluates differential phase-shift (DPS) QKD systems, incorporating realistic experimental imperfections [39–41]. For instance, it models temperature-induced shifts in laser wavelength, relative intensity noise, phase noise, and nonlinear effects in optical fibers, such as dispersion and Kerr nonlinearity. By extending this toolkit with additional modules for dual-polarization IQ modulation and optical hybrids, we provide a versatile platform for cost-efficient analysis of CV-QKD alternatives.

In this work, we introduce a paradigm shift by modeling, simulating, and analyzing a CV-QKD system, departing from traditional discrete-variable (DV) QKD or other discrete-variable communication tasks. This expansion broadens the scope of our simulator, enabling exploration of new horizons in QKD and quantum information theory. Our methodology offers fine-grained control over individual system components, enabling detailed analysis of the quantum signal at every stage of the protocol. This capability facilitates design improvements and parameter optimization, accounting for realistic experimental imperfections. The ultimate goal is to develop a comprehensive simulation package capable of precisely modeling, analyzing, and comparing a wide range of quantum communication tasks. For instance, the modulation format of the quantum signal can be altered simply by adjusting the RF signal driving the IQ modulator. Similarly, the coherent detection scheme—whether homodyne, heterodyne, or intradyne—can be modeled by varying the central wavelengths of the signal and local oscillator lasers. Furthermore, our simulator incorporates imperfections by tuning parameters such as temperature, laser linewidth, and other critical variables, providing a robust platform for evaluating system performance under realistic conditions.

Our paper is organized as follows: In Section 2, we discuss the CV-QKD protocol in general, followed by a secure key rate computation methodology for different categories. In Section 2.2, we discuss the Simulink architecture for Alice's and Bob's nodes. In Section 3, we present CV-QKD in action by show casing various modulation formats and their demodulation using coherent detection and a local oscillator. In Section 4, we discuss various results and explore future possibilities. A detailed description of each optical and electrical component comprising the CV-QKD module is provided in the Appendix.

2. Materials and methods

In this section, we describe the CV-QKD protocol and simulation framework.

2.1. CV-QKD protocol

This section begins by reviewing the coherent-state-based CV-QKD protocol, with a focus on different modulation schemes employed for secure key generation. We further review the secure key rate computation relevant to our case.

Quantum state preparation: In each round, the sender, Alice, randomly modulates the quadratures of coherent states (x_i, p_i) in the X polarization direction to generate the quantum signal. This modulation can be Gaussian-distributed or discrete modulation (QPSK, QAM, etc.). The starting 10 sample values of the in−phase components for different modulation formats are as follows: QPSK: {−1, 1, 1, −1, 1, −1, −1, 1, 1, −1}; QAM: {0.5, −1, 0.5, −1, 1, 0.5, −0.5, −0.5, −1, 1}; and Gaussian: {0.58, −1.25, 0.29, 1.58, −1.54, 1.01, 0.38, −0.65, 0.22, 0.78}. Similarly, she will have the corresponding random values for the quadrature component depending upon the modulation format as follows: QPSK: {1, −1, 1, 1, −1, 1, −1, −1, 1, 1}; QAM: {−0.5, 1, 0.5, 1, −1, −0.5, 0.5, −0.5, 1, −1}; and Gaussian: {1.16, 0.07, −0.69, 0.06, 0.26, −1.45, 1.24, 0.57, −0.13, −1.27}. She chooses Y polarization to send as the pilot tone in the single-sideband modulation with carrier suppression. For this, she applies $\cos \omega_p t$ and $\sin \omega_p t$ at the RF of the I and Q ports of the IQ modulator, respectively. Here, ω_p is the repetition rate of the pilot signal. She then sends the polarization-multiplexed prepared state to the receiver, Bob, after appropriately attenuating the quantum signal, as shown in **Figure 1**. Alice's raw keys, using the sample values of the in-phase and quadrature components for different modulation formats, are as follows: QPSK: {01, 11, 00, 01, 11, 01, 10, 11, 00, 01}; QAM: {1101, 0010, 1111, 0010, 1000, 1101, 0111, 0101, 0010, 1000}; and Gaussian: {0101, 1100, 0011, 0100, 1100, 0111, 0001, 1101, 0010, 0111}. These were obtained by dividing the Gaussian distribution into four bins of equal areas.

Quantum state measurement: After receiving the state, Bob demultiplexes the quantum signal and the pilot tone. He uses a local oscillator to perform coherent detection to obtain the measurement outcome. The pilot tones are used to determine the frequency and phase offset between Bob's measurement outcome and Alice's prepared state using digital signal processing (DSP) routines. The correlation between Alice's symbols and Bob's detected signal is approximately zero (0.89×10^{-6}) when there is frequency and phase offset. After the correction of the frequency and phase offset, Alice's and Bob's symbols have a correlation greater than 90% for a given channel length (40 km).

Public disclosure and parameter estimation: After completing a sufficient number of iterations of the aforementioned steps, Alice and Bob communicate via an authenticated public channel. Alice and Bob randomly select a subset of rounds for testing (say, 15%). For each round in this test subset, Bob discloses his measurement outcome, and using the disclosed information, Alice calculates the secret key rate based on the reverse reconcili-

ation protocol, utilizing the estimated values of transmittance, excess noise, and conditional variance. The protocol is terminated if the parameter estimation reveals that secret key generation is not feasible. Otherwise, the parties proceed with the remaining steps of the protocol.

Raw key generation: This involves the remaining undisclosed signals (85%) for the k^{th} round, used to obtain raw keys for Alice and Bob. Alice discretizes the corresponding prepared state (divides the Gaussian distribution into finite bins) by mapping it into a binary format. Then, the raw key contribution from the kth round is x_k. Alice obtains her string $X = (x_1, \ldots, x, \ldots, x_M)$ for the kth round, and Bob maps his measurement outcome to the corresponding expected symbol after performing offset correction through digital signal processing (DSP). He then obtains the string $Z = (z_1, \ldots, z_k, \ldots, z_M)$. Alice and Bob may further apply post-selection in the discrete modulation case (discarding the rounds that are Δ close to the origin).

Error correction and privacy amplification: Alice and Bob choose robust error correction codes (multidimensional LDPC, polar codes, etc.) and carry out privacy amplification (using Toeplitz matrices). In the end, they generate secret keys. After error correction and privacy amplification (say 50% compression), Alice's and Bob's keys are symmetric and secure. The final keys have no correlation with respect to the sent symbols due to privacy amplification. Generally, for the same value of excess noise and transmittance, a higher modulation format provides more keys. The final key strings for Alice and Bob for different modulation formats are as follows: QPSK: {11, 00, 01, 01, 10}; QAM: {1001, 0110, 0011, 1010, 1101}; and Gaussian: {1101, 1000, 0101, 1101, 0000}. The length difference between the raw key and the secure key is determined by the theoretical secure key rate calculation, as discussed next.

Secure key rate—Gaussian-modulated protocol: The asymptotic secret key rate per pulse, under the assumption of collective attacks and employing reverse reconciliation, is given by

$$R = (1 - FER)(1 - \nu)(\beta I_{AB} - S_{BE}). \quad (1)$$

In this case, *FER* denotes the frame error rate, ν represents the proportion of symbols revealed for parameter extraction, β signifies the efficiency of post-processing, and I_{AB} symbolizes the classical mutual information between Alice and Bob, which can be reliably calculated under ideal heterodyne detection conditions using the expression provided.

$$I_{AB} = \log_2 \frac{V_B + 1}{V_{B|A} + 1} = \log_2 \frac{T(V + \chi) + 1}{T(1 + \chi) + 1}. \quad (2)$$

Here, V represents the variance of the equivalent EPR state on Alice's side, while V_B denotes the variance of the state that Bob obtains. The conditional variance, indicated as $V_{B|A}$, accounts for Bob's measurement outcome. The total channel noise, quantified in shot noise units (SNU), is expressed as $\chi = 1/T - 1 + \epsilon$, which is derived from the channel's transmittance (T) and any excess noise ($\epsilon = \frac{\Delta Q^2_{obs}}{\Delta Q^2_{vac}}$-1). Next, we have to estimate the mutual information between Bob and Eve, S_{BE}. It is important to note that the maximum amount of information accessible to Eve is bounded by the Holevo quantity.

$$S_{BE} = \chi_{BE} = S(E) - S(E|m_B). \quad (3)$$

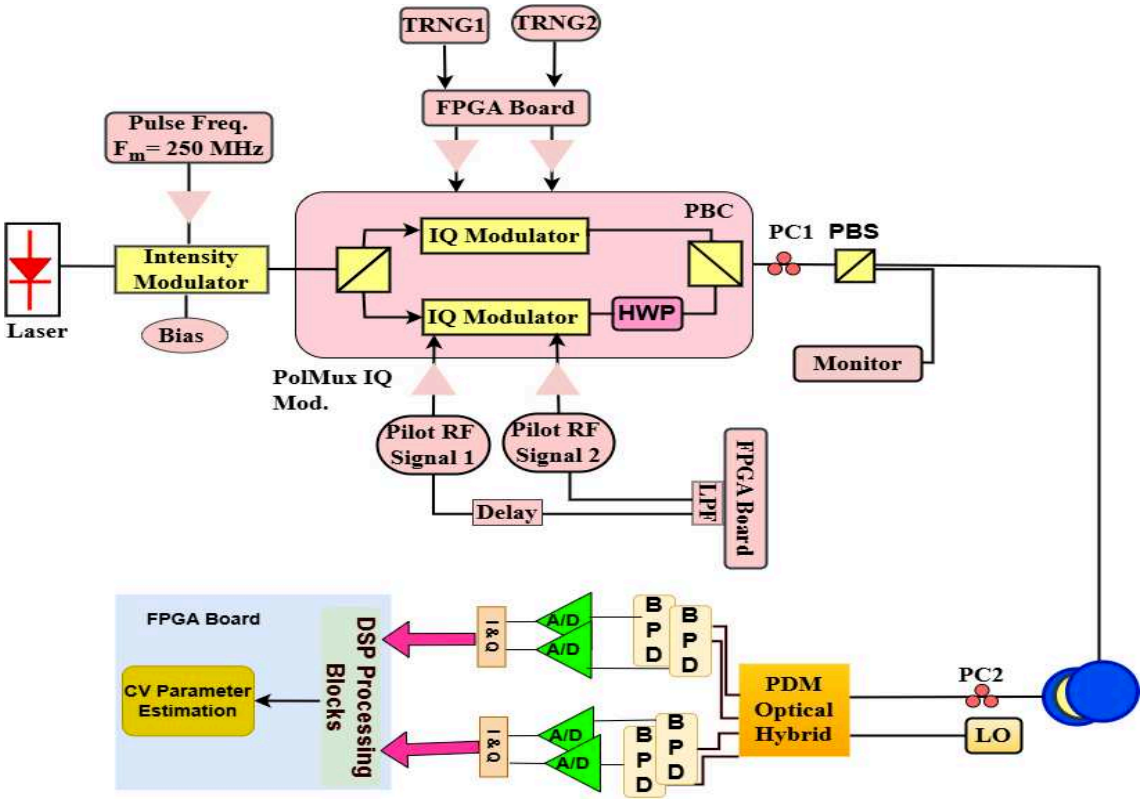


Figure 1 • Schematic diagram of the continuous-variable quantum key distribution. The setup comprises a laser source externally modulated at 250 MHz, feeding into a polarization-multiplexed IQ modulator (PolMux IQ Mod.) controlled by an FPGA board through TRNG1 and TRNG2. The polarization beam combiner (PBC) integrates both modulation paths, with half-wave plate (HWP) adjustment. The receiver architecture features an optical hybrid followed by balanced photodetectors (BPDs) and analog-to-digital converters (A/D), enabling real-time CV parameter estimation through DSP processing. TRNG: true random number generator; PC1(2): Polarization Controller 1 (2); LO: local oscillator.

Here, $S(E)$ denotes the von Neumann entropy of the eavesdropper's state ρ_E, while $S(E|m_B)$ represents the von Neumann entropy conditioned on Bob's measurement outcome. Assuming that Eve holds the purification of the bipartite quantum state ρ_{AB} and invoking the Gaussian extremality theorem to establish an upper bound under the Gaussian assumption [42], the evaluation of the von Neumann entropy is simplified by computing the symplectic eigenvalues of the covariance matrix and the corresponding conditional covariance matrix. The Holevo bound, using the above approach for heterodyne detection, is,

$$\chi_{BE} = G\left(\sqrt{\tfrac{1}{2}\left[\delta + \sqrt{\delta^2 - 4D^2}\right]}\right) + G\left(\sqrt{\tfrac{1}{2}\left[\delta - \sqrt{\delta^2 - 4D^2}\right]}\right) - G\left(\tfrac{T(V\chi+1)+1}{T(V+\chi)+1}\right). \tag{4}$$

Here, δ and D are functions of the transmittance (T), excess noise (ϵ), and variance (V) and are obtained from the covariance matrix. Here, $G(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$.

Secure key rate—discrete-modulated protocol: The secure key rate, **Formula (1)**, in the discrete modulation case contains a p_{pass} term due to post-selection. The estimation of the Holevo bound is usually carried out numerically by using the photon number cut-off assumption [43–47]. The conditional entropy term in the Holevo bound is reformulated in terms of the quantum relative entropy [48, 49]. The idea is to solve the following convex optimization problem, where the constraints depend on the discrete modulation format (QPSK here).

$$\begin{aligned} \min_{\rho_{AB}} \quad & D(G_y(\rho_{AB})||Z[G_y(\rho_{AB})]) \\ \text{subject to} \quad & \mathrm{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{q}] = p_X\langle\hat{q}\rangle_x, \\ & \mathrm{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{p}] = p_X\langle\hat{p}\rangle_x, \\ & \mathrm{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{n}] = p_X\langle\hat{n}\rangle_x, \\ & \mathrm{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{d}] = p_X\langle\hat{d}\rangle_x, \\ & \mathrm{Tr}[\rho_{AB}] = 1, \\ & \rho_{AB} \geq 0. \end{aligned} \tag{5}$$

This minimization problem can be addressed using various methods. We use a linearization approach, as described by Liu et al. [44]. In essence, the numerical method comprises two stages. Initially, we approximate the optimal value of the minimization problem **(5)** within a maximum of $N_i = 100$ iterations. Subsequently, we consider the dual problem of the minimization issue to ensure that the outcome is no greater than the optimal value. Using this approach, we computed the secret key rate versus transmission distance for a QPSK-based CV-QKD system at three different modulation frequencies (10 MHz, 100 MHz, and 250 MHz), as shown in **Figure 2**. Key rates exhibit characteristic exponential decay with distance, showing modulation rate-dependent performance variations. Higher frequencies (250 MHz) demonstrate superior key rates at short distances but experience steeper declines, while lower frequencies (10 MHz) maintain more stable performance over longer distances. The plot quantifies the critical trade-off between bandwidth and maximum achievable range in discrete modulation CV-QKD implementations.

2.2. CV-QKD Simulink blocks

This section presents the modeling framework employed for each module, mirroring the functionality of its corresponding physical device within the system. To emulate the behavior of a practical system, the overall architecture is systematically divided into three primary subsystems: Alice, the quantum channel, and Bob, as shown in **Figure 3**. We first discuss the modeling of Alice's node and then move on to Bob's node.

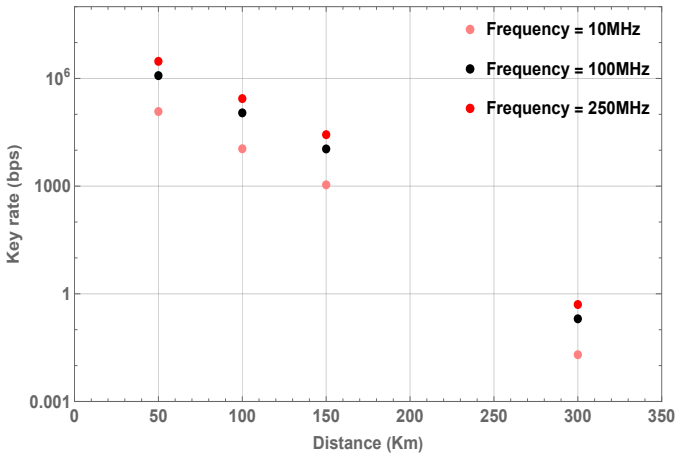


Figure 2 • Secret key rate as a function of transmission distance for different modulation frequencies (10 MHz, 100 MHz, and 250 MHz) in the QPSK-based quantum key distribution system. The key rate demonstrates the expected exponential decay with distance, with higher modulation frequencies achieving superior performance.

2.2.1. Alice's node

Alice's node comprises a laser source and quantum and pilot state preparation components (polarization-multiplexed IQ modulator) in CV-QKD. In practice, the laser module produces two signals, denoted as E_x and E_y, that symbolize the electric field in two orthogonal polarization directions. The intensity of these signals is externally modulated using a pulse carver to ensure a higher extinction ratio. The X-polarization is used to prepare the quantum signal, and the Y-polarization is used to generate the pilot tone. **Figure 4** shows the block diagram for the simulation model. Depending on the modulation format, the signals for the RF and DC of the IQ modulator are selected. We performed Gaussian and discrete modulation of the quantum signal and single-sideband modulation with carrier suppression for the pilot tone. The constellation diagram of various modulation formats is shown in **Figure 5**. When a cosine waveform is modulated onto an optical carrier, it generates two sidebands symmetrically spaced around the carrier frequency, each separated by the modulation frequency. In homodyne or intradyne detection scenarios, these sidebands overlap at nearly the same intermediate frequency, leading to self-interference and signal degradation. To mitigate this, one sideband can be suppressed using appropriate phase control in a Mach–Zehnder IQ modulator, as both sidebands carry redundant information. Additionally, suppressing the optical carrier along with implementing single-sideband (SSB) modulation eliminates low-frequency beat notes, which could otherwise interfere with the quantum signal in the detection process. The purpose of the pilot tone is to determine the phase and frequency offset between Alice's laser and Bob's local oscillator.

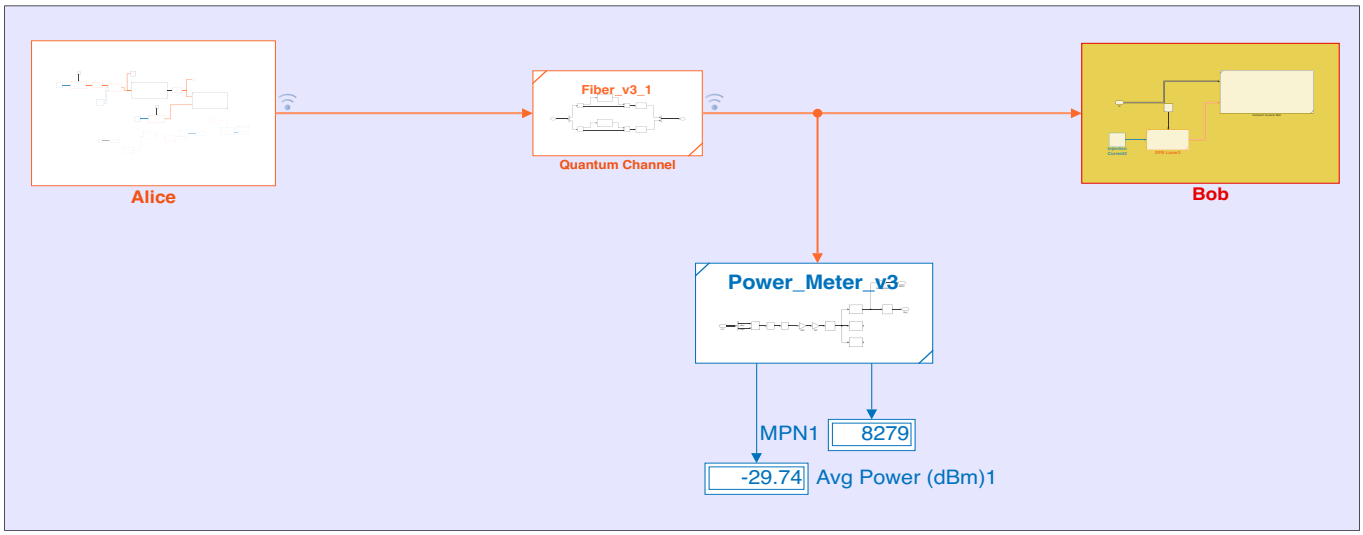


Figure 3 • Complete architecture of the CV-QKD system, showing Alice's node, the quantum channel, and Bob's node. The setup employs a DFB laser with controlled injection current, transmitting through a fiber-based quantum channel. The coherent receiver at Bob's end measures the quantum states, with an integrated power meter to monitor the power at various levels.

This offset is due to the different laser sources and channel action connecting the two nodes. The detailed component-level architecture is provided in Appendix Section. To maintain protocol security, the quantum signal must be kept weak, typically between 0.1 and 10 photons per symbol, depending on channel length and noise conditions. In contrast, the pilot tone needs high optical power to ensure precise phase measurements. To balance these requirements, we applied polarization-selective attenuation, lowering the quantum signal's power by −23 dB relative to the pilot. This adjustment maintained optical phase coherence while enabling independent power control. Using a fiber-based polarization controller (PC) and a polarizing beam splitter (PBS), we selectively attenuated the polarization components. By adjusting the PC, the pilot signal was minimized in the PBS monitoring port, maximizing its strength in the output. Due to the PBS's finite extinction ratio (23 dB), a small portion of the quantum signal leaked through to the output alongside the dominant pilot, resulting in an effective quantum signal strength of approximately 1–10 photons per symbol.

2.2.2. Bob's node

For coherent detection, Bob uses an independent local oscillator with a 20 kHz linewidth and 12 dBm output power. Coherent detection of both the quantum signal and pilot tone was carried out using a polarization-diversity 90° optical hybrid. This hybrid combined the quantum signal and pilot with a shared local oscillator and directed the resulting interference signals to dedicated balanced photodetectors (see **Figure 6**). Two distinct pairs of balanced receivers were employed, one for each quadrature of the quantum signal and pilot. Each receiver pair was optimized based on the characteristics of its corresponding signal path. For quantum data, low-noise photodetectors were used to preserve signal integrity, while the pilot tones were handled by high-bandwidth receivers designed to tolerate higher optical input levels without saturation.

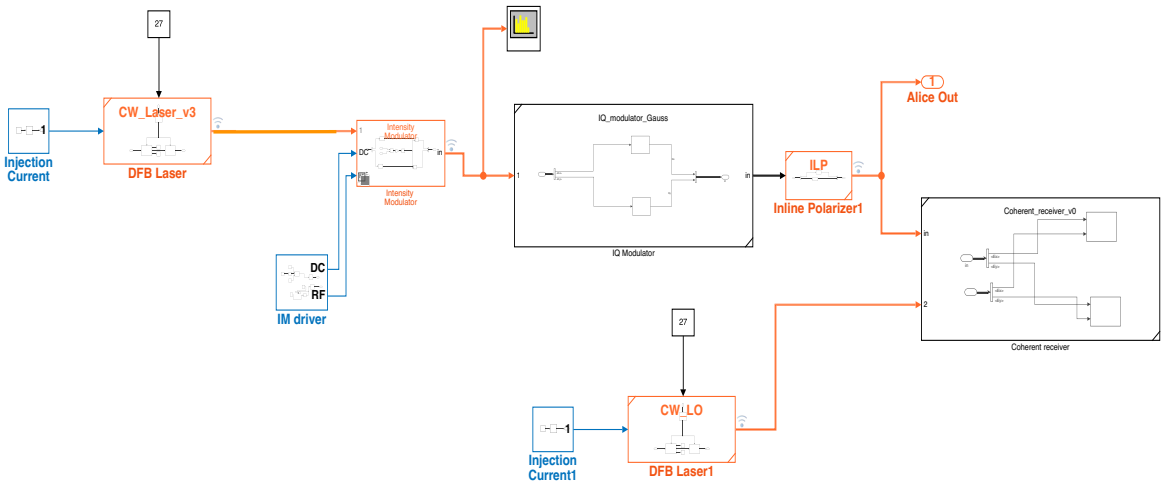


Figure 4 • Detailed layout of Alice's node featuring a DFB laser source feeding into cascaded intensity and IQ modulators. The system includes an intensity modulator for pulse carving, with dedicated injection current controls and RF/DC inputs for precise state preparation. A local oscillator (LO) laser and coherent receiver are integrated for system characterization and calibration and are not part of the experimental implementation.

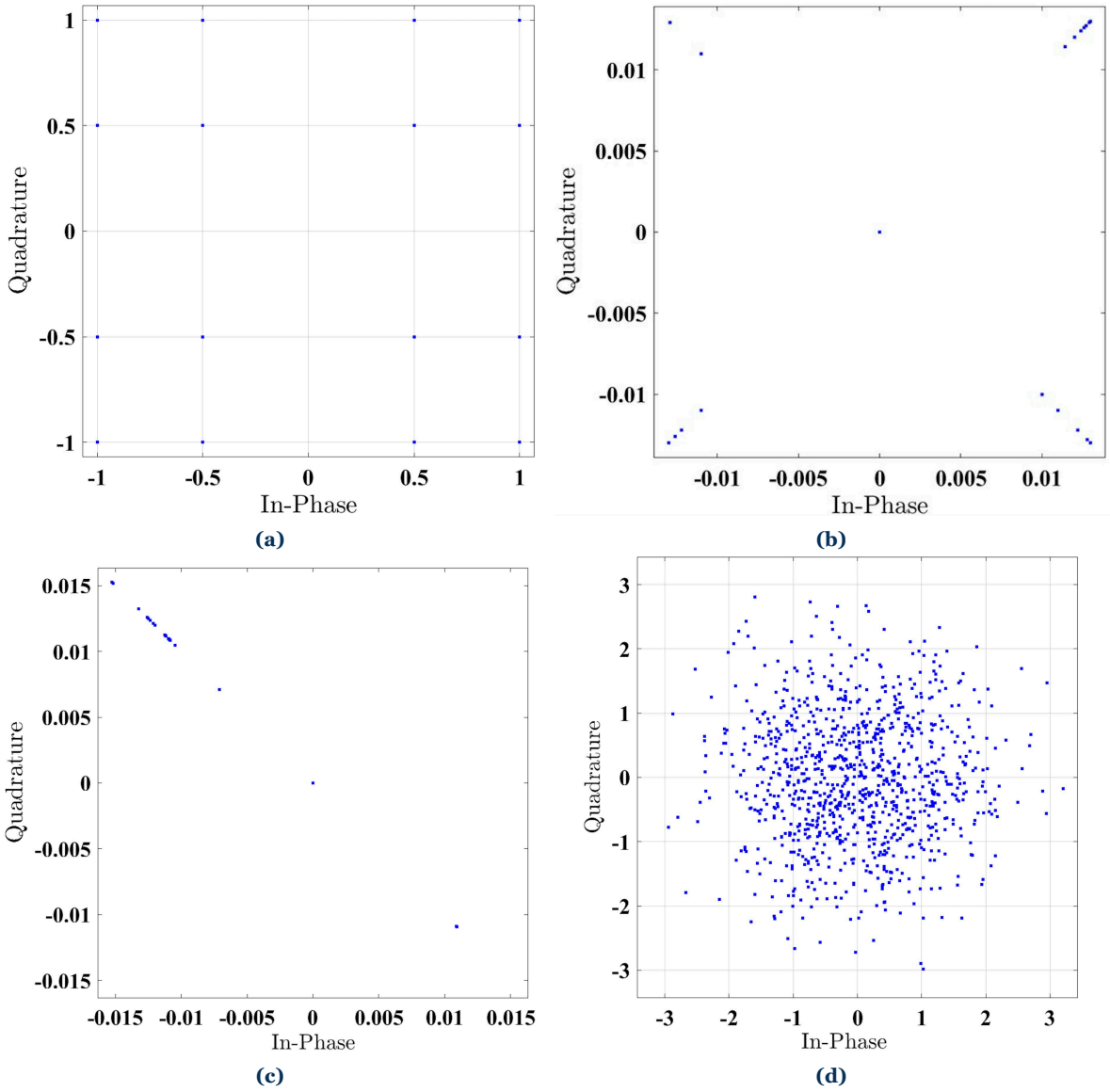


Figure 5 • Constellation diagram of the modulation and demodulation signals at Alice's node. (**a**) Scatter plot of the QAM modulation signal. (**b**) Scatter plot of the QPSK demodulation signal. (**c**) Scatter plot of the demodulated pilot tone signal. (**d**) Scatter plot of the Gaussian-modulated signal.

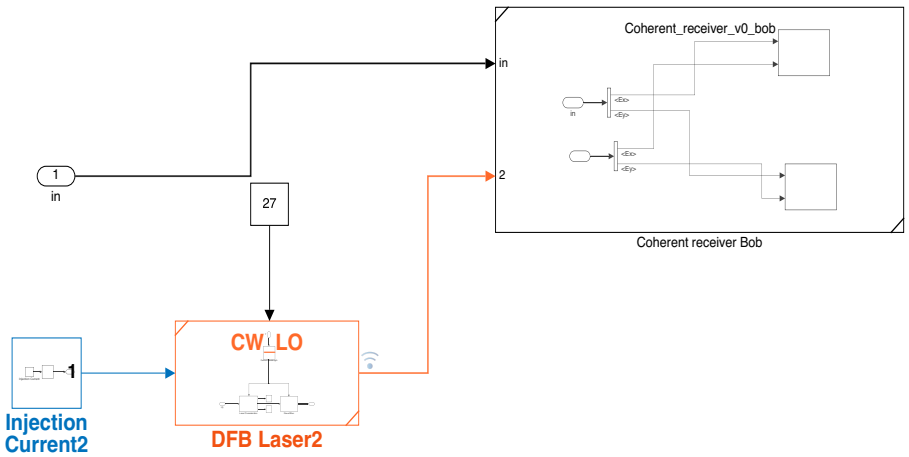


Figure 6 • Bob's node configuration, incorporating a DFB laser serving as a local oscillator with precision current control. The setup includes a coherent receiver for quadrature measurements, with integrated optical-to-electrical conversion for signal processing. The system monitors laser characteristics, including central wavelength stability, to maintain detection fidelity.

3. Results and discussion

In this section, we first demonstrate the performance of our CVQKD experimental simulator and later on compare the discrete modulation with the Gaussian modulation technique.

3.1. CV-QKD in action

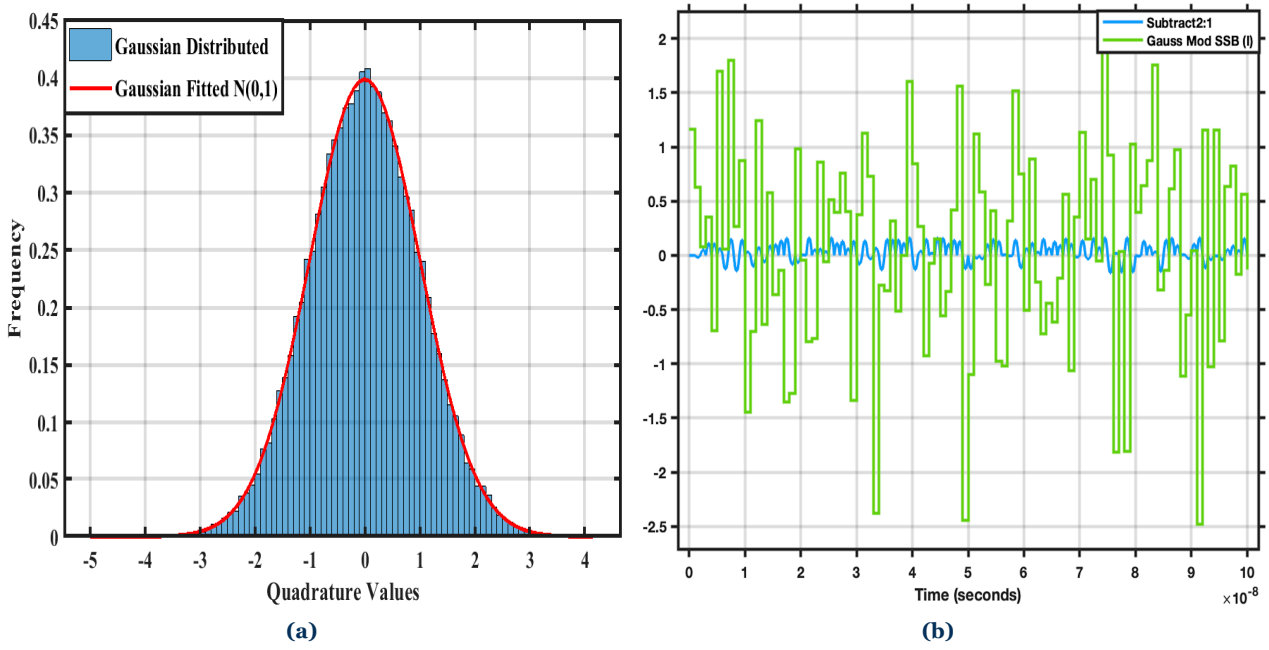
In this section, we demonstrate the efficacy of our experimental simulator in simulating the GG02 CV-QKD protocol. We discuss all the stages of the protocol again and the performance of the simulator in analyzing the signal at each stage. The stages of the GG02 protocol are as follows:

Quantum state preparation: The light generated by the laser source is modeled by two signals that symbolize the electric field in two orthogonal polarization directions. The intensity of these signals is externally modulated using an intensity modulator at 250 MHz to create optical pulses. These optical pulses are further separated into X and Y polarization, where X-polarized optical pulses are modulated (QPSK, QAM, or Gaussian) at a 250 MBaud rate and attenuated to the quantum level, while the Y-polarized optical pulses are modulated in the single-sideband modulation with carrier suppression (SSB-oCS) format at 1 GHz and act as a pilot tone for frequency and phase offset matching with the local oscillator kept at the receiver node. The constellation diagram of various modulation formats is recovered at Alice's node through auxiliary coherent detection, and it is shown in **Figure 5**. Phase and frequency offsets and imperfect DSP are clearly visible in the demodulated signal constellation diagrams. The proof of the security of the Gaussian-modulated CV-QKD is well established. Such modulation is achieved by using the Gaussian-distributed random signal at the RF ports of the IQ modulator. The distribution plot and its demodulation signal are shown in **Figure 7**. For the proper demodulation of the Gaussian signal, the distribution curve is divided into a discrete number of bins, where each bin represents one symbol.

To maintain the protocol's security, the quantum signal must remain sufficiently weak, typically within the range of 0.1 to 10 photons per symbol. In contrast, the pilot tone requires high optical power to enable precise phase and frequency estimation. To obtain these conditions, we applied polarization-dependent attenuation, reducing the quantum signal's power by approximately (23 dB) relative to the pilot tone. This was implemented using an inline polarizer to selectively attenuate specific polarization components, ensuring that the optical phase lock remained intact throughout the process. The output port delivers the 1 GHz pilot tone at peak power, while the finite extinction ratio (23 dB) of the inline polarizer allows a small residual quantum signal to pass. A PBS can produce similar attenuation

Quantum state transmission: The quantum signal and the pilot tones at the output port of the inline polarizer/PBS are then transmitted together via a quantum channel (single-mode optical fiber with no active elements) to the receiver node for coherent detection. The signals undergo chromatic and polarization mode dispersion. Nonlinear effects like the Kerr effect become prominent at longer distances. For further details, see Appendix B. These effects give rise to an imperfect constellation diagram at Bob's node (see **Figure 5**).

Quantum state measurement: Detection at the receiver node was performed coherently using a 12 dBm local oscillator operating with a narrow linewidth in free-running mode. For the simulation, we used the same DFB laser module as in the transmitter node and slightly changed the temperature or central wavelength to make it a local oscillator. The effect of temperature and frequency offset is clearly visible in the plots of the balanced detector signal (see **Figure 8c,d**).



(a) **(b)**

Figure 7 • Gaussian-distributed random modulation signal and its demodulation using coherent detection. (**a**) Gaussian distribution of the random samples for the in-phase component modulation of the quantum signal. (**b**) The Gaussian-modulated RF signal is shown in green and the balanced detector outcome is shown in blue. The two signals show high correlation.

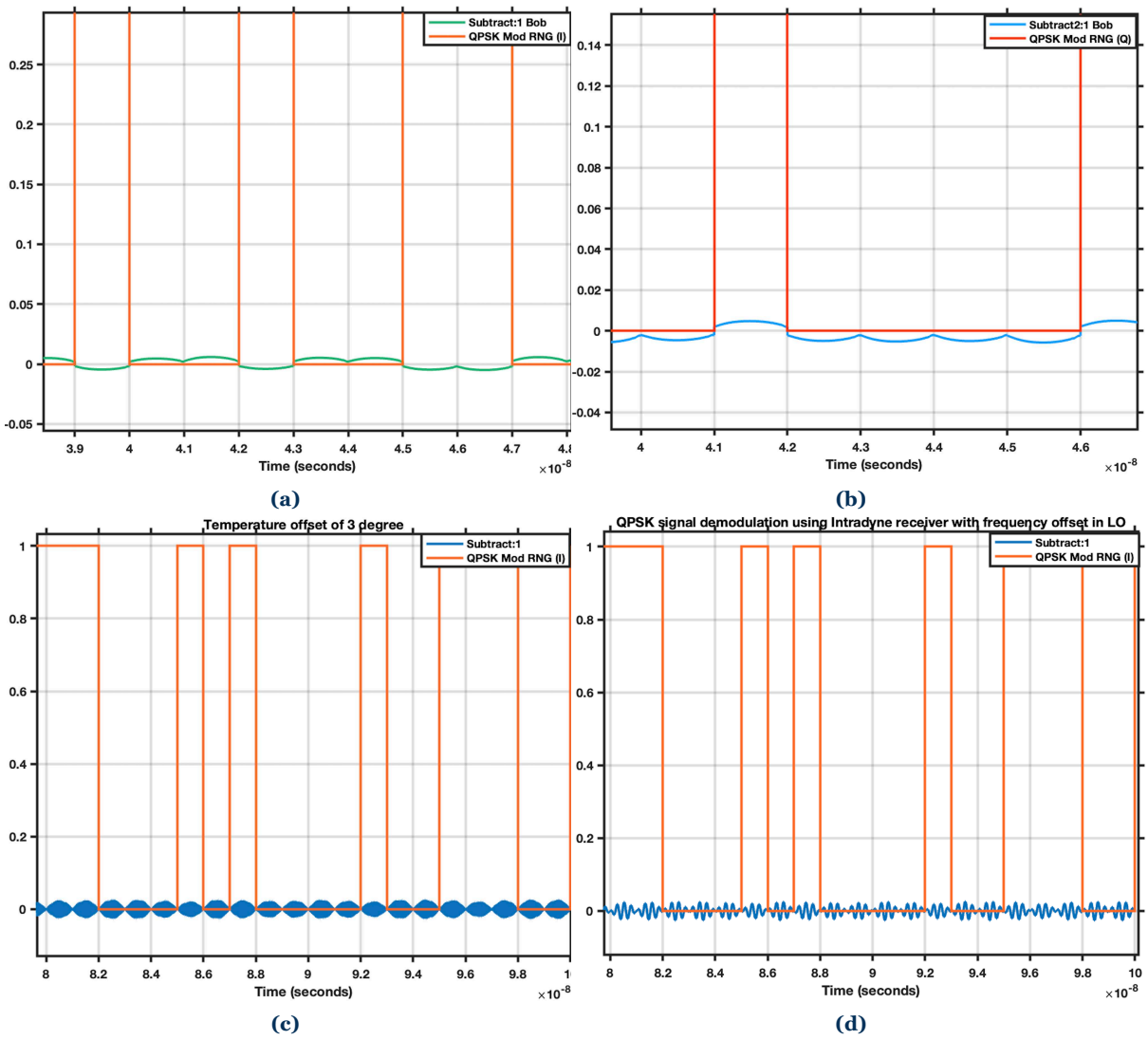


Figure 8 • QPSK demodulation with and without temperature and frequency offset. The temperature offset and frequency offset between Alice's laser source and Bob's local oscillator are 3 degrees and 10 MHz, respectively. (**a**) Decoding in-phase component at Bob's node. (**b**) Decoding quadrature component at Bob's node. (**c**) Balanced detector output with temperature difference between the laser sources. (**d**) Balanced detector output with frequency offset between the two lasers.

The local oscillator is mixed with both the pilot tone and quantum signal using a polarization-diverse 90^o optical hybrid, subsequently sending each component to its assigned balanced detector for coherent measurement. We match the diffential signal of the detectors with Alice's modulated signal. There is a perfect correlation between the modulated and demodulated QPSK signals (see **Figure 8**) after frequency and phase offset correction. The cross-correlation percentage between Alice's and Bob's symbols is more than 90% at a channel length of 40 km. The cross-correlation between Alice's and Bob's symbols is close to zero (0.89×10^{-6}) without frequency and phase offset compensation. The demodulated decision symbols at the receiver node form the raw keys, whereas the modulated symbols at the transmitter form the raw keys. After reverse reconciliation, Alice maps her symbols with respect to Bob's demodulated decision symbols. Alice never discloses her symbol information through the public channel in this mechanism.

Further, using the secure key rate calculations, one can convert the raw keys to secure keys by applying privacy amplification.

4. Conclusions

We have developed a comprehensive Matlab and Simulink-based experimental simulator for continuous-variable quantum key distribution that accurately models the quantum and classical characteristics of optical components. Our simulator demonstrates that polarization-multiplexed quantum signals with discrete modulation and pilot tones exhibit enhanced resilience to experimental imperfections, with further robustness achieved through post-selection. We also modeled and analyzed the effect of temperature and frequency offsets between two laser diodes for coherent detection. The results validate that intradyne detection more effectively mitigates various offsets between nodes, yielding higher key rates under trusted detector noise scenarios.

The simulator's ability to analyze different modulation formats and detection techniques while incorporating realistic imperfections makes it a valuable tool for optimizing CV-QKD implementation. Our findings indicate that current protocols can facilitate key distribution over intercity distances, supporting the development

of cost-effective quantum secure communication networks. The simulation framework provides a foundation for future exploration of quantum communication protocols and security analysis under various experimental conditions. Looking ahead, we envision expanding our simulator to incorporate point-to-multipoint CV-QKD, with the objective of creating an intercity network. Future developments will also focus on a hybrid DV and CV-QKD protocol and modeling additional security threats like side-channel attacks. The simulator's modular architecture allows for the seamless integration of new components and protocols, positioning it as an evolving platform for quantum communication research and development.

Acknowledgments

Appreciation is also extended to Anuj Setia for his contributions to the development of submodules within the DPS-QKD simulation framework. A.R. acknowledges QuNu Labs' SparQ summer internship.

Funding

This research was funded by QuNu Labs Pvt. Ltd. (Bengaluru, India) through a consultancy fee provided to the corresponding author's postdoctoral appointment, which supported the research and simulations.

Author contributions

Conceptualization, S.G., A.M.S. and A.R.; methodology, S.G.; software, S.G.; validation, S.G., A.R. and A.M.S.; formal analysis, S.G.; investigation, S.G. and A.M.S.; resources, S.C.; data curation, S.G.; writing—oiginal draft preparation, S.G. and A.M.S.; writing—review and editing, A.M.S.; visualization, S.G. and V.M.; supervision, R.K.K. and D.S.; project administration, R.K.K.; funding acquisition, D.S. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

QuNu Labs Pvt. Ltd. (Bengaluru, India) provided financial support during the corresponding author's postdoctoral appointment, which influenced the design of the study, as well as the collection, analysis, and interpretation of data. The author is currently employed by QuNu Labs Pvt. Ltd. as Research Lead. The writing of the manuscript and the decision to publish the results were made after rejoining the company with the agreement of all listed authors.

Data availability statement

The data supporting the findings of this publication can be made available upon request.

Additional information

Received: 2025-04-11

Accepted: 2025-07-29

Published: 2025-08-14

Academia Quantum papers should be cited as *Academia Quantum 2025*, ISSN 3064-979X, https://doi.org/10.20935/AcadQuant7844. The journal's official abbreviation is *Acad. Quant.*

Publisher's note

Copyright

Appendix A. Alice's optical component simulation

Appendix A.1. Laser

We present a comprehensive model of a distributed feedback (DFB) semiconductor laser for continuous-variable quantum key distribution, incorporating both quantum and classical noise characteristics. The laser dynamics are governed by coupled rate equations describing photon–carrier interactions in the active cavity:

$$\begin{aligned} \frac{dN(t)}{dt} &= \frac{I(t)}{eV_a} - \frac{N(t)}{\tau_n} - g_0 \frac{N(t)-N_0}{1+\epsilon_c S(t)} S(t) \\ \frac{dS(t)}{dt} &= \left(\Gamma g_0 \frac{N(t)-N_0}{1+\epsilon_c S(t)} - \frac{1}{\tau_p}\right) S(t) + \frac{\beta \Gamma N(t)}{\tau_n} \\ P(t) &= \frac{S(t) V_a \eta_0 h\nu}{2\Gamma \tau_p} \end{aligned} \tag{A1}$$

where $N(t)$ and $S(t)$ represent the carrier and photon densities, respectively, interacting through stimulated and spontaneous emission processes. The output electric field is characterized by

$$E(t) = \sqrt{P(t)} e^{i(\omega_c t + \phi(t))} \tag{A2}$$

Our implementation incorporates two critical noise sources: (1) relative intensity noise (RIN), modeled as white Gaussian noise with a standard deviation of $\sigma_P = \sqrt{10^{RIN/10} \Delta f P_{av}}$, and (2) phase noise, with $\sigma_\phi = 2\pi \Delta\omega \tau$, derived from the spectral linewidth. Temperature-dependent wavelength shifts follow $\Delta\lambda = \lambda_0 + \delta\lambda \Delta T$, where $\delta\lambda$ represents the thermal coefficient.

We demonstrate that this model accurately reproduces both the quantum and classical characteristics essential for CV-QKD applications, including shot-noise-limited intensity fluctuations and

phase coherence properties. The simulation results show excellent agreement with experimental observations of commercial DFB lasers, particularly in the critical parameters of spectral purity and noise characteristics.

This high-fidelity model enables precise prediction of quantum state preparation fidelity in CV-QKD systems, accounting for both fundamental quantum limits and technical noise sources. The framework provides a valuable tool for optimizing quantum communication protocols and evaluating security parameters in practical implementations.

The rate equation model, along with emulation of laser noise and temperature dependence, demonstrates the response of a monochromatic laser with reasonable fidelity. The laser submodule outputs a bus signal with $Ex(t)$ and $Ey(t)$ as its two components. A detailed list of the laser parameters is given in **Table A1**.

Appendix A.2. Intensity modulator

The intensity modulator used is a Mach–Zehnder interferometric modulator (MZIM) for quantum state preparation, focusing on achieving precise amplitude control with high extinction ratios. The modulator architecture employs a dual-electrode configuration with balanced phase control in each arm.

For an input optical field Ei, the output field evolution follows

$$E_o(t) = \frac{1}{2}E_i\left(e^{i\phi_1(t)} + e^{i\phi_2(t)}\right) \tag{A3}$$

Under balanced differential drive conditions, where the electrodes are biased with equal and opposite voltages, the transfer function simplifies to

$$E_o(t) = E_i \cos\left(\frac{\pi V(t)}{V_\pi}\right) \tag{A4}$$

where V_π represents the voltage required for a π phase shift. The extinction ratio, critical for quantum state preparation, is given by

$$ER = \frac{\cos^2\left(\frac{\pi V_1}{V_\pi}\right)}{\cos^2\left(\frac{\pi V_0}{V_\pi}\right)} \tag{A5}$$

Our implementation achieves extinction ratios exceeding 30 dB through precise voltage control (V_1, V_0), enabling high-fidelity quantum state preparation. The modulator's response remains linear within the quantum signal bandwidth, maintaining phase coherence, which is essential for CV-QKD protocols.

Table A1 • List of parameters for DFB laser submodule.

Symbol	Parameter	Value
Γ	Optical confinement factor	0.44
g_0	Gain coefficient	3×10^{-6} cm^3/s
N_0	Initial carrier density	1.2×10^{8} cm^{-3}
ϵ_c	Gain compression factor	3.4×10^{-17} cm^3
τ_p	Photon lifetime	10^{-12} s
β	Spontaneous emission coupling factor	4×10^{-4}
τ_n	Electronic carrier lifetime	3×10^{-9} s
e	Electronic charge	1.602×10^{-19} C
V_a	Active region volume	9×10^{-11} cm^3
η_{DFB}	Differential quantum efficiency	0.1
$N(t)$	Equilibrium carrier density	5.41×10^{10} cm^{-3}
h	Planck's constant	6.626×10^{-34} Js
c	Speed of light	2.99×10^{8} cm^{-3}
λ_0	Central wavelength	1547.72×10^{-9} m
$I(t)$	Injection current	0.012 A
σ_I	Injection current standard deviation	10^{-3} A
$\Delta\omega$	Spectral linewidth	10^4 Hz
RIN	Relative intensity noise	−160 dBm
δ_λ	Temperature variation	0.09×10^{-9} m/K
Δf	System bandwidth	250×10^6
T_L	Laser set temperature	27 °C
ϕ_0	Initial absolute phase	0

This architecture provides a robust platform for generating amplitude-controlled quantum states with minimal phase distortion, which is crucial for maintaining security in quantum key distribution systems. The analytical framework presented enables optimization of driving conditions for arbitrary waveform generation while maintaining quantum state fidelity. A list of parameters is given in the **Table A2**.

Table A2 • List of parameters for laser module.

Symbol	Parameter	Value
IM_{loss}	Insertion loss	-3 dBm
IM_{ER}	Desired extinction ratio	30 dBm
FWHM	Full width half maximum	300×10^{-12} s
V_{DC}	DC bias input to IM	variable
$V_{\text{RF}}(t)$	RF input to IM	variable

Appendix A.3. IQ modulator

IQ modulators are used to externally modulate both the inline and quadrature components of the input electromagnetic field. They consist of two identical parallel interferometers MZI_1 and MZI_2 nested in a third. Both MZI_1 and MZI_2 are driven by the same electrical modulation signal (the same frequency and the same amplitude) with a phase delay, ϕ_e, between them. MZI_1 and MZI_2 are biased using DC voltages, which induce $\pm\Delta\phi_{1/2}$ in each arm of the MZIs. In the same way, MZI_3 is biased with a DC voltage that introduces an optical delay, $\Delta\phi_3$, between the output fields of MZI_1 and MZI_2 (E1 and E2).

$$E_o^{X/Y}(t) = E_1(t) + E_2(t)e^{i\Delta\phi_3} \tag{A6}$$

A dual-polarized IQ modulator is constructed to independently modulate the quantum signal, which is X-polarized, and the pilot tone, which is Y-polarized. The configuration of the RF signal, whether it adopts NRZ, complex exponential, or Gaussian modulation, and the DC signal ($\Delta\phi_{1/2} = 0$) for MZI_1 and MZI_2 is contingent on the modulation format of the quantum signal, which may be QPSK, QAM, or Gaussian.

The pilot tone undergoes single-sideband (SSB) modulation with carrier suppression. This is achieved when the RF signal of MZI_1 is $V_0 \sin(\Omega t)$ and that of MZI_2 is the same but $\pi/2$ phase-delayed. SSB modulation is achieved when we further set $\Delta\phi_{1/2} = \phi_0$ and $\Delta\phi_3 = \pi/2$.

$$\begin{aligned} E_o^Y = E_{in} \Big\{ & J_0(\beta) \cos\left(\tfrac{\Delta\phi_0}{2}\right) e^{i\frac{\pi}{4}} e^{i\omega_0 t} \\ & + 2J_1(\beta) \sin\left(\tfrac{\Delta\phi_0}{2}\right) e^{i\frac{\pi}{2}} e^{i(\omega_0+\Omega)t} \Big\}. \end{aligned} \tag{A7}$$

Here, β is the total phase modulation in each arm for a voltage of V_0. J_i is the i^{th}-order Bessel function. When both modulators MZI_1 and MZI_2 are biased at their minimum transmission, i.e., $\Delta\phi_{1/2} = \Delta\phi_0 = \pi$, there is no longer an optical carrier at ω_0 in the E-field spectrum but only sidebands. Such modulation is called single-sideband modulation with carrier suppression (SSB-CS). This is useful for safeguarding the quantum signal.

$$E_o^Y(t) = E_{in} \left\{ 2J_1(\beta) e^{i\frac{\pi}{2}} e^{i(\omega_0+\Omega)t} \right\}. \tag{A8}$$

If we want to keep the lower sideband instead of the upper sideband, we have to use $\Delta\phi_{1/2} = \Delta\phi_0 = \pi$ and $\Delta\phi_3 = -\pi/2$

$$E_o^Y(t) = E_{in} \left\{ -2J_1(\beta) e^{-i\frac{\pi}{2}} e^{i(\omega_0-\Omega)t} \right\}. \tag{A9}$$

We have considered only first harmonics for simplicity but the spectra of the modulated optical signals would include sets of other symmetric sidebands arranged around the laser carrier peak at frequency f_o, corresponding to higher-order harmonics. The sidebands are displaced from the laser carrier peak frequency at integer multiples of the modulation frequency, $f_s = (f_o \pm nf_m$ with $n = 1, 2, \cdots)$. The relative heights of the sidebands are a function of the modulation depth, which is in turn a function of the peak-to-peak value of the RF driving voltage and the n^{th}-order Bessel function. Specific higher-order sidebands can be suppressed using a combination of the phase delays. A list of parameters is given in **Table A3.**

Table A3 • List of parameters for IQ modulator module.

λ	Operating wavelength	1550 nm
Symbol	Parameter	Value
IQ_{loss}	Insertion loss	-13 dBm
IQ_{PCT}	Polarization cross-talk	18 dBm
IQ_{RL}	Optical return loss	30 dB
V_{DC}	DC bias input to IQ	variable
$V_{\text{RF}}(t)$	RF input to IQ	variable

Appendix A.4. Variable Optical Attenuator (VOA)

The VOA is another crucial device for CVQKD. The primary function of the VOA is to attenuate the signal to the quantum level, reducing the mean photon number per pulse to between 1 and 10. This is also used to ensure that the optical hybrid at Bob's node has a balanced response. The extent of attenuation is dependent on the length of the transmission line, considering that the attenuation level of the VOA can be set to any magnitude. A list of parameters is given in **Table A4**.

Table A4 • List of parameters for variable optical attenuator submodule.

Symbol	Parameter	Value
VOA_{att}	Desired attenuation	variable

Appendix B. Optical fiber

Here, we carry out an analysis of quantum state evolution in optical fibers for continuous-variable quantum key distribution (CV-QKD), incorporating both linear and nonlinear effects through the nonlinear Schrödinger equation (NLSE). The propagation dynamics are solved using the split-step Fourier method (SSFM), yielding

$$\frac{dA}{dz} = A(\hat{D} + \hat{N}) \tag{A10}$$

where the differential operators are

$$\begin{aligned} \hat{D} &= -\frac{\alpha}{2} + \frac{\iota}{2}\beta_2\frac{\delta^2}{\delta t^2} + \frac{1}{6}\beta_3\frac{\delta^3}{\delta t^3} \pm \frac{\iota\Delta\tau}{2}\frac{\delta}{\delta t} \\ \hat{N} &= \iota|A\sqrt{\gamma}|^2 \end{aligned} \tag{A11}$$

The linear operator $\hat{D}$ encompasses attenuation (α), chromatic dispersion (β_2), third-order dispersion (β_3), and polarization

mode dispersion ($\Delta\tau$). The nonlinear operator $\hat{N}$ captures Kerr effects through the nonlinearity coefficient γ.

In the quantum regime, three critical phenomena emerge: 1. group velocity dispersion (GVD), causing temporal broadening; 2. self-phase modulation (SPM), inducing intensity-dependent phase shifts; and 3. polarization mode dispersion (PMD) from fiber birefringence.

At typical CV-QKD power levels (<-10 dBm), we demonstrate that scattering nonlinearities (SBS, SRS) become negligible, while four-wave mixing (FWM) and cross-phase modulation (XPM) require consideration only in wavelength-multiplexed implementations.

This formalism enables precise prediction of quantum state evolution, which is crucial for optimizing CV-QKD protocols for deployed fiber networks. In theory, the nonlinear effects and dispersion work in conjunction with the transmission fiber. As the SSFM is only an approximation method, these two factors are broken up and solved individually. The fiber transmission distance is partitioned into a large number of segments of width h. Within a segment, the effect of nonlinearity is included at the mid-plane with linear dispersion effects at both ends. Both dispersion and nonlinearity can be solved through an analytical approach, which involves (i) converting from the time domain to the Fourier domain, (ii) adding a phase shift for the linear effect, (iii) taking an inverse Fourier transform and converting it back into time domain, and (iv) adding a phase shift for the nonlinear shift. The following effects are included in the model: loss, group velocity dispersion (GVD), third-order dispersion, polarization mode dispersion (PMD), and self-phase modulation (SPM). A list of relevant parameters is given in **Table A5**.

Table A5 • List of parameters for optical fiber module.

Symbol	Parameter	Value
L	Fiber length	40 Km
α	Attenuation per Km	0.2 dB/Km
β_2	2nd-order CD factor	25×10^{-24} s^2/Km
β_3	3rd-order CD factor	-0.3×10^{-36} s^3/Km
$\Delta\tau$	Differential group delay	0.2×10^{-12} s/Km
γ	Nonlinear coefficient	0.78 W^{-1} Km^{-1}
NFFT	Number of samples for FFT	200
dz	Step size for SSFM	0.1 Km

Appendix C. Bob's optical component simulation

Bob's node contains a DFB laser module, as describe under Alice's node's optical components, and an optical hybrid integrated with photodetectors. The DFB laser module serves as a local oscillator. The frequency and phase offsets between the two lasers are computed using the pilot tone and rigorous DSP iterations. We have already discussed the mathematical architecture of the DFB laser module and therefore our focus is on the optical hybrid at Bob's node.

Appendix C.1. Optical hybrid

The optical hybrid enables the extraction of the phase and amplitude of the modulated signal by mixing it with the local oscillator signal for coherent detection. We have designed a dual-polarization 90^o optical hybrid for the simultaneous detection of the quantum signal and pilot tones. The combined signal coming from Alice's node via the quantum channel is first separated using a polarization beam splitter. The interference of the X-polarized quantum signal and the X-polarized local oscillator takes place at the two-input, two-output beam splitter. For this, a quantum signal is input at input port-1 of the beam splitter after passing through a quarter-wave plate (QWP) and the local oscillator signal is input at port-2 after passing through a half-wave plate (HWP). The output optical field from the two ports of the beam splitter is passed through two separate polarizing beam splitters, which are connected to photodiodes. The outputs of the four photodiodes are as follows:

$$\begin{aligned}
P_{PD_1} &= \frac{1}{4}|E_Q|^2 + \frac{1}{8}|E_{LO}|^2 + \frac{1}{2\sqrt{2}}E_Q E_{LO}\cos[(\omega_Q - \omega_{LO})t \\
&\quad +\phi(t) - \pi/2] \\
P_{PD_2} &= \frac{1}{4}|E_Q|^2 + \frac{1}{8}|E_{LO}|^2 - \frac{1}{2\sqrt{2}}E_Q E_{LO}\cos[(\omega_Q - \omega_{LO})t \\
&\quad +\phi(t) - \pi/2] \\
P_{PD_3} &= \frac{1}{4}|E_Q|^2 + \frac{1}{8}|E_{LO}|^2 + \frac{1}{2\sqrt{2}}E_Q E_{LO}\cos[(\omega_Q - \omega_{LO})t \\
&\quad +\phi(t)] \\
P_{PD_4} &= \frac{1}{4}|E_Q|^2 + \frac{1}{8}|E_{LO}|^2 - \frac{1}{2\sqrt{2}}E_Q E_{LO}\cos[(\omega_Q - \omega_{LO})t \\
&\quad +\phi(t)]
\end{aligned} \tag{A12}$$

The differential power of the first two photodetectors contains information about the inline modulation and that of photodetectors three and four contains quadrature modulation information as follows:

$$\begin{aligned}
P_I^Q &= P_{PD_1} - P_{PD_2} = \frac{1}{2}E_Q E_{LO}\sin[(\omega_Q - \omega_{LO})t + \phi(t)] \\
P_Q^Q &= P_{PD_3} - P_{PD_4} = \frac{1}{2}E_Q E_{LO}\cos[(\omega_Q - \omega_{LO})t \\
&\quad +\phi(t)]
\end{aligned} \tag{A13}$$

Similarly, the modulation information for the pilot tones is determined by using the other polarization detection mechanism of the optical hybrid. A list of the parameters of the optical hybrid is given in **Table A6**.

Table A6 • List of parameters for optical hybrid module.

Symbol	Parameter	Value
IL_Q	Insertion loss of quantum signal	7 dB
IL_{LO}	Insertion loss of local oscillator signal	8 dB
ϕ_{I-Q}	Phase shift between I and Q	90°
PSR	Polarization splitting ratio	20 dB

References

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6. doi: 10.1145/359340.359342

2. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science; 1994 Nov 20–22; Santa Fe, NM, USA. SFCS-94; Washington (DC): IEEE Computer Society Press; 1994. p. 124–34. doi: 10.1109/SFCS.1994.365700

3. Grover LK. A fast quantum mechanical algorithm for database search. arXiv. 1996. preprint arXiv: quant-ph/9605043. doi: 10.48550/arXiv.quant-ph/9605043

4. Long GL. Grover algorithm with zero theoretical failure rate. Phys Rev A. 2001;64(2):022307. doi: 10.1103/PhysRevA.64.022307

5. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett. 2002;88(5):057902. doi: 10.1103/PhysRevLett.88.057902.

6. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301–50. doi: 10.1103/RevModPhys.81.1301

7. Weedbrook C, Pirandola S, Ralph TC. Continuous-variable quantum key distribution using thermal states. Phys Rev A. 2012;86(2):022318. doi: 10.1103/PhysRevA.86.022318

8. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat Photonics. 2013;7(5):378–81. doi: 10.1038/nphoton.2013.63

9. Zhang Y, Bian Y, Li Z, Yu S, Guo H. Continuous-variable quantum key distribution system: past, present, and future. Appl Phys Rev. 2024;11(1):011318. doi: 10.1063/5.0179566

10. Bian Y, Li Y, Xu X, Zhang T, Pan Y, Huang W, et al. Highly stable power control for chip-based continuous-variable quantum key distribution system. Opt Lett. 2024;49(9):2521. doi: 10.1364/OL.522320

11. Bian Y, Pan Y, Xu X, Zhao L, Li Y, Huang W, et al. Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip. Appl Phys Lett. 2024;124(17):174001. doi: 10.1063/5.0203130

12. Wei SH, Jing B, Zhang X, Liao J, Yuan C, Fan B, et al. Towards real world quantum networks: a review. Laser Photonics Rev. 2022;16(3):2100219. doi: 10.1002/lpor.202100219

13. Liu CJ, Chao Y, Wang L, Li QS. Continuous-variable measurement-device-independent quantum key distribution with multi-ring discrete modulation. Opt Express. 2024;32(18):31549. doi: 10.1364/OE.531896

14. Aquina N, Cimoli B, Das S, Hövelmanns K, Weber FJ, Okonkwo C, et al. A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. EPJ Quantum Technol. 2025;12(1):51. doi: 10.1140/epjqt/s40507-025-00350-5

15. Liao Q, Fei Z, Huang L, Fu X. Practical continuous-variable quantum secret sharing using local local oscillator. Commun Phys. 2025;8(1):138. doi: 10.1038/s42005-025-02061-w

16. Qi B, Huang LL, Qian L, Lo HK. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. Phys Rev A. 2007;76(5):052323. doi: 10.1103/PhysRevA.76.052323

17. Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R, Grangier P. Field test of a continuous-variable quantum key distribution prototype. New J Phys. 2009;11(4):045023. doi: 10.1088/1367-2630/11/4/045023

18. Huang JZ, Weedbrook C, Yin ZQ, Wang S, Li HW, Chen W, et al. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. Phys Rev A. 2013;87(6):062329. doi: 10.1103/PhysRevA.87.062329

19. Ma XC, Sun SH, Jiang MS, Liang LM. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. Phys Rev A. 2013;87(5):052309. doi: 10.1103/PhysRevA.87.052309

20. Qin H, Kumar R, Alleaume R. Saturation attack on continuous-variable quantum key distribution system. In: Lewis KL, Hollins RC, Merlet TJ, Gruneisen MT, Dusek M, Rarity JG, et al., editors, Emerging technologies in security and defence; and quantum security II; and unmanned sensor systems X. vol. 8899. Bellingham (WA): SPIE; 2013. p. 88990N. doi: 10.1117/12.2028543

21. Jouguet P, Kunz-Jacques S, Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys Rev A. 2013;87(6):062313. doi: 10.1103/PhysRevA.87.062313

22. Wath Y, Hariprasad M, Shah F, Gupta S. Eavesdropping a quantum key distribution network using sequential quantum unsharp measurement attacks. Eur Phys J Plus. 2023;138(1):54. doi: 10.1140/epjp/s13360-023-03664-4

23. Kish SP, Thapa C, Sayat M, Suzuki H, Pieprzyk J, Camtepe S. Mitigation of channel tampering attacks in continuous-variable quantum key distribution. Phys Rev Res. 2024;6(2):023301. doi: 10.1103/PhysRevResearch.6.023301

24. Zhou Z, Huang P, Wang T, Zeng G. Security loophole induced by photorefractive effect in continuous-variable quantum key distribution system. Opt Express. 2025;33(10):21736. doi: 10.1364/OE.562658

25. Wang T, Huang P, Zhou Y, Liu W, Ma H, Wang S, et al. High key rate continuous-variable quantum key distribution with a real local oscillator. Opt Express. 2018;26(3):2794. doi: 10.1364/OE.26.002794

26. Wang T, Huang P, Wang S, Zeng G. Carrier-phase estimation for simultaneous quantum key distribution and classical communication using a real local oscillator. Phys Rev A. 2019;99(2):022318. doi: 10.1103/PhysRevA.99.022318

27. Wang H, Pi Y, Huang W, Li Y, Shao Y, Yang J, et al. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. Opt Express. 2020;28(22):32882. doi: 10.1364/OE.404611

28. Chin HM, Hajomer AAE, Jain N, Andersen UL, Gehring T. Machine learning based joint polarization and phase compensation for CV-QKD. In: Optical fiber communication conference (OFC) 2023. Washington (DC): Optica Publishing Group; 2023. p. Th3J.2. doi: 10.1364/OFC.2023.Th3J.2

29. Alsaui A, Alghofaili Y, Venkitesh D. Machine learning and time-series decomposition for phase extraction and symbol classification in CV-QKD. Phys Scr. 2024;99(7):076008. doi: 10.1088/1402-4896/ad538c

30. Huang L, Huang P, Wei S, Xu Y, Li H, Wang T, et al. Efficient carrier-recovery method for simple self-referenced continuous-variable quantum key distribution with a long-short-term memory network. Phys Rev Appl. 2024;22(5):054082. doi: 10.1103/PhysRevApplied.22.054082

31. Feng Y, Jin J, Zhang K, Chen Z, Jiang XQ, Huang P, et al. Multidimensional reconciliation scheme using deep learning in continuous-variable quantum key distribution. New J Phys. 2025;27(5):053201. doi: 10.1088/1367-2630/adcf45

32. Pascual-Garcia C, Bäuml S, Araújo M, Liss R, Acín A. Improved finite-size key rates for discrete-modulated continuous-variable quantum key distribution under coherent attacks. Phys Rev A. 2025;111(2):022610. doi: 10.1103/PhysRevA.111.022610

33. Mailloux LO, Morris JD, Grimaila MR, Hodson DD, Jacques DR, Colombi JM, et al. A modeling framework for studying quantum key distribution system implementation nonidealities. IEEE Access. 2015;3:110–30. doi: 10.1109/ACCESS.2015.2399101

34. Cao Y, Zhao Y, Wang J, Yu X, Ma Z, Zhang J. SDQaaS: software defined networking for quantum key distribution as a service. Opt Express. 2019;27(5):6892. doi: 10.1364/OE.27.006892

35. Chatterjee R, Joarder K, Chatterjee S, Sanders BC, Sinha U. qkdSim, a simulation Toolkit for quantum key distribution including imperfections: performance analysis and demonstration of the B92 protocol using heralded photons. Phys Rev Appl. 2020;14(2):024036. doi: 10.1103/PhysRevApplied.14.024036

36. Fan-Yuan GJ, Chen W, Lu FY, Yin ZQ, Wang S, Guo GC, et al. A universal simulating framework for quantum key distribution systems. Sci China Inf Sci. 2020;63(8):180504. doi: 10.1007/s11432-020-2886-x

37. Bera S, Gupta S, Majumdar AS. Device-independent quantum key distribution using random quantum states. Quantum Inf Process. 2023;22(2):109. doi: 10.1007/s11128-023-03852-2

38. Roy P, Bera S, Gupta S, Majumdar AS. Device-independent quantum secure direct communication under non-Markovian quantum channels. Quantum Inf Process. 2024;23(5):170. doi: 10.1007/s11128-024-04397-8

39. Sethia A, Banerjee A. A MATLAB-based modelling and simulation package for DPS-QKD. J Mod Opt. 2022;69(7):392–402. doi: 10.1080/09500340.2022.2041752

40. Gupta S. Experimental simulation of the quantum secure direct communication using MATLAB and Simulink. Eur Phys J Plus. 2023;138(10):913. doi: 10.1140/epjp/s13360-023-04532-x

41. Gupta S, Agarwal I, Mogiligidda V, Kumar Krishnan R, Chennuri S, Aggarwal D, et al. ChaQra: a cellular unit of the Indian quantum network. Sci Rep. 2024;14(1):16752. doi: 10.1038/s41598-024-67495-8

42. Wolf MM, Giedke G, Cirac JI. Extremality of gaussian quantum states. Phys Rev Lett. 2006;96(8):080502. doi: 10.1103/PhysRevLett.96.080502

43. Lin J, Lütkenhaus N. Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. PHysical Rev Appl. 2020;14(6):064030. doi: 10.1103/PhysRevApplied.14.064030

44. Liu WB, Li CL, Xie YM, Weng CX, Gu J, Cao XY, et al. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. PRX Quantum. 2021;2(4):040334. doi: 10.1103/PRXQuantum.2.040334

45. Upadhyaya T, van Himbeeck T, Lin J, Lütkenhaus N. Dimension reduction in quantum key distribution for continuous-and discrete-variable protocols. PRX Quantum. 2021;2(2):020325. doi: 10.1103/PRXQuantum.2.020325

46. Kanitschar F, Pacher C. Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection. Phys. Rev. Appl. 2022;18(3):034073. doi: 10.1103/PhysRevApplied.18.034073

47. Wang P, Zhang Y, Lu Z, Wang X, Li Y. Discrete-modulation continuous-variable quantum key distribution with a high key rate. New J Phys. 2023;25(2):023019. doi: 10.1088/1367-2630/acb964

48. Coles PJ, Metodiev EM, Lütkenhaus N. Numerical approach for unstructured quantum key distribution. Nat Commun. 2016;7(1):11712. doi: 10.1038/ncomms11712

49. Winick A, Lütkenhaus N, Coles PJ. Reliable numerical key rates for quantum key distribution. Quantum. 2018:2:77. doi: 10.22331/q-2018-07-26-77