NANOSYSTEMS:
PHYSICS, CHEMISTRY, MATHEMATICS

Goncharov R.K., et al. *Nanosystems: Phys. Chem. Math.*, 2022, **13** (4), 372–391.
http://nanojournal.ifmo.ru
DOI 10.17586/2220-8054-2022-13-4-372-391

Original article

Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks

Roman K. Goncharov[a], Alexei D. Kiselev[b], Eduard O. Samsonov[c], Vladimir I. Egorov[d]

ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia

[a]rkgoncharov@itmo.ru, [b]alexei.d.kiselev@gmail.com, [c]eosamsonov@itmo.ru, [d]viegorov@itmo.ru

Corresponding author: R. K. Goncharov, rkgoncharov@itmo.ru

PACS 03.67.-a, 42.50.-p

ABSTRACT In this paper, using the full security framework for continuous-variable quantum key distribution (CV-QKD), we provide a composable security proof for the CV-QKD system in a realistic implementation. We take into account equipment losses and contributions from various components of excess noise and evaluate performance against collective and coherent attacks assuming trusted hardware noise. The calculation showed that the system remains operable at channel losses up to 10.2 dB in the presence of collective attacks and up to 7.5 dB in the presence of coherent ones.

KEYWORDS quantum key distribution, continuous variables, security proof, composability, trusted noise.

ACKNOWLEDGEMENTS The work was done by Leading Research Center "National Center for Quantum Internet" of ITMO University by order of JSCo Russian Railways.

FOR CITATION Goncharov R. K., Kiselev A. D., Samsonov E. O., Egorov V. I. Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks. *Nanosystems: Phys. Chem. Math.*, 2022, **13** (4), 372–391.

1. Introduction

Quantum key distribution (QKD) [1] is a special method of generating a secure key between two parties, Alice and Bob, which will ensure the privacy of transmitted information in the era of the quantum computer. Historically, the first protocols to be presented were discrete variable (DV) ones [2, 3], where information was encoded in the state of a single photon: polarization, phase or time bin. However, over time, continuous-variable (CV) protocols [4–6] have been introduced, which are considered more efficient, high-rate and cost-effective due to the use of homodyne/heterodyne detection systems instead of single photon detectors.

Considering the security of QKD systems, one must take into account that each of them has a finite physical implementation that is not ideal, which opens up opportunities for the eavesdropper, Eve, to carry out a multiple attacks and extract part of the secret key. To prevent this threat, for each protocol, a complex system for assessing the information available to Eve and the acceptable level of errors is being developed.

Currently, a fairly significant amount of work has been presented, covering the topic of security of CV-QKD protocols [7–14]. Of the protocols most suitable for practical implementation, the GG02 protocol [6, 15] stands out, for which the security is proven against coherent (general) attacks, taking into account the finite-key effects. Moreover, models of untrusted and trusted hardware noise are considered [12]. The latter is preferable, since many security levels imply that Eve does not have access to Alice's and Bob's blocks, moreover, accounting for untrusted noise makes the protocol essentially unusable.

Thus, this paper will present a full security proof of CV-QKD on a realistic implementation with trusted hardware noise against general attacks. In Section 2 we describe an optical configuration of the CV-QKD scheme, in Sections 3–5 we give a description of the protocol in the trusted noise scenario and consider a possibility of specific attacks that go beyond general security proof framework. In Section 6 we provide a technique of evaluation and monitoring of experimental parameters and in Section 7 we clarify security analysis and estimate the finite-length secure key generation rate. In Section 8 we discuss the results and draw the appropriate conclusions.

2. Optical CV-QKD scheme configuration

The optical scheme of the described protocol is shown in Fig. 1 and consists of the following blocks:

- Alice block, in which the generation of signal states (Gaussian modulation) and a local oscillator (LO) is carried out, after which, by means of polarization-time multiplexing, they sent to Bob. Gaussian modulation itself can be done in two stages: amplitude modulation with a Rayleigh distribution and phase modulation with a uniform phase distribution; as a result, the complex signal amplitude value will correspond to the Gaussian distribution [16]. It should also be noted that the need for reference signal, which is used in the phase protocols of the DV-QKD [3, 17], is no longer necessary in this case.
- Quantum channel block, which in this work is represented by an optical fiber.
- Bob block, in which demultiplexing and heterodyne detection are carried out.

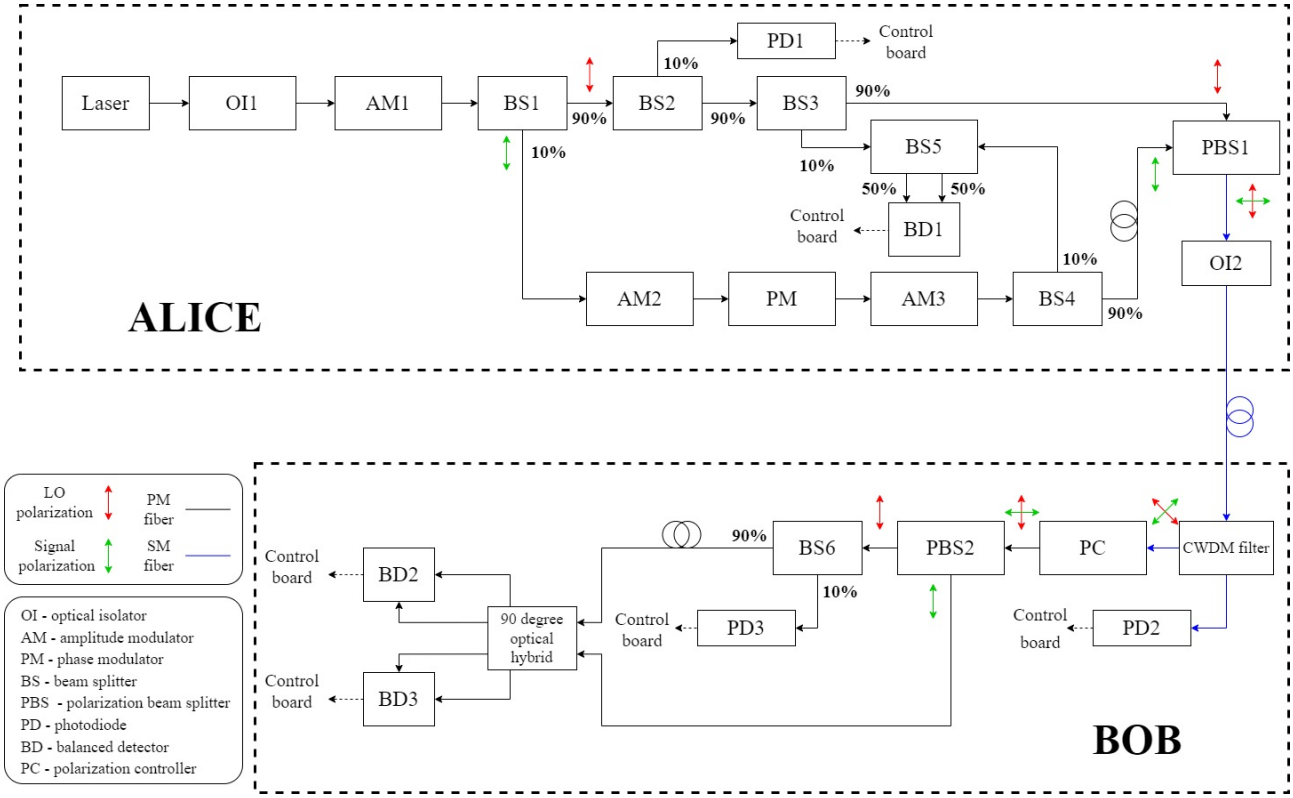

FIG. 1. Scheme of typical setup for CV-QKD with Gaussian modulation and heterodyne detection.

In the considered configuration, Alice uses the same laser to generate LO and signal states modulated according to the Gaussian distribution, which then experience the procedure of polarization-time multiplexing before sending through the quantum channel. Bob then performs a demultiplexing procedure and heterodyne detection. Fig. 1 also shows additional elements for monitoring.

In Alice block, a continuous wave (CW) laser with a central wavelength of 1550 nm and a spectral line width of 100 kHz is used. The width of the spectral line makes it possible to estimate the coherence time, and also affects the amount of phase noise. Coherent detection systems require the use of sources with a narrow spectral line. The Bob block uses a polarization-maintaining optical fiber of the Panda type due to the sensitivity of the optoelectronic components to polarization and implementation polarization multiplexing. The optical isolator OI1 is used in order to avoid backlight due to reflection on the optical scheme elements in the laser module. An amplitude modulator AM1 is used to form identical optical pulses with a repetition rate of 50 MHz and a duration of 3 ns. Laser pulses are then divided by amplitude into two arms using a 10/90 beam splitter BS1: the signal arm (10%) and LO arm (90%).

The second 90/10 beam splitter BS2 in the LO arm is used to separate 10% of the optical pulse power and direct it to the photodiode PD1, which allows one to organize feedback with an amplitude modulator to control the power of LO.

In the signal arm, Gaussian modulation of optical pulses occurs using an amplitude modulator AM2 and a phase modulator PM. Amplitude modulation is realized according to the Rayleigh distribution with a given variance. Phase modulation is implemented according to a uniform distribution in the range from 0 to 2π. The amplitude modulator AM3 is used as a fast attenuator with a wide range of extinction coefficient to set the average number of photons in an optical pulse. Every second pulse in the signal arm is a reference pulse and is not subjected to amplitude and phase modulation on amplitude modulators AM1 and AM2 and phase modulator PM. The modulators are controlled by a digital-to-analog converter (DAC), which is not indicated on Fig. 1.

In the signal and LO arms, 90:10 beam splitters BS3 and BS4 are used to separate part of the signal and LO pulses to control the power and variance (feedback for amplitude modulators AM1 and AM2) using a homodyne detector, which is carried out using 50/50 beam splitter BS5 and balanced detector BD1. For successful balanced detection, it is necessary that the optical paths of the signal and LO are identical.

In order to avoid the interaction of signal pulses and LO before their detection in Bob's side, time-division and polarization multiplexing is used. Time-division multiplexing is implemented by increasing length of the signal arm in Alice's side by an amount corresponding to half the pulse repetition period compared to LO arm. Polarization multiplexing is implemented using a polarization combiner PBS1 with a single-mode (SM) output, to which polarization maintaining fibers of two arms are connected with mutually orthogonal slow optical axes.

A SM optical isolator OI2 is used to prevent backlighting of Alice from the channel output. Alice and Bob are connected through a SM optical fiber of the G.652.D standard with a length of 25 km.

On Bob side, the signal and LO enter the CWDM filter with a central wavelength of 1550 nm. The use of a CWDM filter is due to protection against backlight at a different wavelength from the channel input. The output of the CWDM filter which corresponds to the reflected light is connected with the monitor photodiode PD2, by the signal from which one can analyse the presence or absence of backlights. The output of the CWDM filter which corresponds to the transmitted light, is connected with the input of the polarization controller PC, which is used to compensate for polarization distortions in the SM optical fiber between Alice and Bob. The input of a polarization beam splitter PBS2 is connected to the output of the polarization controller, which is used for polarization demultiplexing of the signal and LO. In the LO arm, there is a delay line for demultiplexing signals in time domain and also a 90:10 beam splitter BS6, which is used to organize the feedback of the polarization controller: a part of LO pulse power (10%) is sent to the photodiode PD3 to determine the optical power. The other output of the 90/10 beam splitter, which corresponds to 90% optical power, is connected to LO input of the 90-degree optical hybrid. In the signal arm, after the output of the polarizing beam splitter PBS2, it is connected to the signal input of the 90-degree optical hybrid. The 90-degree optical hybrid has four outputs: two outputs correspond to the sum and the difference amplitude of the signal field and LO with zero additional relative phase and two outputs correspond to an additional phase equal to 90 degrees. The outputs of the 90-degree optical hybrid are connected to the inputs of two balanced detectors. The signal from the balanced detectors is entered to analog-to-digital converter (ADC), which is not shown in Fig. 1).

3. GG02 protocol features

3.1. Gaussian modulation of coherent states

In the CV-QKD with Gaussian modulation [6,15], Alice prepares coherent states (with a given value of amplitude and phase) with quadrature components q and p which are realizations of two independent and identically distributed random variables $\mathcal{Q}$ and $\mathcal{P}$, which have the same Gaussian distribution with zero mean and given variance

$$\mathcal{Q} \sim \mathcal{P} \sim \mathcal{N}\left(0,\, \tilde{V}_{\mathrm{A}}\right), \tag{1}$$

where $\tilde{V}_{\mathrm{A}}$ is a modulation variance.

Alice prepares a sequence of coherent states $|\alpha_1\rangle, \ldots |\alpha_j\rangle, \ldots, |\alpha_N\rangle$ of the form:

$$|\alpha_j\rangle = |q_j + ip_j\rangle, \text{ for } q_j \in \mathcal{Q},\, p_j \in \mathcal{P}. \tag{2}$$

In this case, the equations for the eigenvalues are satisfied in shot noise units (SNU)

$$\hat{a}|\alpha_j\rangle = \alpha_j|\alpha_j\rangle, \tag{3}$$

$$\frac{1}{2}(\hat{q} + i\hat{p})|\alpha_j\rangle = (q_j + ip_j)|\alpha_j\rangle, \tag{4}$$

where $\hat{a}$ is a creation operator and $\hat{p}$, $\hat{q}$ are a quadrature operators.

The mean photon number in each individual state is estimated as follows

$$\langle n_j\rangle = \langle\alpha_j|\hat{n}|\alpha_j\rangle = |\alpha_j|^2 = q_j^2 + p_j^2. \tag{5}$$

Given that q_j and p_j taken from the distribution in Eq. (1), the mean photon number over the ensemble of states prepared by Alice is

$$\langle n\rangle = \langle\mathcal{Q}^2\rangle + \langle\mathcal{P}^2\rangle = 2\tilde{V}_{\mathrm{A}}. \tag{6}$$

To calculate the variance of the quadrature operator $V(\hat{q}) = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2$, it is necessary to find the averaged values:

$$\langle \hat{q} \rangle = \langle \alpha | \hat{q} | \alpha \rangle = 0, \tag{7}$$

$$\begin{aligned} \langle \hat{q}^2 \rangle &= \langle \alpha | \hat{q}^2 | \alpha \rangle = \langle \alpha | (\hat{a} + \hat{a}^\dagger)^2 | \alpha \rangle = \\ &= \langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle + \langle \alpha | \hat{a}\hat{a}^\dagger | \alpha \rangle + \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = \\ &= \alpha^2 + (\alpha^*)^2 + \alpha^* \alpha + 1 + \alpha^* \alpha = \\ &= q^2 - p^2 + 2iqp + q^2 - p^2 - 2iqp + 2(q^2 + p^2) + 1 = \\ &= 4q^2 + 1. \end{aligned} \tag{8}$$

Considering that the values q and p are realizations of the random variables $\mathcal{Q}$ and $\mathcal{P}$, respectively, we can write:

$$\langle \hat{q}^2 \rangle = 4\langle \mathcal{Q}^2 \rangle + 1 = 4\tilde{V}_{\mathrm{A}} + 1, \tag{9}$$

$$\langle \hat{p}^2 \rangle = 4\langle \mathcal{P}^2 \rangle + 1 = 4\tilde{V}_{\mathrm{A}} + 1. \tag{10}$$

According to Eqs. (9), one has:

$$V \equiv V(\hat{q}) = V(\hat{p}) \equiv V = 4\tilde{V}_{\mathrm{A}} + 1 \equiv V_{\mathrm{A}} + 1. \tag{11}$$

In Eq. (11), the transition from the variance of random variable corresponding to the quadrature distribution to the variance of quadrature operator is carried out. It should be noted that there is also a shot noise component in SNU (equal to one).

Combining (6) and (11), we can express the average number of photons over the ensemble in terms of the variance of quadrature operator

$$\langle n \rangle = \frac{1}{2}(V - 1) = \frac{1}{2}V_{\mathrm{A}}. \tag{12}$$

After the preparation stage, Alice sends the $|\alpha_j\rangle$ state to the Gaussian quantum channel, after which Bob performs coherent detection and decodes information about the sent state in the case of heterodyne detection or the projection of its quadrature components in the case of homodyne detection. It should be emphasized that in this paper only heterodyne detection is considered.

3.2. Gaussian sequence processing

This subsection briefly describes the stages of classical data post-processing, which means Alice's modulation and Bob's detection results data.

The first step is sifting. Despite sifting is not implied in the case of heterodyne detection (in which the sequence after the distribution session and before error correction can be considered as a sifted key), it is worth mentioning that in CV-QKD with homodyne detection, Alice and Bob choose the bases they use to prepare and measure the states respectively, using independently and identically distributed generated random bits. In these cases, the sifting step eliminates all uncorrelated signals when different bases were used for preparation and measurement. The presence of signal bases is more typical for CV-QKD protocols with discrete modulation, however, in protocols with Gaussian modulation and homodyne detection, sifting means discarding the quadrature not measured by Bob.

The second step is parameter estimation. After transmitting and detecting a sequence of states, legitimate parties compare a random subset of their data. This comparison allows one to estimate the quantum channel parameters: transmittance and excess noise of the channel, from which they can calculate a mutual information I_{AB} and evaluate an information χ available to Eve. If χ is greater than βI_{AB}, where $\beta \in [0,\ 1]$ is the reconciliation efficiency, the protocol is aborted at this point.

If $\beta I_{\mathrm{AB}} > \chi$, users go to the third, information reconciliation step, which is a form of error correction procedure.

The fourth step is confirmation. After the reconciliation procedure, legitimate parties perform a confirmation step using a family of universal hash functions [18] to limit the chance that error correction fails: Alice or Bob chooses one particular hash function with uniform probability and announces its choice over the classical channel. Users apply this hash function to their key to get a hash code. Subsequently, Alice and Bob exchange and compare their hash codes. If the values are different, the keys are considered compromised and the protocol is aborted; if the values are equal, then it is considered that an upper bound on the probability that the keys are not identical has been obtained. This error rate depends on the length of the hash codes and the type of hash functions used.

The fifth and final step is privacy amplification. After successfully passing the confirmation stage, Alice and Bob will have the same bit string with a very high probability. However, Eve has some information about the key, so to reduce the chance that she successfully guesses part of the key to an acceptable value, users perform a privacy amplification protocol by applying a seeded randomness extraction algorithm to their bit strings, which uses a family of 2-universal hash functions.

3.3. Quantum channel description

The Gaussian quantum channel is characterized by the transmittance coefficient (taking into account losses directly in the channel, losses in the equipment and detection efficiency) and noise (on Alice side, in the channel, and on Bob side). The potential advantage of Eve depends on both characteristics. The noise in the channel can be expressed as [1, 13, 19]

$$\Xi_{\text{ch}} = \frac{1 - T_{\text{ch}}}{T_{\text{ch}}} + \xi_{\text{A}}, \tag{13}$$

where T_{ch} is a quantum channel transmittance, ξ_{A} is a excess noise (in SNU).

The excess noise itself includes variances of all noise sources

$$\xi_{\text{A}} = \xi_{\text{modul, A}} + \xi_{\text{Raman, A}} + \xi_{\text{phase, A}} + \cdots, \tag{14}$$

where $\xi_{\text{modul, A}}$ is the modulation noise, $\xi_{\text{Raman, A}}$ is the Raman noise, and $\xi_{\text{phase, A}}$ is the phase noise.

Similarly, the detector noise can be estimated as [1, 13, 14, 19]

$$\Xi_{\text{det}} = \frac{1 - T_{\text{rec}}\eta_{\text{det}}}{T_{\text{rec}}\eta_{\text{det}}} + \frac{v_{\text{el}}}{T_{\text{rec}}\eta_{\text{det}}}, \tag{15}$$

where η_{det} is the balanced detector efficiency, v_{el} is the electronic noise of the balanced detector and T_{rec} is the transmittance coefficient responsible for losses in the receiver module.

For a more convenient notation, it can be written as

$$T_{\text{det}} \equiv T_{\text{rec}}\eta_{\text{det}}. \tag{16}$$

The total noise related to the channel input is then determined by the sum of the channel noise and the detector noise normalized to T_{ch}

$$\Xi = \Xi_{\text{ch}} + \frac{1}{T_{\text{ch}}}\Xi_{\text{det}}. \tag{17}$$

After the signal state passing through a channel with noise and losses, Bob measures the total variance of the quadrature operator as [1, 13, 14, 19]

$$\begin{aligned} V_{\text{B}} &= V\left(\hat{q}_{\text{B}}\right) = V\left(\hat{p}_{\text{B}}\right) = T_{\text{ch}}T_{\text{det}}(V + \Xi) = \\ &= T_{\text{ch}}T_{\text{det}}\left(V + \frac{1 - T_{\text{ch}}}{T_{\text{ch}}} + \xi_{\text{A}} + \frac{1}{T_{\text{ch}}}\left(\frac{1 - T_{\text{det}}}{T_{\text{det}}} + \frac{v_{\text{el}}}{T_{\text{det}}}\right)\right) = \\ &= T_{\text{ch}}T_{\text{det}}V - T_{\text{ch}}T_{\text{det}} + T_{\text{ch}}T_{\text{rec}}\eta_{\text{det}}\xi_{\text{A}} + 1 + v_{\text{el}} \equiv \\ &\equiv TV - T + T\xi_{\text{A}} + 1 + v_{\text{el}} = \\ &= T(V - 1) + T\xi_{\text{A}} + 1 + v_{\text{el}}. \end{aligned} \tag{18}$$

Since the parameter v_{el} is the noise variance in SNU and can be considered stochastically independent of other noise sources, it can be considered as another component of the excess noise, i.e. $v_{\text{el}} \equiv \xi_{\text{det}}$, thus

$$T\xi_{\text{A}} + \xi_{\text{det}} = T\left(\xi_{\text{A}} + \frac{1}{T}\xi_{\text{det}}\right) \equiv T\xi_{\text{tot, A}} = \xi_{\text{tot, B}} \equiv \xi, \tag{19}$$

$$V_{\text{B}} = T(V - 1) + 1 + \xi = TV_{\text{A}} + 1 + \xi. \tag{20}$$

3.4. Signal-to-noise ratio and mutual information

The signal-to-noise ratio is expressed as

$$\text{SNR} = \frac{P_{\text{S}}}{P_{\text{N}}}, \tag{21}$$

where P_{S} is the total signal power and P_{N} is the total noise power.

The purposed model makes it possible to separate the signal and noise components in the variance of the quadrature operator observed by Bob

$$V_{\text{B}} = \frac{T}{\mu}V_{\text{A}} + 1 + \frac{\xi}{\mu}, \tag{22}$$

where $\mu \in \{1;\ 2\}$ is the homodyne/heterodyne detection system parameter, respectively.

Thus, the signal-to-noise ratio for the purposed protocol is as follows

$$\text{SNR} = \frac{\frac{1}{\mu}TV_{\text{A}}}{1 + \frac{1}{\mu}\xi}. \tag{23}$$

Mutual information between Alice and Bob in this case is evaluated as [13]

$$I_{\text{AB}} = \frac{\mu}{2}\log_2(1 + \text{SNR}) = \frac{\mu}{2}\log_2\left(1 + \frac{\frac{1}{\mu}TV_{\text{A}}}{1 + \frac{1}{\mu}\xi}\right). \tag{24}$$

As it has been already mentioned, the purposed protocol assumes a heterodyne detection method, i.e. $\mu = 2$. According to Eq. (24), despite the increase in mutual information by a factor of two (two quadratures per message are detected at once, instead of one), the signal-to-noise ratio decreases. Obviously (estimating the rate of increase of logarithmic functions), the advantage of heterodyne detection in terms of estimating mutual information will be observed only at large TV_{A}.

4. Trusted hardware noise. Holevo bound

After variable ρ_{AB} has been removed from the shared state equation, it can be viewed as a pure two-particle state with a common Alice and Bob on one side and Eve on the other. As such, it can be written in terms of the Schmidt decomposition

$$|\Psi_{\mathrm{ABE}}\rangle = \sum_i \sqrt{\lambda_i}\,|\psi_i\rangle_{\mathrm{AB}}\,|\phi_i\rangle_{\mathrm{E}}\,, \tag{25}$$

where λ_j is a real non-negative number.

Taking a partial trace over subsystems gives one

$$\mathrm{Tr}_{\mathrm{E}}\,\rho_{\mathrm{AB}} = \rho_{\mathrm{AB}} = \sum_i \lambda_i |\psi_i\rangle_{\mathrm{AB}}\langle\psi_i|, \tag{26}$$

$$\mathrm{Tr}_{\mathrm{AB}}\,\rho_{\mathrm{AB}} = \rho_{\mathrm{E}} = \sum_i \lambda_i |\phi_i\rangle_{\mathrm{E}}\langle\phi_i|. \tag{27}$$

The von Neumann entropy depends only on the λ_i components, which, due to the Schmidt decomposition, are the same for ρ_{AB} and ρ_{E}. Therefore, the von Neumann entropy of Eve is the same as the entropy shared by Alice and Bob

$$S_{\mathrm{E}} = S_{\mathrm{AB}} = -\sum_i \lambda_i \log_2 \lambda_i. \tag{28}$$

Then, the following transformation is obvious

$$\chi_{\mathrm{E}} = S_{\mathrm{E}} - S_{\mathrm{E|B}} = S_{\mathrm{AB}} - S_{\mathrm{A|B}}. \tag{29}$$

In the trusted noise model [12], the noise coming from the Alice's and Bob's equipment is assumed to be trusted, that is, Eve cannot manipulate it. The same applies to equipment losses. In this context, it is necessary to clarify Eq. (19)

$$\xi = T\xi_{\mathrm{pr}} + T_{\mathrm{det}}\xi_{\mathrm{ch}} + \xi_{\mathrm{rec}}, \tag{30}$$

where ξ_{pr} is the Alice excess noise, ξ_{ch} is the channel excess noise, and ξ_{rec} is the Bob excess noise.

Assuming that the detection devices are well calibrated and reliable, T_{rec} and ξ_{rec} are beyond Eve's influence. Then the covariance matrix describing its von Neumann entropy prior to measurement by Bob is as follows

$$\Sigma_{\mathrm{AB}}^{\text{trusted rec.}} = \begin{pmatrix} V\mathbf{1}_2 & \sqrt{T_{\mathrm{ch}}(V^2-1)}\sigma_z \\ \sqrt{T_{\mathrm{ch}}(V^2-1)}\sigma_z & (T_{\mathrm{ch}}(V-1)+1+\xi_{\mathrm{ch}})\,\mathbf{1}_2 \end{pmatrix}. \tag{31}$$

The matrix itself can be represented in the form

$$\begin{pmatrix} a\mathbf{1}_2 & c\sigma_z \\ c\sigma_z & b\mathbf{1}_2 \end{pmatrix}. \tag{32}$$

The symplectic eigenvalues of this matrix are expressed as

$$v_{1,\,2} = \frac{1}{2}(z \pm (b-a)), \tag{33}$$

where $z = \sqrt{(a+b)^2 - 4c^2}$.

Although in the trusted noise model the quantities T_{rec} and ξ_{rec} do not contribute to S_{E}, though they do affect Alice measurements and, consequently, Eve entropy $S_{\mathrm{E|B}}$.

In the trusted noise scenario, the eavesdropper can only manipulate the state in the channel and carry out purifying in the same place. This means that the state of the system must be viewed through three distinct subsystems in the entanglement base scenario. Let the state "Alice-Bob-Eve" consist of two entangled states and a thermal state, each of which is uniquely determined by its variance: one entangled state $\mathrm{EPR}_{\mathrm{AB}}$ with variance V used for key exchange between Alice and Bob, one entangled state $\mathrm{EPR}_{\mathrm{ch}}$ with variance W_{ch} for modeling noise and loss in the quantum channel and thermal state $\mathrm{Th}_{\mathrm{rec}}$ with variance W_{rec} to simulate the noise and losses of the receiver. The beam splitters, one with T_{ch} transmittance and one with T_{rec} transmittance, mix the initial Bob's entangled state modes with the channel state and

the thermal state modes, respectively. The general state before the action of the beam splitters can be represented by the covariance matrix

$$\Sigma_{\text{tot},\,0} = \text{EPR}_{\text{AB}} \oplus \text{EPR}_{\text{ch}} \oplus \text{Th}_{\text{rec}} = \\ = \begin{pmatrix} V\mathbf{1}_2 & \sqrt{V^2-1}\sigma_z & 0 & 0 & 0 \\ \sqrt{V^2-1}\sigma_z & V\mathbf{1}_2 & 0 & 0 & 0 \\ 0 & 0 & W_{\text{ch}}\mathbf{1}_2 & \sqrt{W_{\text{ch}}^2-1}\sigma_z & 0 \\ 0 & 0 & \sqrt{W_{\text{ch}}^2-1}\sigma_z & W_{\text{ch}}\mathbf{1}_2 & 0 \\ 0 & 0 & 0 & 0 & W_{\text{rec}}\mathbf{1}_2 \end{pmatrix}. \tag{34}$$

It can be noted here that the eavesdropper attack on the quantum channel involves only two entangled states, EPR_{AB} and EPR_{ch}, which guarantees purifying as part of an attack. Unitary equivalence with complete purifying thus makes it easier to express the state on Bob's side: in the general case, it must be represented by another entangled state [14].

The beam splitter in the channel affects Alice's mode and one of the EPR_{ch} state modes; the second beam splitter affects Bob's mode and the thermal state simulating the detection module

$$\text{BS}_{\text{ch}} = \begin{pmatrix} \mathbf{1}_2 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{T_{\text{ch}}}\mathbf{1}_2 & \sqrt{1-T_{\text{ch}}}\mathbf{1}_2 & 0 & 0 \\ 0 & -\sqrt{1-T_{\text{ch}}}\mathbf{1}_2 & \sqrt{T_{\text{ch}}}\mathbf{1}_2 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1}_2 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1}_2 \end{pmatrix}, \tag{35}$$

$$\text{BS}_{\text{rec}} = \begin{pmatrix} \mathbf{1}_2 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{T_{\text{det}}}\mathbf{1}_2 & 0 & 0 & \sqrt{1-T_{\text{det}}}\mathbf{1}_2 \\ 0 & 0 & \mathbf{1}_2 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1}_2 & 0 \\ 0 & -\sqrt{1-T_{\text{det}}}\mathbf{1}_2 & 0 & 0 & \sqrt{T_{\text{det}}}\mathbf{1}_2 \end{pmatrix}. \tag{36}$$

Denoting the sequence of both beam splitters as $\text{BS}_{\text{tot}} = \text{BS}_{\text{rec}}\text{BS}_{\text{ch}}$, the total quantum state is transformed as follows

$$\Sigma_{\text{tot}} = \text{BS}_{\text{tot}}\Sigma_{\text{tot},0}\text{BS}_{\text{tot}}^T. \tag{37}$$

To simplify expressions for the covariance matrix, it should be considered block by block. Thus, the block describing the Alice-Bob subsystem is transformed as follows

$$\Sigma_{\text{AB}} = \begin{pmatrix} V\mathbf{1}_2 & \sqrt{T_{\text{ch}}}\sqrt{T_{\text{det}}}\sqrt{V^2-1}\sigma_z \\ \sqrt{T_{\text{ch}}}\sqrt{T_{\text{det}}}\sqrt{V^2-1}\sigma_z & \begin{pmatrix} T_{\text{ch}}T_{\text{det}}V \\ +(1-T_{\text{ch}})\,T_{\text{det}}W_{\text{ch}} \\ +(1-T_{\text{det}})\,W_{\text{rec}} \end{pmatrix} \end{pmatrix}. \tag{38}$$

Let the variances for entangled states be defined as

$$W_{\text{ch}} = \frac{\xi_{\text{ch}}}{1-T_{\text{ch}}} + 1, \tag{39}$$

$$W_{\text{rec}} = \frac{\xi_{\text{rec}}}{1-T_{\text{det}}} + 1. \tag{40}$$

Then the variance of Bob's quadrature operator is as follows

$$V_{\text{B}} = T_{\text{ch}}T_{\text{det}}(V-1) + 1 + T_{\text{det}}\xi_{\text{ch}} + \xi_{\text{rec}} = \\ = T_{\text{ch}}T_{\text{det}}(V-1) + 1 + \xi_{\text{ch},B} + \xi_{\text{rec}}. \tag{41}$$

The final expression for the Alice-Bob block is

$$\Sigma_{\text{AB}} = \begin{pmatrix} V\mathbf{1}_2 & \sqrt{T}\sqrt{V^2-1}\sigma_z \\ \sqrt{T}\sqrt{V^2-1}\sigma_z & (T(V-1)+1+\xi)\,\mathbf{1}_2 \end{pmatrix}. \tag{42}$$

The Eve block is described by the matrix

$$\Sigma_{\mathrm{E}} = \begin{pmatrix} \left(\left(1-T_{\mathrm{ch}}\right)V + T_{\mathrm{ch}}W_{\mathrm{ch}}\right)\mathbf{1}_2 & \sqrt{T_{\mathrm{ch}}}\sqrt{\mathrm{W}_{\mathrm{ch}}^2-1}\sigma_z \\ \sqrt{T_{\mathrm{ch}}}\sqrt{W_{\mathrm{ch}}^2-1}\sigma_z & W_{\mathrm{ch}}\mathbf{1}_2 \end{pmatrix}. \tag{43}$$

This matrix can be described in the form given by Eq. (32), so its symplectic eigenvalues can be calculated by Eq. (33). It can be verified that the entropy of Eve S_{E} is the same as the entropy shared by Alice and Bob and obtained from their mutual covariance matrix in the trusted receiver noise scenario from Eq. (31), which is expected when Eve purifies the state of Alice and Bob, i.e.

$$S_{\mathrm{E}} \equiv S\left(\Sigma_{\mathrm{E}}\right) = S\left(\Sigma_{\mathrm{AB}}^{\text{trusted rec.}}\right) \equiv S_{\mathrm{AB}}. \tag{44}$$

Now, in order to get $S_{\mathrm{E|B}}$, we have to calculate $\Sigma_{\mathrm{tot|B}}$, i.e. the covariance matrix of the common state of the remaining modes after the projective measurement of the receiver mode. It is convenient to represent Σ_{tot} so that the Alice's mode is located in the last row and column. This can be done by using a permutation matrix, which allows to rearrange the third and fourth rows (columns) down (to the right) when multiplied by Σ_{tot} from the left (right) [14]:

$$P_{3,\,4\to9,\,10} = \begin{pmatrix} \mathbf{1}_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1}_2 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1}_2 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1}_2 \\ 0 & \mathbf{1}_2 & 0 & 0 & 0 \end{pmatrix}, \tag{45}$$

$$\Sigma'_{\mathrm{tot}} = P_{3,4\to9,10}\Sigma_{\mathrm{tot}}P_{3,4\to9,10}^T. \tag{46}$$

Since $P_{3,\,4\to9,\,10}P_{3,\,4\to9,\,10}^T = \mathbf{1}$, the above permutation is a similarity transformation and therefore leaves the eigenvalues of the matrix Σ_{tot} invariant. The covariance matrix itself now looks like this:

$$\Sigma'_{\mathrm{tot}} = \begin{pmatrix} \Sigma_{\mathrm{A,\,ch,\,rec}} & \Sigma_{\mathrm{C}} \\ \Sigma_{\mathrm{C}}^T & \Sigma_{\mathrm{B}} \end{pmatrix}, \tag{47}$$

where $\Sigma_{\mathrm{A,\,ch,\,rec}} \in \mathbb{R}^{8\times8}$ is a matrix describing the Alice's mode and the state of the channel and the detection module, $\Sigma_{\mathrm{B}} \in \mathbb{R}^{2\times2}$ is a matrix describing the Bob's mode, and $\Sigma_C \in \mathbb{R}^{8\times2}$ is a matrix describing quadrature correlations between $\Sigma_{\mathrm{A,\,ch,\,rec}}$ and Σ_{B}.

The $\Sigma_{\mathrm{tot|B}}$ matrix after a projective measurement of the Bob's mode depends on whether it performs homodyne or heterodyne detection.

In the case of heterodyne detection, the remaining modes are projected into the state described by the 8×8 matrix

$$\Sigma_{\mathrm{tot|B}} = \Sigma_{\mathrm{A,\,ch,\,rec}} - \frac{1}{V_{\mathrm{B}}+1}\Sigma_{\mathrm{C}}\Sigma_{\mathrm{C}}^T. \tag{48}$$

Again, there is no need to evaluate the entire covariance matrix. Instead, one can evaluate a block describing the eavesdropper information that is two modes representing the entangled state that was used to model the noise and the channel loss. The block itself is expressed as follows

$$\Sigma_{\mathrm{E|B}} = \frac{1}{V_{\mathrm{B}}+1}\begin{pmatrix} e_1\mathbf{1}_2 & e_2\sigma_z \\ e_2\sigma_z & e_3\mathbf{1}_2 \end{pmatrix}, \tag{49}$$

$$\begin{aligned} e_1 = {} & V\left(\left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}} + T_{\mathrm{rec}}W_{\mathrm{ch}} + 1\right) + \\ & + T_{\mathrm{ch}}\left(W_{\mathrm{ch}} - V\right)\left(1 + \left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}}\right), \end{aligned} \tag{50}$$

$$e_2 = \sqrt{T_{\mathrm{ch}}\left(W_{\mathrm{ch}}^2-1\right)}\left(T_{\mathrm{rec}}V + \left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}} + 1\right), \tag{51}$$

$$e_3 = \left(1-T_{\mathrm{rec}}\right)W_{\mathrm{ch}}W_{\mathrm{rec}} + T_{\mathrm{rec}}T_{\mathrm{ch}}\left(VW_{\mathrm{ch}} - 1\right) + T_{\mathrm{rec}} + W_{\mathrm{ch}}. \tag{52}$$

Considering that the matrix $\Sigma_{\mathrm{E|B}}$ can also be represented in the form of Eq. (32), then the symplectic eigenvalues can also be represented similarly to Eq. (33) as

$$v_{3,\,4} = \frac{z \pm \left(e_3 - e_1\right)}{2\left(V_B+1\right)}, \tag{53}$$

$$z = \sqrt{\left(e_1+e_3\right)^2 - 4e_2^2}. \tag{54}$$

Thus, the necessary values for estimating the Holevo bound in the presence of collective attacks in the trusted receiver noise scenario have been obtained. Further, the model will need to be supplemented taking into account the lack of access of Eve to the noise of Alice in order to consider the full scenario of trusted noise from trusted nodes.

The noise on the Alice side can be composed of the noise from laser power fluctuation and imperfect modulation [13, 20]. Models of such trusted Alice noise for collective attacks are presented in [14, 21–23]. This noise is modeled analogously to the noise of the channel and the detection module using an additional thermal state $\mathrm{Th}_{\mathrm{pr}}$ with variance

$$W_{\mathrm{pr}} = \frac{\xi_{\mathrm{pr}}}{1 - T_{\mathrm{pr}}} + 1, \tag{55}$$

where T_{pr} is the transmittance coefficient of Alice module.

Then the Alice noise measured by Bob will be $\xi_{\mathrm{pr,\,B}} = T_{\mathrm{ch}} T_{\mathrm{rec}} \xi_{\mathrm{pr}}$. The thermal state $\mathrm{Th}_{\mathrm{pr}}$ interacts with Bob's mode through a beam splitter with a transmittance $T_{\mathrm{pr}} \to 1$, since the initial signal power is assumed already at the output of the Alice module. While the limit $T_{\mathrm{pr}} \to 1$ would result in $W_{\mathrm{pr}} \to \infty$, the noise $(1 - T_{\mathrm{pr}})\, W_{\mathrm{pr}} = \xi_{\mathrm{pr}} + 1 - T_{\mathrm{pr}} \to \xi_{\mathrm{pr}}$ of the mode reflected into the channel will be finite and good certain.

The problem can again be reduced to considering only two modes available to Eve, reducing the eigenvalue problem to a second degree polynomial. This allows one to describe the trusted noise of Alice and Bob using simple analytical expressions.

The overall initial state now includes the thermal state responsible for the Alice's noise

$$\Sigma_{\mathrm{tot},0} = \mathrm{EPR}_{\mathrm{AB}} \oplus \mathrm{Th}_{\mathrm{pr}} \oplus \mathrm{EPR}_{\mathrm{ch}} \oplus \mathrm{Th}_{\mathrm{rec}}. \tag{56}$$

Then one should redesignate the sequence of all beam splitters $\mathrm{BS}_{\mathrm{tot}} = \mathrm{BS}_{\mathrm{rec}} \mathrm{BS}_{\mathrm{ch}} \mathrm{BS}_{\mathrm{pr}}$. Then the symplectic transformation, analogous to Eq. (37), will change the block of the covariance matrix related to the eavesdropper as

$$\Sigma_{\mathrm{E}} = \begin{pmatrix} \left((1 - T_{\mathrm{ch}})\,(V + \xi_{\mathrm{pr}}) + T_{\mathrm{ch}} W_{\mathrm{ch}}\right) \mathbf{1}_2 & \sqrt{T_{\mathrm{ch}}} \sqrt{W_{\mathrm{ch}}^2 - 1}\, \sigma_z \\ \sqrt{T_{\mathrm{ch}}} \sqrt{W_{\mathrm{ch}}^2 - 1}\, \sigma_z & W_{\mathrm{ch}} \mathbf{1}_2 \end{pmatrix}. \tag{57}$$

Obviously, the matrices from Eqs. (43) and (57) coincide up to the replacement $V \to V + \xi_{\mathrm{pr}}$. The symplectic eigenvalues v_1 and v_2 (required for calculating S_{E}) are again obtained by Eq. (33). To calculate v_3 and v_4 for $S_{\mathrm{E|B}}$, $\Sigma_{\mathrm{tot|B}}$ must be rearranged according to the modified shared state structure.

Thus, after substitution $T_{\mathrm{pr}} = 1$ and with the accuracy of replacement $V \to V + \xi_{\mathrm{pr}}$, Eve's covariance matrix after heterodyne detection by Bob has the form in accordance with Eq. (49). The symplectic eigenvalues v_3 and v_4 are again obtained by Eqs. (50)–(52).

The advantage of this model is that as equipment losses increase, the Holevo bound decreases faster than mutual information [14].

5. Gaussian quantum channel modeling

The Gaussian quantum channel, as has already been mentioned in this paper, is characterized by two parameters: the transmittance and excess noise. Often CV-QKD papers do not provide clarifications on the components of these characteristics [16, 24, 25]: an analytical assessment has been carried out only for some components.

Modeling the parameters of the Gaussian channel is necessary to obtain the value of the signal-to-noise ratio, which will be maintained at a given distance.

As has already been demonstrated in the previous section, the transmittance is composite, which is why it cannot be estimated in the aggregate, which, for example, was done in [24, 26]. This assumption significantly improves the performance and the amount of allowable losses in the stability analysis but remains incorrect.

So, given that the quantum channel is an optical fiber channel, the transmittance can be estimated in accordance with the well-known expression [27]:

$$T_{\mathrm{ch}} = 10^{-\zeta L/10}, \tag{58}$$

where ζ is the fiber attenuation in dB/km.

The coefficient T_{det} can be obtained from the equipment loss and the detector efficiency as:

$$T_{\mathrm{det}} = \eta_{\mathrm{det}} 10^{-\mathrm{losses}/10}, \tag{59}$$

where losses is the cumulative losses on Alice's equipment.

Here, it should be clarified that T_{det} is the transmittance in the signal arm, T'_{det} is a transmittance in the LO arm. The latter will be necessary for estimating the excess noise. Both coefficients are calculated using Eq. (59) taking into account the fact that losses in both arms are different. For example, the power of LO is expressed as

$$P_{\mathrm{LO}} = T'_{\mathrm{det}} P_{\mathrm{LO,\,A}}, \tag{60}$$

where $P_{\mathrm{LO,\,A}}$ is the power of LO at the output of Alice.

The cumulative losses on the equipment in the Bob module are presented in Table 1.

TABLE 1. Cumulative losses in the signal arm and in the arm of LO obtained from [28–35]

Arm	Name of the optical component	Insertion loss, dB
Signal	FC/APC Connectors	3
	CWDM-filter	0.6
	Polarization controller	0.05
	Polarizing beam splitter	0.6
	90-degree hybrid	3
	All components	7,25
LO	FC/APC Connectors	3,6
	CWDM-filter	0.6
	Polarization controller	0.05
	Polarizing beam splitter	0.6
	Beam splitter 10/90 6	0.85
	90-degree hybrid	3
	All components	8.7

In many theoretical works, the excess noise values are approximated and fixed [14, 25, 36–38]. This is motivated by the fact that in real CV-QKD systems, the excess noise, as well as the transmittance, is estimated from experimental data on the variances of quadrature operators. As far as strictly theoretical works are concerned, the substitution is necessary only for illustrative purposes. However, for a theoretical performance evaluation of the considered CV-QKD system, it is necessary to take into account various noise sources, which will be further carried out in accordance with work [13].

Like the transmittance, excess noise is compound. In this case, the excess noise components are:

- Alice module noises:
  - laser power fluctuations noise;
  - DAC noise;
- channel noises:
  - phase noise;
- Bob module noises:
  - common-mode rejection ratio (CMRR) noise;
  - internal noise of the balanced detector;
  - ADC noise.

Laser power fluctuations noise contains two components, signal and LO ones

$$\xi_{\mathrm{RIN,\,sig}} = V_{\mathrm{A}}\sqrt{\mathrm{RIN}_{\mathrm{sig}} B_{\mathrm{sig}}}, \tag{61}$$

$$\xi_{\mathrm{RIN,\,LO}} = \frac{1}{4}\mathrm{RIN}_{\mathrm{LO}} B_{\mathrm{LO}} V, \tag{62}$$

$$\xi_{\mathrm{RIN}} = \xi_{\mathrm{RIN,\,LO}} + \xi_{\mathrm{RIN,\,sig}}, \tag{63}$$

where $\mathrm{RIN}_{\mathrm{sig}}$ is the relative intensity noise (RIN) of signal, $\mathrm{RIN}_{\mathrm{LO}}$ is the relative intensity noise of LO, B_{sig} is a signal spectrum width, and B_{LO} is the LO spectrum width.

It is important to note that due to the fact that both the signal and LO emit from the same laser, the spectral width and the relative intensity noise for them will be the same [13], i.e. $B_{\mathrm{sig}} = B_{\mathrm{LO}} \equiv B$, $\mathrm{RIN}_{\mathrm{sig}} = \mathrm{RIN}_{\mathrm{LO}} \equiv \mathrm{RIN}$.

The excess noise caused by noise from the modulating voltage side is estimated by the inequality [13]

$$\xi_{\mathrm{DAC}} \leq V_{\mathrm{A}} \left(\pi\alpha \frac{\sqrt{V_{\mathrm{q}}}}{V_\pi} + \frac{1}{2}\pi^2\alpha^2 \frac{V_{\mathrm{q}}}{V_\pi^2} \right)^2, \tag{64}$$

$$V_{\mathrm{q}} = \mathrm{LSB}^2/12 = V_{\mathrm{FS}}^2/(12 \cdot 2^{2N_{\mathrm{res}}(f_{\mathrm{rep}})}). \tag{65}$$

where V_π is the voltage required to reverse the phase by π, α is the DAC gain coefficient, V_{q} is the converter output voltage variance, LSB is the least significant bit, V_{FS} is the full-scale voltage range of the converter, and N_{res} is the DAC resolution.

Coherent quantum signal detection requires a well calibrated phase and frequency relationship between the signal and LO. In addition, the signal initially carries a certain level of phase noise. This phase noise, as well as relative phase shifts,

can be compensated with a strong reference sent by Alice [39–42]. The reference (or pilot) signal carries well-known phase with a fixed phase relation to the original signal pulse. Bob performs heterodyne detection of the reference signal by measuring its quadratures q and p. It can determine the deviation from a fixed and time-constant reference phase. Any of such measured phase shift is used to appropriately correct the measured phase of the quantum signal. The remaining phase noise is then expressed as [13]

$$\xi_{\mathrm{PR}} = \frac{1}{2} V_{\mathrm{A}} \frac{V_{\mathrm{pt}}}{N_{\mathrm{pt}} \langle N_{\mathrm{pt}} \rangle}, \tag{66}$$

where V_{pt} is the variance of the quadrature operator of the reference signal, N_{pt} is the number of the reference signals, $\langle N_{\mathrm{pt}} \rangle$ is the average number of photons in the reference pulse.

It should be noted that in the presented paper, it is assumed that for each signal message there is a reference signal, i.e. the number of reference signals is half of the total number of messages.

It is convenient to express the internal noise of the balanced detector in terms of a characteristic called clearance C, which is defined as the ratio of the total experimental variance of the zero power signal (dispersion shot noise $V_0(\hat{q})$ and electronic noise of dispersion $V_{\mathrm{det}}(\hat{q})$) and variance $V_{\mathrm{det}}(\hat{q})$ caused only by detector electronic noise:

$$C = \frac{V_0(\hat{q}) + V_{\mathrm{det}}(\hat{q})}{V_{\mathrm{det}}(\hat{q})}. \tag{67}$$

The shot noise variance depends linearly on the power of LO, which, however, is limited by the saturation limit of the detector's PIN diodes. Experimentally, the numerator of Eq. (67) can be determined by measuring the quadrature variance of LO when it is mixed with the vacuum inlet. The denominator is the remaining quadrature variance after LO is disconnected from the detector. In SNU by definition $V_0(\hat{q}) = 1$, and the equation becomes as follows

$$C = \frac{1 + V_{\mathrm{det}}(\hat{q})}{V_{\mathrm{det}}(\hat{q})} = \frac{1 + \xi_{\mathrm{det}}}{\xi_{\mathrm{det}}}. \tag{68}$$

Thus, the noise of the balanced detector relative to the clearance, taking into account one/two detectors in homo-/heterodyne detection, respectively, is the following one

$$\xi_{\mathrm{det}} = \mu \frac{1}{C - 1}. \tag{69}$$

An experimental evaluation of ξ_{det} was carried out for the General Photonics OEM Balanced Detector (BPD-003) with the operating frequency band of 200 MHz (see Fig. 2). The choice of the detector was based on the following parameters for the optimal signal-to-noise ratio:

- low noise equivalent power — indicates the possibility of detecting signals with a power comparable to that of shot noise;
- high gain coefficient — allows one to detect low power signals with high attenuation of LO;
- high CMRR — shows the gain quality;
- a wide operating frequency band — allows one to increase the frequency of sending states, which, in accordance with the current technical level, should be about MHz [16, 24, 26]. The established relationship between the excess noise of the detector and its operating frequency band is linear [13], so a too large range can lead to a high level of the internal detector noise.

The dependence of the excess noise of the detector and, as a result, the signal-to-noise ratio on the operating frequency band does not have a minimum due to linearity, however, as can be seen in Fig. 2, the obtained noise level in the considered detector is quite low and corresponds to the level established by [13,24]. So, for example, with the total loss of 13.7 dB (5 dB in the channel and 8.7 dB in the LO arm), $\xi_{\mathrm{det}} = 0.093$ is observed in [13] at operating frequency band of the detector is 250 MHz. In [24], one obtains $\xi_{\mathrm{det}} \sim 10^{-1}$, based on the given data.

According to the obtained dependence of the excess noise of the balanced detector on the input power of LO, one can observe an increase in the contribution of the noise with a decrease in its values. In practice, a decrease in power is associated with an increase in losses. The resulting dependence will be used later in the overall assessment of the total excess noise. The experimental background of the obtained formula is related to the fact that the proposed models do not take into account the full composition of the balanced detector.

A realistic differential amplifier will amplify not only the difference current with a coefficient g, but also to a small extent with a coefficient g_{CM} their average value of the input photocurrents in the subtractive circuit. As a characteristic for estimating such amplification, CMRR [43] is used:

$$\mathrm{CMRR} = \left| \frac{g}{g_{\mathrm{CM}}} \right|. \tag{70}$$

Noise dependent on CMRR is calculated as [13]:

$$\xi_{\mathrm{CMRR}} = \frac{\mu}{4\mathrm{CMRR}^2} \left(\frac{h f V_{\mathrm{A}}^2}{4\tau P_{\mathrm{LO}}} \mathrm{RIN}_{\mathrm{sig}} B_{\mathrm{sig}} + \frac{\tau}{hf} P_{\mathrm{LO}} \mathrm{RIN}_{\mathrm{LO}} B_{\mathrm{LO}} \right), \tag{71}$$

where P_{LO} is a LO power, τ is the pulse duration, f is the optical frequency and h is Planck's constant.

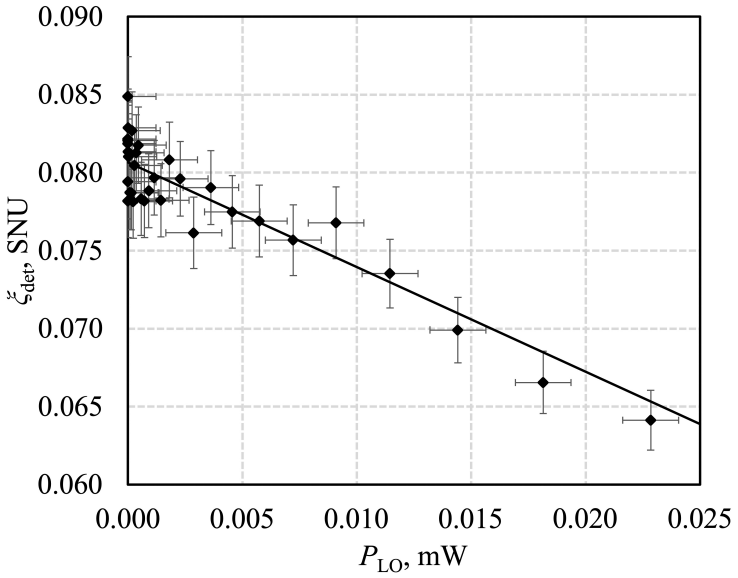

FIG. 2. Dependence of the excess noise of the balanced detector on the input power of LO for General Photonics OEM Balanced Detector (BPD-003).

The incoming signal pulse will be received and amplified by Bob's balanced detector, where the output voltage will be proportional to the measured quadrature. However, if the output voltage is quantized by DAC, it will introduce additional error into the measured signal, thereby contributing to excess noise as [13]:

$$\xi_{\text{ADC}} = \mu \frac{\tau V_{\text{q}}}{hf\ \text{g}^2 \rho^2 P_{\text{LO}}}, \tag{72}$$

where g is the gain coefficient of the electrical circuit of the balanced detector and ρ is the photodiode responsivity.

It should be noted that in Eqs. (64) and (72) the output voltage variance of DAC and ADC are equal, because they are selected with the same scope and resolution.

The calculation of the components of the total excess noise was carried out in accordance with the parameters specified in Table 2. The substantiation of the variance of the quadrature operator is given below in Sec. 6.1. It is important that in the considered case of transmitted LO (see Fig. 1), the power of the LO, as well as the signal power, depends significantly on the losses on equipment and in the channel, which must be taken into account in assessing the excess noise related to the receiver.

6. Evaluation and monitoring of experimental parameters

This subsection describes the procedure for assessing, optimizing and monitoring the key parameters of the CV-QKD. Since the selection of parameters directly affects the secure key generation rate, it is necessary to introduce a boundary with respect to which the calculation will be carried out.

In the general case, the secure key generation rate K is determined by

$$K = f_{\text{sym}} \cdot r, \tag{73}$$

where f_{sym} is the repetition rate and r is the secure key fraction.

The asymptotic secure key generation rate in terms of a message with ideal post-processing for the CV-QKD system in the case of collective attacks is given by the Devetak-Winter bound [45] as

$$r_{\text{coll}}^{\text{asympt}} \geqslant I_{\text{AB}} - \chi. \tag{74}$$

Given the non-ideal reverse reconciliation, the bound can be refined as

$$r_{\text{coll}}^{\text{asympt}} \geqslant (1 - \text{FER})\,(\beta I_{\text{AB}} - \chi_{\text{EB}})\,, \tag{75}$$

where $\text{FER} \in [0,\ 1]$ is the frame error rate (FER).

The quantities I_{AB} and χ_{EB} are respectively obtained by Eqs. (24) and (29). The dependence of these quantities on losses in the quantum channel is shown in Fig. 3.

It can be seen that the Holevo bound does not exceed the mutual information at large distances, thereby keeping the secure key generation rate positive (see Fig. 4). Such an assessment poorly reflects reality, because with an infinite number of messages, and, hence, with an infinite sample for estimating the parameters and an infinite number of reference signals, the excess noise in the channel is very small. At the same time, the excess noise and losses on the Bob side are still large.

TABLE 2. Parameters used in modeling excess noise obtained from Refs. [13,44]

Parameter	Description	Value	Units
V_{A}	Alice's modulation variance	6.77	SNU
RIN	RIN	$10^{-14.5}$	Hz^{-1}
B	laser spectrum width	10^4	Hz
V_π	voltage required to reverse the phase by π	5	V
α	DAC gain	8	a.u.
V_{q}	variance of output voltage of converter	$1.94{\cdot}10^{-11}$	V
V_{FS}	full-scale voltage range of DAC	1	V
N_{res}	DAC resolution	16	bit
V_{pt}	variance of pilot signal	1.2	SNU
n_{pt}	number of pilot signals	$3 \cdot 10^8$	–
$\langle N_{\mathrm{pt}} \rangle$	mean photon number in pilot puls	600	–
μ	homo-/heterodyning parameter	2	–
$P_{\mathrm{LO},\,A}$	Alice's output LO power	$2{\cdot}10^{-3}$	W
T_{det}	transmittance of signal arm	$10^{-0,745}$	a.u.
T'_{det}	transmittance of LO arm	$10^{-0,89}$	a.u.
τ	pulse duration	$3{\cdot}10^{-9}$	s
f	optical frequency	$1.934 \cdot 10^{14}$	Hz
h	Planck's constant	$6.63{\cdot}10^{-34}$	J·s
g	balanced detector's gain	10^5	V/A
ρ	photodiode responsivity	0.85	A/W
CMRR	CMRR	30	dB

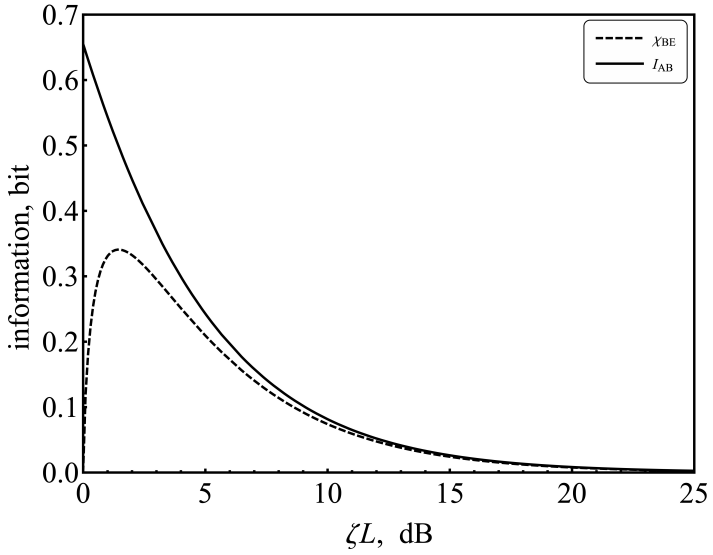

FIG. 3. Mutual information I_{AB} and the Holevo bound χ_{BE} versus losses in the quantum channel.

Limitations on the quantum channel length, as, for example, in [14], are due to the fact that the excess noise model uses not analytical expressions, but approximate fixed values. It can also be noted that when using error correction codes over an alphabet of size q, each symbol of the code corresponds to $\log_2 q$ bits, and for a given code rate R, which is selected based on the channel parameters, one can write [13]:

$$R \log_2 q = \beta I_{\mathrm{AB}}. \tag{76}$$

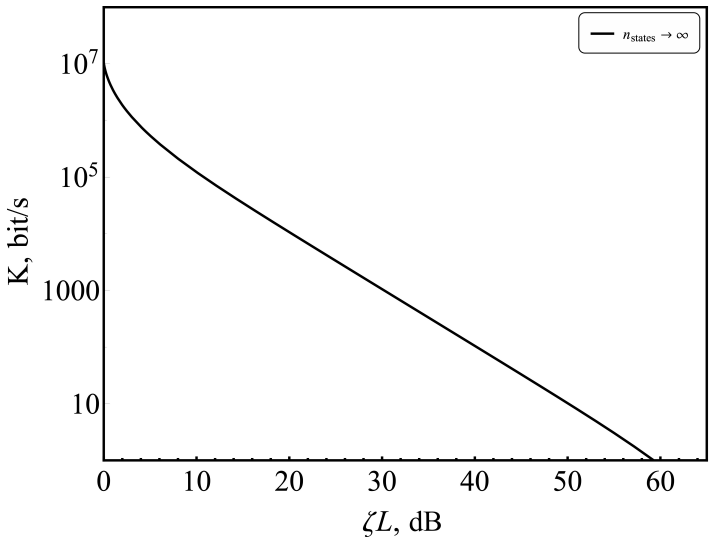

FIG. 4. Dependence of the secure key generation rate in the asymptotic limit on losses in the quantum channel considering the presence of collective attacks.

6.1. Mean photon number optimization

Obviously, an increase in the variance of Alice's quadrature operator V_{A}, which specifies the average number of photons over an ensemble of states (see Eq. (12)), will lead to a proportional increase in the signal-to-noise ratio (see Eq. (21)). That is, an increase in the average number of photons in the signal will give better discrimination of the Gaussian states up to the limits provided by the detector. However, it must be taken into account that in this case, Eve will also receive more information. In this regard, it is necessary to estimate the value of V_{A} by maximizing the value of the secure key fraction r at the target distance.

Thus, with a target loss in the quantum channel of 5 dB and the efficiency of the reconciliation procedure $\beta = 0.95$, the optimal value V_{A} is 6.77 SNU, which is obtained by maximizing the adjusted value of r from Eq. (99). It is important to note that this parameter is significantly affected by the total number of states n_{states}, which, in turn, determines the limit for the number of reference signals.

6.2. Parameter estimation

The Bob measurement data does not initially correspond to the Gaussian quantum information terminology. For this reason, it is necessary to introduce a conversion coefficient ϕ, expressed in V^2/SNU, which converts the original data to SNU. To keep track of possible changes to the calibration parameters, this procedure should be repeated during the key exchange step. Instead of the variance of the quadrature operator, Bob measures the voltage variance (see Eq. (22))

$$V(U) = \phi V\left(\hat{q}_{\mathrm{B}}\right). \tag{77}$$

Alice and Bob randomly jointly select n_{pe} from n_{states} distributed signals and publicly disclose the corresponding μn_{pe} value pairs. Under the collective Gaussian attack assumption, these pairs are independent and equally distributed Gaussian variables. In accordance with the maximum likelihood method, the following estimate can be obtained from the sample

$$V(U) = \langle U^2 \rangle - \langle U \rangle^2 = \frac{1}{\mu n_{\mathrm{pe}}} \sum_{i=1}^{\mu n_{\mathrm{pe}}} U_i^2 - \left(\frac{1}{\mu n_{\mathrm{pe}}} \sum_{i=1}^{\mu n_{\mathrm{pe}}} U_i \right)^2, \tag{78}$$

where U_i is a measured voltage value.

Approximately the parameter ϕ can be estimated as

$$\phi \approx P_{\mathrm{LO}} \rho^2 g^2 B_{\mathrm{BD}} h f, \tag{79}$$

where B_{BD} is an operating frequency of the balanced detector.

However, the coefficient ϕ must be determined experimentally more precisely. To do this, Bob disables the signal input ($TV_{\mathrm{A}} = \xi_{\mathrm{ch}} = 0$) and, instead, measures the quadratures of the vacuum state. Then, the variance of the Bob quadrature operator is as follows

$$V(\hat{q}_B) = 1 + \frac{\xi_{\mathrm{rec}}}{\mu}, \tag{80}$$

$$V(U) = \phi + \phi\frac{\xi_{\mathrm{rec}}}{\mu} \equiv \phi + N_{\mathrm{rec}}. \tag{81}$$

It should be noted that ϕ is linearly directly proportional to the LO power, while the detector noise is inversely proportional, as shown in Eq. (72) and as can be seen from Fig. 2 (the analytical formula for the detector noise is presented in [13]). Therefore, the product of two is constant with respect to P_{LO}

$$\phi \propto P_{\mathrm{LO}}, \tag{82}$$

$$\xi_{\mathrm{rec}} \propto \frac{1}{P_{\mathrm{LO}}}, \tag{83}$$

$$\frac{\partial N_{\mathrm{rec}}}{\partial P_{\mathrm{LO}}} = \frac{\partial(\phi\xi_{\mathrm{rec}})}{\partial P_{\mathrm{LO}}} = 0. \tag{84}$$

Thus, in the case of $P_{\mathrm{LO}} = 0$, the coefficient ϕ will become zero, but N_{rec} will remain unchanged, since it does not depend on the LO power. Therefore, when not only the signal but also the LO input are disabled, Eq. (81) becomes

$$V(U) = N_{\mathrm{rec}}. \tag{85}$$

Now, for a given voltage dispersion $V(U)$, obtained with a given non-zero LO power, we can write the final formula for ϕ:

$$\phi = V(U) - N_{\mathrm{rec}}. \tag{86}$$

The quantity ϕ is the quadratic measure of the voltage of exactly one SNU, still assuming that only the vacuum input is measured, i.e. $TV_{\mathrm{A}} = 0$. For subsequent parameter estimation, Bob divides his measured voltages representing q and p by $\sqrt{\phi}$ and any calculated voltage variance by ϕ, so that all his data will be represented in SNU system.

6.3. Confidence intervals

Depending on the chosen security model (trusted or untrusted noise), when estimating the parameters, it is necessary to set certain confidence intervals. Since the noise of the equipment is assumed to be trusted in the model under consideration, the total transmittance for Bob (in Eq. (60)) must be estimated in terms of the best case, while the transmittance and the excess noise of the channel — in terms of the worst.

As have already been mentioned, Alice and Bob have a sample of μn_{pe} independent and equally distributed pairs $\{x_i,\, y_i\}_{i=1}^{\mu n_{\mathrm{pe}}}$, where x_i and y_i are Gaussian variables, which are related by the ratio of the channel with additive white Gaussian noise:

$$y = \sqrt{T}x + \mathcal{N}(0,\, \xi). \tag{87}$$

For pairs of values, estimates of the transmittance and the excess noise are determined:

$$\hat{T} = \frac{\sum_{i=1}^{\mu n_{\mathrm{pe}}} x_i y_i}{\sum_{i=1}^{\mu n_{\mathrm{pe}}} x_i^2}, \tag{88}$$

$$\hat{\xi} = \frac{1}{\mu n_{\mathrm{pe}}} \sum_{i=1}^{\mu n_{\mathrm{pe}}} (y_i - \hat{T}x_i). \tag{89}$$

It should be taken into account that corrections must be introduced, depending on the belonging of the noise for a correct assessment of the mutual information and the Holevo bound. At the same time, the channel model with additive noise is preserved. The corrections themselves are expressed as [38]:

$$\mathrm{Corr}_{\xi,\,j} = w\sqrt{\mathrm{Var}(\hat{T}_j^{1/2})} = w\frac{\xi_j + \mu}{\sqrt{2\mu n_{\mathrm{pe}}}}, \tag{90}$$

$$\mathrm{Corr}_{T,\,j} = w\sqrt{\mathrm{Var}(\hat{\xi}_j)} = 2w\sqrt{\frac{2T_j^2 + T_j(\xi_j + \mu)/V_{\mathrm{A}}}{\mu n_{\mathrm{pe}}}}, \tag{91}$$

where w is the confidence factor, m is the number of signals for parameter estimation and j is the parameter that defines belonging to Alice/channel/Bob.

Such approximations are correct up to $O(n_{\mathrm{pe}}^{-1})$. The expression $\mathrm{Var}(\hat{T}^{1/2})$ can be further approximated for large n_{pe}, so a more optimistic estimate can be written

$$\mathrm{Corr}_{T,\,j} = 2w\xi_j/V_{\mathrm{A}}\sqrt{T_j/(\mu n_{\mathrm{pe}})}. \tag{92}$$

However, the estimate from Eq. (91) will be used for performance analysis.

Thus, it is necessary to carry out the replacement as follows

$$T'_{\text{det}} \longrightarrow T'_{\text{det}} + \text{Corr}_{T,\,\text{full}}, \tag{93}$$

$$T_{\text{ch}} \longrightarrow T_{\text{ch}} - \text{Corr}_{T,\,\text{ch}}, \tag{94}$$

$$\xi_{\text{ch}} \longrightarrow \xi_{\text{ch}} + \text{Corr}_{\xi,\,\text{ch}}\,. \tag{95}$$

Each of these estimates limits the corresponding actual value to within the error probability ε_{pe}, if denote

$$w = \frac{\sqrt{2}}{\text{erf}\,(1-2\varepsilon_{\text{pe}})} \approx \sqrt{2\ln(1/\varepsilon_{\text{pe}})}. \tag{96}$$

Approximation in Eq. (96) is allowed for small $\varepsilon_{\text{pe}} \leq 10^{-17}$.

7. Estimating the finite-length secure key generation rate

After parameter estimation, each initial sequence of n_{states} dimensions goes into n symbols to be processed into the final key using error correction and privacy amplification procedures. For each information block, errors are successfully corrected with a probability of $1 - \text{FER}$. The value of this probability depends on the signal-to-noise ratio, the target reconciliation efficiency β, and the ε-criteria correctness ε_{cor}. The latter limits the probability that local bit strings of Alice and Bob are different after error correction and successful execution of the validation procedure.

On average, $n(1-\text{FER})$ signals from the information block remain for the privacy amplification procedure. This final step is implemented with the ε-security parameter ε_{sec}, which limits the trace distance between the final key and the ideal key, which has no correlation with the eavesdropper. In the QKD paradigm, it is necessary to take into account the pessimistic assessment of information distributed among users. In this case, not Shannon entropies, but smoothed Renyi min-entropies are used, which are reduced to the former through the asymptotic equipartition property [46]. The smoothness determines the allowable error fluctuations. In turn, ε-security is technically decomposed as:

$$\varepsilon_{\text{sec}} = \varepsilon_{\text{s}} + \varepsilon_{\text{h}}, \tag{97}$$

where ε_{s} is the min-entropy smoothing parameter and ε_{h} is the parameter that determines the match of hash codes after privacy amplification procedure.

All declared ε-security parameters are set small (for example, $2^{-33} \approx 10^{-10}$) and form a general security criteria

$$\varepsilon = 2(1-\text{FER})\varepsilon_{\text{pe}} + \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}. \tag{98}$$

7.1. Satisfying the composability criteria of CV-QKD protocol in the presence of collective attacks

Taking into account the finiteness of the keys and the requirement that the protocol under consideration be composable in the presence of collective attacks, the boundary from Eq. (75) is refined, and the secure key generation rate in terms of the message is expressed as [7, 8, 37, 38]

$$r_{\text{coll}}^{\text{finite}} \geqslant \frac{n(1-\text{FER})}{n_{\text{states}}}\left(\beta I_{\text{AB}}(w) - \chi_{\text{EB}}(w) - \frac{\Delta_{\text{AEP}}}{\sqrt{n}} + \frac{\Theta}{n}\right), \tag{99}$$

$$\Delta_{\text{AEP}} = 4\log_2(2\sqrt{d}+1)\sqrt{\log_2\left(\frac{18}{(1-\text{FER})^2\varepsilon_{\text{s}}^4}\right)}, \tag{100}$$

$$\Theta = \log_2\left[(1-\text{FER})\left(1-\varepsilon_{\text{s}}^2/3\right)\right] + 2\log_2\sqrt{2}\varepsilon_{\text{h}}, \tag{101}$$

where n is the number of characters left to process the final key, n_{states} is the number of states, Δ_{AEP} is the correction according to asymptotic equipartition property [46], Θ is the correction coefficient that combines hash mismatch accounting after privacy amplification procedure according to Lemma 2 of [47] and a leak on the error correction procedure [37, 38], d is the size of the effective alphabet after the final digitization of the continuous variables of Alice and Bob and ε_j is the security parameter.

To improve performance, Δ_{AEP} can be refined as [38, 48]

$$\Delta_{\text{AEP}} = 4\log_2(\sqrt{d}+2)\sqrt{\log_2\left(\frac{18}{(1-\text{FER})^2\varepsilon_{\text{s}}^4}\right)}. \tag{102}$$

The value of n, in turn, is obtained from n_{states} as follows

$$n = n_{\text{states}} - (n_{\text{pt}} + n_{\text{pe}}), \tag{103}$$

where n_{pt} is the number of reference signals and n_{pe} is the number of signals given for parameter estimation.

7.2. Security of CV-QKD protocol against coherent attacks

So far, the security of the CV-QKD protocol with the Gaussian modulation in the presence of Gaussian collective attacks has been substantiated. The level of security for a protocol with heterodyne detection can be extended to security against coherent attacks using the mathematical apparatus from [49].

Let the protocol $\mathcal{P}$, which uses coherent states as information carriers, be ε-secure with a secure key generation rate of finite length $r_{\text{coll}}^{\text{finite}}$ in the presence of collective Gaussian attacks, and $\mathcal{P}$ can be symmetrized with respect to the representation of the group of unitary matrices in the Fock space. This symmetrization is equivalent to applying an identical random orthogonal matrix to the classical continuous variables [49], which is certainly possible for a protocol that implies heterodyne detection. The symmetrized protocol can be denoted as $\tilde{\mathcal{P}}$.

Then it can be assumed that users jointly perform the so-called energy tests on the sample $n_{\text{et}} = f_{\text{et}} n$ from random inputs for some coefficient $f_{\text{et}} < 1$. In each test, the parties measure the local average of the number of photons, which can be extrapolated from the data, and calculate the average over the n_{et} tests. If these averages exceed the specified thresholds (d_{A} for Alice and d_{B} for Bob), the protocol is aborted. Setting $d_{\text{A}} \geqslant V_{\text{A}}/2 + O(n_{\text{et}})$ guarantees almost successful passing of the test with probability $p_{\text{et}} \approx 1$ in typical scenarios, where the signals are attenuated and the noise is not too high, at large values of n_{et} [37]. Also, for a channel with losses and sufficiently small excess noise, the average number of photons reaches Bob, which is clearly less than in the state prepared by Alice, which means that the successful value for d_{B} can be chosen to be d_{A}, i.e. relies $d_{\text{A}} = d_{\text{B}} \equiv d_{\text{et}}$.

Thus, the parties are moving to the symmetrized $\tilde{\mathcal{P}}$ protocol, which will now use $\tilde{n} = n_{\text{states}} - n_{\text{coh}}$ signals to generate secret quantum keys, where $n_{\text{coh}} \equiv n_{\text{pt}} + n_{\text{pe}} + n_{\text{et}}$.

Moreover, additional privacy amplification is required, reducing the output key string by [37, 38, 49] Φ_n

$$\Phi_n = 2\left[\log_2 \binom{K_n + 4}{4}\right], \tag{104}$$

$$K_n = \max\left\{1, 2\tilde{n} d_{\text{et}} \frac{1 + 2\sqrt{\vartheta} + 2\vartheta}{1 - 2\sqrt{\vartheta / f_{\text{et}}}}\right\}, \tag{105}$$

$$\vartheta = (2\tilde{n})^{-1} \ln(8/\varepsilon). \tag{106}$$

Assuming that the original protocol has ε security criteria against collective Gaussian attacks, otherwise the security criteria for the symmetrized protocol against coherent attacks goes to [49]

$$\varepsilon' = K_n^4 \varepsilon / 50. \tag{107}$$

It should be noted that a very strict limitation on ε-parameters is implied. In particular, this means that ε_{pe} must be sufficiently small (for example, 10^{-43}, as suggested by [25, 37]), and the corresponding coefficient confidence w must be calculated using Eq. (96).

Given the changed length of the input sequence and the change in the security criteria, Eq. (99) is rewritten as

$$r_{\text{coh}}^{\text{finite}} \geqslant \frac{\tilde{n}(1 - \text{FER})}{n_{\text{states}}} \left(\beta I_{\text{AB}}(w) - \chi_{\text{EB}}(w) - \frac{\Delta_{\text{AEP}}}{\sqrt{n}} + \frac{\Theta - \Phi_n}{n}\right). \tag{108}$$

7.3. Analysis of the potential performance of CV-QKD system

The dependence of the finite-length secure key generation rate in the presence of collective and coherent attacks on losses in the quantum channel is shown in Fig. 5. The corresponding parameters are presented in the Tables 2 and 3. A significant contribution to the performance of any system CV-QKD is made by the number of states, while increasing this parameter imposes a limit on the computing resource. In the case under consideration, this value was estimated from the calculation of memory characteristics and information processing speed, i.e. the number of states was chosen as large as possible to fully record information about them in high-speed memory of the type DDR. It is supposed to use the Kria K26 computing module from Xilinx with a memory of 4 GB, of which 2 GB is allocated for data. With further increase in the number of states, information will need to be recorded in a larger, but low-speed memory, using which, the final rate of generation of the secret quantum key will be lower. For this reason, there is a limitation on the amount of recorded information about states in memory caused by the use of high-speed memory.

The marginal losses in the quantum channel in CV-QKD in the presence of collective attacks are 10.2 dB, in the presence of coherent — 7.5 dB.

Ensuring the security of the CV-QKD protocol with Gaussian modulation against coherent attacks, in turn, requires not only a significant limitation on security criteria, but also an increase in the number of messages to maintain the proper performance level.

According to the collective attack security criteria set in p. 7.1 (see also Table 3), the number of states is $6 \cdot 10^8$. Each quantum signal pulse is followed by a reference pulse in such a way that the total number of quantum signal pulses and reference pulses is $6 \cdot 10^8$ for each block. For each quantum message, the random number generator generates 32 bits: 16 bits each to determine the value of each of the quadratures.

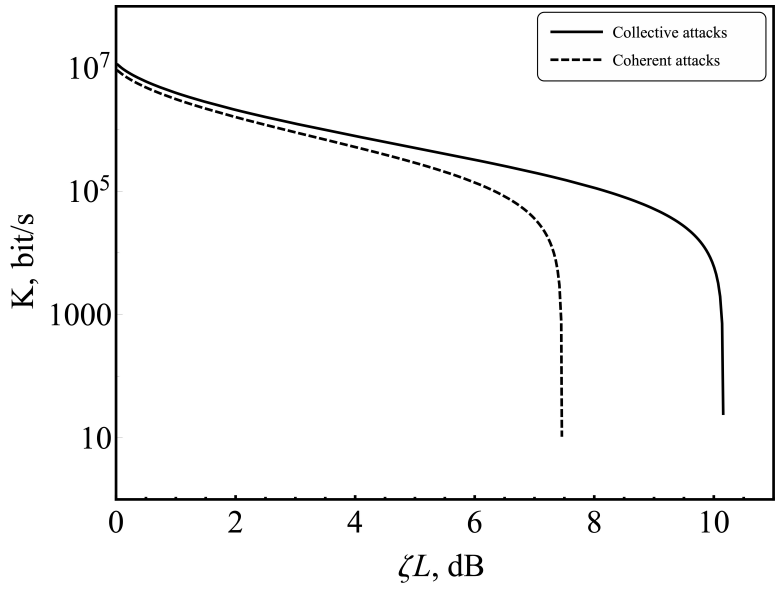

FIG. 5. Dependence of the secure key generation rate of finite length in the presence of collective and coherent attacks on losses in the quantum channel.

TABLE 3. Parameters used to evaluate the performance of the CV-QKD system. Security parameters are selected in accordance with the works [25, 36–38]

Parameter	Description	Value (collective attacks)	Value (coherent attacks)	Units
n_{states}	number of states	$6 \cdot 10^8$	$6 \cdot 10^8$	–
β	reconciliation efficiency	0.95	0.95	a.u.
FER	frame error rate	0.03	0.03	a.u.
d	size of the effective alphabet	10^4	10^4	bit
n_{pe}	number of signals for parameter estimation	$6 \cdot 10^7$	$6 \cdot 10^7$	–
f_{et}	fraction os states for energy tests	0.2	0	a.u.
w	confidence	6.34	14.07	a.u.
ε_{s}	smoothness parameter	10^{-10}	10^{-43}	a.u.
ε_{h}	parameter that determines hash code match	10^{-10}	10^{-43}	a.u.
ε	general security parameter	$5.6 \cdot 10^{-9}$	$1.3 \cdot 10^{-9}$	a.u.

Alice in the process of generating the message writes the package number without taking into account the reference pulses, using 27 bits for this (5 bits are laid down for redundancy to align the word to 4 bytes), as well as a 4-byte number obtained using a software random number generator implemented on the basis of the FPGA Alice module. Bob detects both quadratures of each message received from the channel. Given that half of the states are reference pulses and two quadrature values are recorded for each state, legitimate users within each block write down information about $6 \cdot 10^8$ quantum state quadrature values. During detection, Bob writes the number of the message (which accounts for 4 bytes) and 4 bytes of information about the two registered values of quadratures of quantum messages to high-speed DDR memory, as well as 4 bytes of information about the two registered values of the quadratures of the reference pulses.

Information about the registered reference pulse quadratures is used to compensate for the phase shift of quantum messages as a result of transmission over a quantum channel, after which this information is deleted from memory. Every ten states, Bob randomly selects one to be used for channel characterization (for the parameter estimation procedure). For the remaining messages, insignificant bits are discarded in the part containing information about quadratures, as a result

of which eight bits remain out of 32 bits of information. On average, each package has 5.3 bytes of information. The time taken for detection and storage is 12 seconds.

To evaluate the channel, states are disclosed for which insignificant bits have not been discarded. After that, errors are corrected using multi-level encoding and multi-stage decoding [50–52]. During error correction, three of the four bits are revealed, thereby reducing the bit sequence to a length of $5.4 \cdot 10^8$ bits.

After the error correction is completed, universal hashing is used to exhaustively verify that all Alice and Bob sequences are the same (confirmation procedure). Hashing of the key with corrected errors is performed both in Alice's and Bob's blocks. As a result of hashing, users still have hash codes on their hands. Bob sends the received hash code to Alice. She then compares the values of two hash codes: the one calculated in her block and the one received from Bob. The result of the comparison is then transmitted to him. If the values do not match, then the processing of this sifted key stops without generating a secret key. The key that has not passed the confirmation procedure is erased from memory on both sides.

A 2-universal hash function is used at the privacy amplification step. The input is a key with corrected errors. The corrected key is loaded in blocks. The ratio of the length of the output sequence after privacy amplification procedure to the length of the input sequence is 1:66.

Since the post-processing of the sequence is faster than writing information to memory during detection, these processes can be performed in parallel.

8. Conclusion

In this paper, we have carried out a theoretical analysis of the performance of the realistic CV-QKD system. Our estimates show that performance can be maintained with losses as low as 10 dB in the most common assumption of collective attacks. In the presence of coherent attacks, there is a noticeable drop in allowable losses (down to 7 dB), and at the same time, tougher security criteria must be taken into account, which are still quite difficult to satisfy in practice. Further work will be focused on creating an experimental setup in accordance with what is described in the article and evaluating the performance of a real system.

References

[1] Pirandola S., Andersen U.L., Banchi L., Berta M., Bunandar D., Colbeck R., Englund D., Gehring T., Lupo C., Ottaviani C., Pereira J.L., Razavi M., Shamsul Shaari J., Tomamichel M., Usenko V.C., Vallone G., Villoresi P., and Wallden P., Advances in quantum cryptography. *Advances in Optics and Photonics*, 2020, **12**, P. 1012.

[2] Bennett C.H., Brassard G., Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 2014, **560**(12), P. 7–11.

[3] Bennett C.H., Brassard G., Mermin N.D., Quantum cryptography without Bell's theorem. *Physical Review Letters*, 1992, **68**(2), P. 557–559. .

[4] Ralph T.C., Continuous variable quantum cryptography. *Phys. Rev. A*, 1999, **61**(1), P. 010303.

[5] Cerf N.J., Lévy M., Assche G.V., Quantum distribution of Gaussian keys using squeezed states. *Physical Review A*, 2001, **63**(4), P. 052311.

[6] Grosshans F., Van Assche G., Wenger J., Brouri R., Cerf N.J., Grangier P., Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, **421**(1), P. 238–241.

[7] Leverrier A., Grosshans F., Grangier P., Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 2010, **81**(6), P. 062343.

[8] Leverrier A., Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Physical Review Letters*, 2015, **114**(2), P. 070501.

[9] Ghorai S.,Grangier P.,Diamanti E., and Leverrier A., Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X*, 2019, **9**(6), P. 021059.

[10] Lin J., Upadhyaya T., Lütkenhaus N., Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Phys. Rev. X*, 2019, **9**(12).

[11] Denys A., Brown P., Leverrier A., Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 2021, **5**(9), P. 540.

[12] Usenko V., Filip R., Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense. *Entropy*, 2016, **18**(1), P. 20. .

[13] Laudenbach F., Pacher C., Fung C.-H. F., Poppe A., Peev M., Schrenk B., Hentschel M., Walther P., and Hübel H., Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Advanced Quantum Technologies*, 2018, **1**(8), P. 1800011.

[14] Laudenbach F., Pacher C., Analysis of the Trusted-Device Scenario in Continuous-Variable Quantum Key Distribution. *Advanced Quantum Technologies*, 2019, 2(11), P. 1900055.

[15] Weedbrook C., Lance A.M., Bowen W.P., Symul T., Ralph T.C., Lam P.K., Quantum Cryptography Without Switching. *Physical Review Letters*, 2004, **93**(10), P. 170504.

[16] Huang D., Huang P., Lin D., and Zeng G., Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 2016, **6**(5), P. 19201.

[17] Bennett C.H., Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 1992, **68**(5), P. 3121–3124.

[18] Carter J., Wegman M.N., Universal classes of hash functions. *Journal of Computer and System Sciences*, 1979, **18**(4), P. 143–154.

[19] Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Du M.\ifmmode \checks\else š\fiek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution. *Reviews of Modern Physics*, 2009, **81**(9), P. 1301–1350.

[20] Jouguet P., Kunz-Jacques S., Diamanti E., and Leverrier A., Analysis of imperfections in practical continuous-variable quantum key distribution, *Physical Review A*, 2012, **86**(9), P. 032309.

[21] Filip R., Continuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, 2008, **77**(2), P. 22310.

[22] Usenko V.C., Filip R., Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, 2010, **81**(2), P. 022318.

[23] Jacobsen C., Gehring T., and Andersen U., Continuous Variable Quantum Key Distribution with a Noisy Laser. *Entropy*, 2015, **17**(7), P. 4654–4663.

[24] Zhang Y., Chen Z., Pirandola S., Wang X., Zhou C., Chu B., Zhao Y., Xu B., Yu S., and Guo H., Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, *Physical Review Letters*, 2020, **125**(6), P. 010502.
[25] Hosseinidehaj N., Lance A.M., Symul T., Walk N., and Ralph T.C., Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection. *Physical Review A*, 2020, **101**(5), P. 052335.
[26] Jouguet P., Kunz-Jacques S., Leverrier A., Grangier P., and Diamanti E., Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 2013, **7**(5), P. 378–381.
[27] Agrawal G.P., *Fiber-optic communication systems*, vol. 222. John Wiley & Sons, 2012.
[28] Polarization Insensitive Isolator (ISO) http://www.lightcomm.com/product/view/typeid/235/id/268.html.
[29] Polarization Maintaining Fused Standard Coupler (PMC) http://www.lightcomm.com/home/product/view/typeid/189/id/206.html.
[30] Intensity Modulators https://photonics.ixblue.com/store/lithium-niobate-electro-optic-modulator/intensity-modulators.
[31] Phase Modulators https://photonics.ixblue.com/store/lithium-niobate-electro-optic-modulator/phase-modulators.
[32] Polarization Beam Combiner/Splitter (PBC/PBS) http://www.lightcomm.com/product/view/typeid/190/id/212.html.
[33] 90-Degree Optical Hybrid http://www.optoplex.com/Optical_Hybrid.htm.
[34] Polarization Maintaining Isolator (PMISO) http://www.lightcomm.com/product/view/typeid/190/id/211.html.
[35] HIGH SPEED POLARIZATION CONTROLLER-SCRAMBLER (OEM VERSION) https://www.ozoptics.com/ALLNEW_PDF/DTS0143.pdf.
[36] Hosseinidehaj N., Walk N., and Ralph T.C., Optimal realistic attacks in continuous-variable quantum key distribution. *Physical Review A*, 2019, **99**(5), P. 1–11.
[37] Pirandola S., Limits and security of free-space quantum communications. *Physical Review Research*, 2021, **3**(3), P. 013279.
[38] Pirandola S., Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Physical Review Research*, 2021, **3**(10), P. 043014.
[39] Qi B., Lougovski P., Pooser R., Grice W., and Bobrek M., Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Physical Review X*, 2015, **5**(10), P. 041009.
[40] Soh D.B., Brif C., Coles P.J., Lütkenhaus N., Camacho R.M., Urayama J., and Sarovar M., Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, 2015, **5**(4), P. 1–15.
[41] Kleis S., Rueckmann M., and Schaeffer C.G., Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics Letters*, 2017, **42**(4), P. 1588.
[42] Laudenbach F., Schrenk B., Pacher C., Hentschel M., Fung C.-H.F., Karinou F., Poppe A., Peev M., and Hübel H., Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, 2019, **3**(10), P. 193.
[43] Szynowski J., CMRR analysis of instrumentation amplifiers. *Electronics Letters*, 1983, **19**(14), P. 547.
[44] Tang X., Kumar R., Ren S., Wonfor A., Penty R., and White I., Performance of continuous variable quantum key distribution system at different detector bandwidth. *Optics Communications*, 2020, **471**(9), P. 126034.
[45] Devetak I. and Winter A., Distillation of secret key and entanglement from quantum states, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2005, **461**(1), P. 207–235.
[46] Tomamichel M., Colbeck R., and Renner R., A fully quantum asymptotic equipartition property. *IEEE Transactions on information theory*, 2009, **55**(12), P. 5840–5847.
[47] Tomamichel M., Schaffner C., Smith A., and Renner R., Leftover Hashing Against Quantum Side Information. *IEEE Transactions on Information Theory*, 2011, **57**(8), P. 5524–5535.
[48] Tomamichel M., *Quantum Information Processing with Finite Resources*. Cham: Springer International Publishing, 2016.
[49] Leverrier A., Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Physical Review Letters*, 2017, **118**(5), P. 200501.
[50] Van Assche G., Cardinal J., and Cerf N., Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE Transactions on Information Theory*, 2004, **50**(2), P. 394–400.
[51] Mani H., *Error Reconciliation Protocols for Continuous-Variable Quantum Key Distribution*. PhD thesis, Technical University of Denmark, 2021.
[52] Wen X., Li Q., Mao H., Wen X., and Chen N., Rotation Based Slice Error Correction Protocol for Continuous-variable Quantum Key Distribution and its Implementation with Polar Codes. *arXiv preprint arXiv:2106.06206*, 2021, **6**, P. 1–17.

Submitted 30 May 2022; revised 16 June 2022; accepted 17 June 2022

Information about the authors:

Roman K. Goncharov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; rkgoncharov@itmo.ru

Alexei D. Kiselev – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; alexei.d.kiselev@gmail.com

Eduard O. Samsonov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; eosamsonov@itmo.ru

Vladimir I. Egorov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; viegorov@itmo.ru

Conflict of interest: the authors declare no conflict of interest.