DOI: 10.17725/j.rensit.2024.16.255

Key features of continuous-variable quantum key distribution protocols

Evgenii V. Burlakov, Alexander V. Korobov

Moscow Technical University of Communications and Informatics, https://mtuci.ru/

Moscow 111024, Russian Federation

E-mail: e.v.burlakov@mtuci.ru, a.v.korobov@mtuci.ru

Received November 08, 2023, peer-reviewed November 15, 2023, accepted November 22, 2023, published April 25, 2024

Abstract: **The key features of continuous variables quantum key distribution protocols are considered in the paper. The motivation for studying and developing methods of quantum cryptography is substantiated. The main aspects inherent to continuous-variable protocols are highlighted, and they are classified based on various characteristics, peculiarities, and implementation variants. A detailed examination of a protocol example with discrete modulation and signal registration through balanced homodyne detection is provided. A classification of attacks on the quantum protocol is presented. A general overview of post-processing methods is given. The role of noise is indicated, and approaches to assessing the level of security applicable to continuous-variable protocols are discussed. In conclusion, the main conclusions regarding the current status of this problem are presented, and aspects requiring further study are identified.**

Keywords: **quantum information, quantum cryptography, quantum key distribution, continuous variables, homodyne detection**

PACS: 03.67.Dd, 42.50.Dv, 89.70.+c

For citation: Evgenii V. Burlakov, Alexander V. Korobov. Key features of continuous-variable quantum key distribution protocols. *RENSIT: Radioelectronics. Nanosystems. Information Technologies*, 2024, 16(2):255-266e. DOI: 10.17725/j.rensit.2024.16.255.

Contents

1. INTRODUCTION

The second quantum revolution is believed by many scientists to be underway, characterized by a rapid advancement of quantum technologies [1, 2]. Indeed, many of the fundamental properties of quantum mechanics, such as quantum entanglement [3], teleportation [4] and the no-cloning theorem [5], have been experimentally verified and form the basis of ideas that can be used for practical purposes. At the same time, as we live in the era of informational technology, the role of information in our lives has become more significant, manifesting in various ways. The fusion of quantum technology and informatics leads to the emergence of a new field known as quantum informatics [6, 7]. One of the

branches of quantum informatics is quantum cryptography [8-11]. Throughout human history, we have sought confidential ways of exchanging information, and the relevance of this problem increases over time. Nowadays, the functioning of the military, government, and banking sectors is inconceivable without cryptography.

It is known that to achieve theoretically secure communication, it is sufficient to use the method of a one-time pad (Vernam cipher) [12]. This method partially reduces the problem of exchanging secret messages to the problem of distributing a secret key that encodes the messages transmitted between two parties. Currently, classical encryption algorithms are most commonly used for key distribution [13]. The reliability of most of these algorithms is not mathematically proven and is based on the fact that, to date, there is no classical efficient algorithm for factoring large numbers [14]. Therefore, in the future, after the possible creation of efficient algorithms for factoring large numbers or sufficiently powerful quantum computers [15], modern classical key distribution methods will have to be abandoned.

Quantum cryptography aims to address the challenge of distributing a secret key by leveraging the principles of quantum mechanics, which ensures that the secrecy of the key is protected by the fundamental laws of nature. The BB-84 quantum key distribution protocol [16] is based on the quantum-mechanical no-cloning theorem [5]. The protocol is designed in such a way that any attempt by an eavesdropper (Eve) to intercept information about the key can always be detected by specific coordinated actions of the users distributing the key (Alice and Bob). BB-84 was the first historically significant quantum key distribution protocol and still remains one of the most reliable protocols. However, research in this field is constantly conducted, and other quantum cryptography protocols have since been proposed, such as E-91 [17], B-92 [18], GG-02 [19], and Lo-05 [20], each with their unique features. Special emphasis should be given to the continuous-variable protocols (CV QKD) [19, 21]. This work aims to outline the findings of scientific research on the crucial aspects of continuous variable quantum key distribution protocols, establish the necessity for additional exploration and advancement in this area, and identify the aspects that demand further investigation.

2. FEATURES AND VARIANTS OF CV QKD PROTOCOLS

As the 2000s commenced, it became clear that for the purposes of quantum cryptography, methods where information about the secret key is encoded in the value of the optical field complex amplitude (CV QKD) could be used [19, 21-23]. This quantity is a continuous quantum variable, meaning that when measured, it gives a value that continuously changes within a certain range of values. This is the difference between a continuous quantum variable and a qubit [6], whose measurement results form a discrete spectrum. The no-cloning theorem of unknown quantum states is valid for continuous variables as well as for discrete variables, which is also a factor underlying the security of such protocols [24].

Continuous variable protocols are comparatively less frequently implemented in experiments when compared to discrete variable QKD protocols. The reason for this is the difficulties in proving their security [24], especially for protocols with so-called non-Gaussian modulation, as well as the sensitivity of protocol implementations to various types of noise [25]. However, CV QKD has several attractive features that are not present in protocols based on discrete

variables. Continuous variable quantum key distribution employs multiphoton laser pulses (approximately 250 photons per pulse) [21], which enhances the speed of secret key generation. Additionally, there is no need for a single-photon source [26-28] or detector [29], which are commercially expensive and still imperfect for QKD purposes.

More and more researchers are directing their attention to the protocols belonging to the CV QKD category. CV QKD protocols have already been implemented in optical fibers [30], free space [31], and single-pass [19] and two-pass schemes [32]. Variations of CV QKD have also been implemented with a local oscillator (reference signal) available only on the receiver's side (local-local oscillator) [33], which significantly improves the protocol's reliability. Depending on the modulation type, CV QKD protocols can be divided into protocols with Gaussian [19] and non-Gaussian [34] modulation. Protocols with Gaussian modulation are more complex to implement, but their security against coherent attacks (general attacks) is justified [35]. Protocols with non-Gaussian (most often discrete) modulation often have simpler technical implementations and post-processing algorithms, but their security justifications are more challenging. Coherent optical field states are commonly used as signal states, but squeezed [36] and thermal states [37] can also be used. A distinctive part of CV QKD protocols is the balanced homodyne detection procedure [38]. There are variations of CV QKD in which this procedure is replaced by heterodyne detection [38]. This not only improves the generation speed of the secret key but also enables the omission of a requirement for a source of random [39, 40] or pseudo-random numbers on Bob's side.

3. DESCRIPTION OF THE BALANCED HOMODYNE DETECTION METHOD

As noted above, performing balanced homodyne detection is an important and specific part of CV QKD protocols, so it makes sense to describe this procedure individually. The laser field with high precision can be described by a coherent state $|\alpha\rangle$, where $a = A\exp(i\varphi) = g + ip$ is a complex parameter encoding the amplitude and the constant (initial) phase component of the optical signal. These characteristics can be unambiguously converted into signal quadrature components: the "coordinate" q and the "momentum" p [22]. The reason for these quantities being given their names is due to the fact that, in the quantum description of the electromagnetic field, they have the same (up to a constant) commutation relationship as the coordinate and momentum operators of a quantum-mechanical particle: $[\hat{q}, \hat{p}] = i$.. Consequently, this implies that they are subject to the Heisenberg uncertainty principle, i.e. there is a definite relationship between the variances of these quantities (**Fig. 1**). The "coordinate" q and the "momentum" p of the signal state can be experimentally measured as follows [22]: the signal state is interfered with a local oscillator (a homodyne, reference optical field) of the same frequency on a symmetric beam splitter. Then, each of the output beams of the beam splitter is directed onto a photodiode of the homodyne detector (**Fig. 2**). It can be shown that, depending on the phase difference θ, between the signal and the homodyne, the resulting differential photocurrent I is proportional to either the "coordinate" q, or the "momentum" p, or their combination.

$$I \sim q\cos\theta + p\sin\theta. \quad (1)$$

The detector amplifies the photocurrent I and converts it into a voltage output, which is then sent to an oscilloscope for transmission.

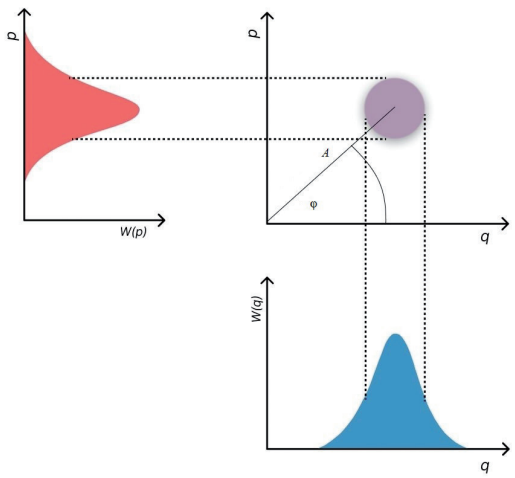

Fig. 1. *A visual representation of a signal coherent state* $|\alpha\rangle$ *omplex amplitude . The end of the amplitude vector is surrounded by a "uncertainty circle" reflecting the presence of inherent quantum noise that cannot be eliminated.*

The data from the oscilloscope is processed to recover information about the quadrature components. Thus, by adjusting the phase difference θ between the signal and the local oscillator, Bob effectively selects which quadrature he will measure. The explained detection method is utilized for not just CV QKD, but also for a procedure known as quantum tomography [41], which involves the reconstruction of a quantum state from homodyne detection data. For example, the quadrature components are arguments of the Wigner function $W(q,p)$ [42-45], an important object in quantum optics that represents a quasi-probability distribution function.

4. DESCRIPTION OF THE CV QKD PROTOCOL USING DISCRETE MODULATION

Below a protocol variant for CV QKD with discrete modulation using coherent states and homodyne detection is presented. Such a protocol typically has a simpler technical implementation compared to protocols

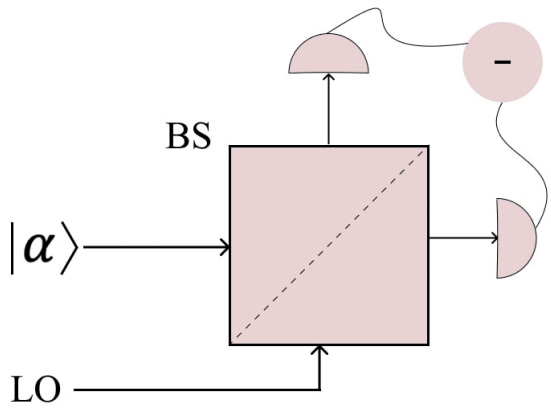

Fig. 2. *A symmetric beam splitter is used to combine the coherent signal state* $|\alpha\rangle$ *and a reference optical field (local oscillator). The resulting beams are directed onto the photodiodes of a homodyne detector, which transforms the incident radiation into a difference photocurrent.*

with Gaussian modulation, and at the same time still capture many important aspects of continuous variable quantum key distribution. Additionally, it best illustrates the analogy with the well-known BB84 protocol, especially when using vector diagram visualization methods (**Fig. 3, 4**).

A typical scheme for implementing the CV QKD protocol with discrete modulation is as follows [11]:

1. The sender (Alice) generates a random complex value $|\alpha\rangle$, where $a = A\exp(i\varphi) = q + ip$ – is a fixed parameter, φ can take one of four values: $\varphi = \{0, \pi/2, \pi, 3\pi/2\}$. Moreover, the values $\varphi = \{0,\pi\}$ encode q, and the values $\varphi = \{\pi/2, 3\pi/2\}$ encode p.

2. Alice repeats step 1 several times, i.e. she generates a set of complex parameters $\{\alpha\}$. On the basis of this set, alternately creates and sends coherent states $\{|\alpha\rangle\}$ in the form of separate parcels (laser pulses) to the recipient (Bob).

3. Bob, using the method of balanced homodyne detection, measures one of two quadrature components in each parcel:

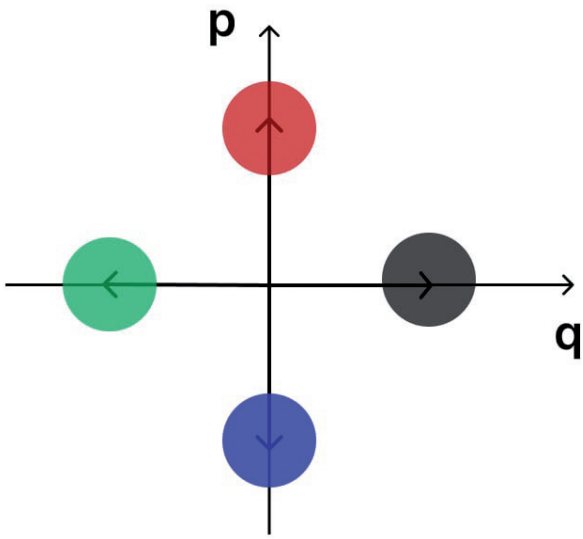

Fig. 3. *Visualization of the first and second steps of the protocol using the method of vector diagrams. Alice prepares one of the four states in each parcel.*

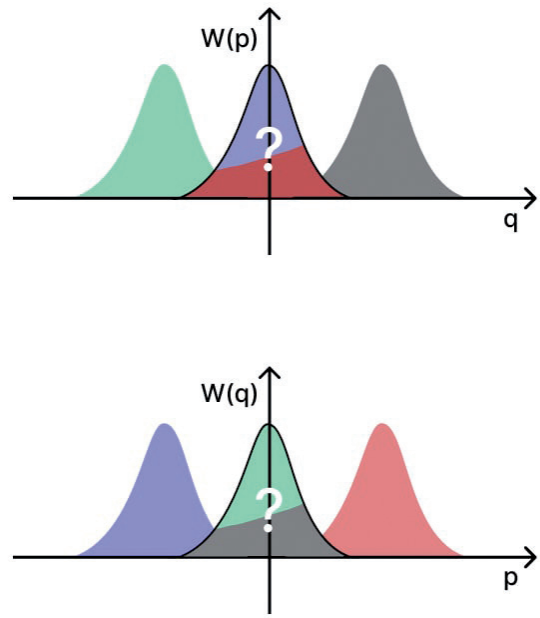

Fig. 4. *Visualization of the third step of the protocol. Bob, using the method of balanced homodyne detection, projects the received state onto a vertical or horizontal axis, measuring either the "coordinate" q or the "momentum" p.*

"coordinate" q or "momentum" p. In other words, it regulates at its own discretion the phase difference between the signal and the homodyne θ. According to formula (1), $\theta = 0$ corresponds to the "coordinate" measurement, and $\theta = \pi/2$ to the "momentum" measurement. The measurement results constitute Bob's raw key.

4. Bob informs Alice via an open channel which variable (q or p) he measured in each parcel, without giving its value. It is assumed that before the start of the key distribution procedure, Alice and Bob synchronized the phases of the signals and clearly know what is taken as q, and what is p.

5. Alice uses the information received from Bob to obtain her "raw" key, discarding those values of the sequence of random variables, which, when measuring, Bob made a mistake with the choice of phase. For example, the parcel encoded the q, and Bob measured the p.

6. Alice generates a binary key. The parcels remaining after the previous paragraph with the values $\varphi = \{0,\pi/2\}$ are assigned 1, and the messages with the values $\varphi = \{\pi, 3\pi/2\}$ are assigned 0.

7. Bob analyzes the average value of the photocurrent obtained as a result of homodyne detection of each specific parcel from the set received from Alice. If it is positive and corresponds to the value A, then it assigns 1 to this parcel, if it is negative and corresponds to the value $-A$, then it assigns 0. If the average value of the photocurrent is close to zero, then this means that Bob did not guess right the basis, and such parcels are rejected.

If the average value of the photocurrent observed by Bob falls between the values of A, or $-A$, or 0, and there is a rise in the variance of the photocurrent, it is possible that an eavesdropper (Eve) is monitoring the communication channel.

The key difference between protocols with Gaussian modulation is that the complex

numbers $a = A\exp(i\varphi) = q + ip$, that Alice generates can take not all four different values, but be generated according to a two-dimensional Gaussian distribution centered at the origin and variance V_A. Then the resulting variance of quadratures, taking into account quantum noise in the appropriate units, is equal to $V = V_A + 1$.

The proposed protocol does not require either a source or a single-photon detector. The protocol is commonly implemented in an optical fiber using lasers that emit radiation at a wavelength of 1550 nm as the radiation source [46]. As a detection device, balanced homodyne detectors with inexpensive photodiodes based on silicon or gallium arsenide are used [47]. The scheme proposed above does not take into account some of the aspects that arise during technical implementation. These aspects include: the properties of a local oscillator, the noise and losses in the communication channel and in the detector, signal polarization distortions, properties of amplitude and phase modulators of the optical fields, stabilization of the visibility of the interference pattern. For details on these and some other issues, please refer to the bibliography [25].

5. CLASSIFICATION OF ATTACKS

The classification of attacks can be carried out in several ways [11]. An Eavesdropper (Eve) can conduct attacks on the protocol or attacks on its technical implementation. Attacks on the protocol can be divided into two groups: indirect attacks, using Eve's auxiliary quantum system, referred to as an ancilla, and direct attacks, which do not involve the use of an ancilla. Attacks using an ancilla can be further categorized into three types: individual, collective, and coherent. In individual attacks, Eve prepares multiple ancillas, with each ancilla interacts with the corresponding quantum state of Alice (or Bob), which directly carries information about the key. At a later time, Eve performs measurements on each ancilla separately, obtaining certain information about the secret key. In the case of a collective attack, each ancilla also interacts with a specific quantum information system. However, Eve conducts a collective measurement on all ancillas simultaneously, enabling her to obtain more information than in the case of individual measurements. The third type of possible attack is the coherent attack, which is the most general type of attack. In this type of attack, Eve's ancilla represents, in general, a multi-level quantum system that interacts with all information states at once. Subsequently, Eve performs measurements on her ancilla at an opportune moment. In some cases, it is possible to show the equivalence between collective and coherent attacks. However, in general, it is not always possible to explicitly construct a coherent attack or specify the maximum amount of information that Eve will gain from such an attack. Analyzing individual and collective attacks is generally more straightforward. Furthermore, it allows us to address the fundamental question of whether the protocol is secret in principle, meaning it satisfies the necessary condition of secrecy.

6. CLASSICAL POST-PROCESSING

Similar to all quantum protocols, classical post-processing is necessary for CV QKD: the data resulting from the quantum part of the protocol must be classically processed to obtain the final secret key. Classical post-processing includes [11] several stages: key sifting – parcels in which Alice and Bob were unable to determine each other's bases, are discarded. Parameter Estimation – Alice and Bob publicly disclose a portion of the key in order to estimate parameters such as link loss and additional noise. These values are essential for computing the mutual information between Alice and Bob, as well as the Holevo quantity. [7].

Information reconciliation – Alice and Bob use classical information reconciliation algorithms to check the success of the previous steps. Such algorithms include Slice reconciliation [48], Multidimensional reconciliation [49], LDPC codes [50]. A distinction is also made between direct and reverse reconciliation, in the case of CV QKD, reverse reconciliation is preferable. Confirmation – at this stage, a family of universal hash functions is usually applied to the key in order to make sure that the error correction is successful. Privacy amplification – Alice and Bob perform a hashing procedure to uniformly compress the key and obtain the final secret key. Authentication - in each of the steps above, Alice and Bob must be sure that they are exchanging information with each other, and not with a third party that can play the role of Bob for Alice, and for Bob to play the role of Alice.

7. NOISE ANALYSIS FOR CV QKD

The noise level in communication channels and equipment is a critical aspect of all quantum cryptography protocols, as the noise may contain information that could be valuable to an eavesdropper. It is assumed that Eve possesses all the required resources to extract information from the noises. In CV QKD, the role of noise goes to an even higher level, the presence of Eve can be determined by the level of quantum noise, so the influence of additional noise of a different nature should be minimized. Additional noises include: non-ideal noise of the QKD system [25], leakage noise in the detector χ_{det}, overlap noise due to non-ideal visibility of the interference pattern, noise of instability in signal intensity and local oscillator χ_{Lo}, noise of non-ideal modulation, Raman scattering noise χ_{Ram}, measurement discretization noise. If the noises are stochastically independent, then their variances add up:

$$\chi = \chi_{det} + \chi_{Lo} + \chi_{Ram}. \quad (2)$$

From the point of view of vector diagrams (Fig. 1), additional noise adds up to quantum noise, which effectively increases the circle of uncertainty.

Additional noise is frequently categorized into two groups: those that Eve can access and those that are inaccessible to Eve. For example, "original" (ORM) and "realistic" (RRM) noise models are distinguished [38]. Such classifications make it easier to analyze secrecy in some cases. So, for example, it does not seem too rough an assumption that Eve does not have access to a local oscillator, if it is completely on the side of Alice and cannot be transferred [25]. Nonetheless, the conditional nature of such classifications somewhat restricts the inferences that can be made.

8. SECURITY ANALYSIS

Let N be the number of transmissions that Alice and Bob share as a result of the quantum part of the protocol. After Alice and Bob perform the basis reconciliation procedure, they obtain a list of symbols of length $n \leq N$, which is referred to as the raw key. After undergoing classical post-processing, Alice and Bob compress the secret key, obtaining the final secret key of length $l \leq n$. One can consider the scenario in which the number of transmissions tends towards infinity, often referred to as the asymptotic limit, and introduce the quantity r, denoted as the "secret fraction" [11]:

$$r = \lim_{N\to\infty} \frac{l}{n}. \quad (3)$$

The quantity (3) appears in many security proofs of quantum protocols. Additionally, parameters such as the raw key generation rate R, which can be estimated experimentally, i.e., the number of raw key symbols that can be generated by the QKD system per unit of time, are introduced. Similarly, the secret key generation rate is also introduced $K = Rr$.

In the case of an individual attack, the Csiszár-Korner formula is applicable for r [51]:

$$r^{\infty}_{Shannon} = I_{AB} - I_{BE}, \quad (4)$$

where I_{AB} – Shannon mutual information between Alice and Bob [52], a fraction of shared secret bits possessed by Alice and Bob. This parameter can be accurately computed during the phase of reverse reconciliation, if the reconciliation is not perfect, which is often the case in practice, value I_{AB} should be replaced by βI_{AB}, where $\beta < 1$ reconciliation parameter. Similarly, mutual information between Alice and Eve I_{AE} is determined in the same manner, and also between Bob and Eve I_{BE}. For the case of CV QKD, reverse reconciliation is preferable, so in formula (4) we use I_{BE}. In the case of direct reconciliation, should be used I_{AE} instead of I_{BE}.

For the CV QKD protocol with Gaussian modulation, these quantities are equal [53]:

$$I_{AB} = \frac{1}{2}\log_2 \frac{V+\chi}{1+\chi},$$
$$I_{BE} = \frac{1}{2}\log_2 \left((\eta T)^2 (V+\chi)(V^{-1}+\chi)\right), \quad (5)$$

where $V = V_A + 1$, V_A – the Alice's gaussian modulation variance, χ – the correction term that takes into account the influence of additional noise sources (2), η – the detector quantum efficiency, T – the transmission line losses. The expression for I_{BE} may differ from (5), and this quantity depends on the model of additional noise and on the permissible actions of Eve, which are dictated by the chosen model [53].

In the case of a collective attack, the Devetak-Winter [54] formula is applicable for the quantity r:

$$r^{\infty}_{Holevo} = I_{AB} - I_{BE},$$

where χ_{BE} – Holevo quantity [7] is the fundamental bound on the information that can be obtained by Eve, this quantity is achieved with quantum collective measurements. The Holevo quantity can be computed after considering the equivalent EPR version of the protocol using the symplectic eigenvalues of the covariance matrix γ_{AB} of Alice and Bob, at moments before (γ_{AB}) and after ($\gamma_{A|B}$) Bob's projective measurements. The covariance matrix is also expressed in terms of the protocol parameters. [55]. Then, for the Holevo quantity, we have:

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right),$$
$$G(x) = (x+1)\log_2(x+1) - (x)\log_2(x),$$
$$\lambda_{1,2} = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \quad (6)$$
$$\lambda_{3,4} = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}],$$

where

$$A = V^2(1-2T) + 2T + T^2(V + \chi_{line})^2,$$
$$B = T^2(\chi_{line} + 1)^2,$$
$$C = \frac{V\sqrt{B} + T(V + \chi_{line}) + A\chi_{\text{hom}}}{T(V + \chi_{tot})},$$
$$D = \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{tot})}.$$

The expression for χ_{BE} may also differ from (6) depending on the chosen noise model and Eve's capabilities. The above expression (6) is constructed for what is known as the "realistic" model [55], in which:

$$\chi_{tot} = \chi_{line} + \chi_{\text{hom}} / T,$$
$$\chi_{\text{hom}} = \frac{1 + v_{el}}{\eta} - 1,$$
$$\chi_{line} = \frac{1}{T} - 1 + \varsigma,$$

where ν_{e1} – detector electronic noise, ς – the excess noise.

There are indications that for CV QKD, a coherent attack does not provide any new information to Eve compared to a collective attack [24].

There are other approaches to assess security, for instance, the Renner's epsilon

criterion [56], which is based on the trace distance:

$$\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\| \le \varepsilon,$$

where $\rho_{S_A S_B E}$ – the density matrix of Alice, Bob, and Eve obtained after the key distribution session. S_A, S_B – the final keys of Alice and Bob, where the index E denotes the quantum register of Eve, τ_{SS} – the density matrix corresponding to a uniform key distribution of length l. ρ_E – the density matrix of Eve, which is factorized with respect to the systems of Alice and Bob and is uncorrelated with them. The criterion has a transparent interpretation, and the matrix $\tau_{SS} \otimes \rho_E$ reflects some ideal outcome of quantum key distribution, while the matrix $\rho_{S_A S_B E}$ represents the actual situation. Then "closer" the real situation is to the ideal one, the better it is for Alice and Bob. This criterion holds true in the case of any Eve's attack and does not rely on the asymptotic limit of key generation.

9. CONCLUSION

Therefore, the potential for continuous-variable protocols is significant and can be implemented with the current level of technological advancement. Such protocols continue to be at the forefront in terms of a secret key rate (about 2.3 Mbps at distance 25 km [57]). Moreover, the distance over which a secret key can be distributed has significantly increased due to the relatively new methods of classical post-processing. Further research, both theoretical and experimental, requires the development and consideration models of noises that occur during the practical implementation of the protocol. Additionally, it is essential to analyze and unify the numerous existing models. Another important area of research is CV QKD protocols secrecy proving. Unconditional security has only been proven for a small number of main CV QKD protocols. For many practically important CV QKD protocols, security has only been proven against collective attacks in the asymptotic regime. Despite their specifics, continuous variable quantum key distribution (CV QKD) protocols may emerge as a significant rival to protocols with discrete variables such as BB-84 in the future.

REFERENCES

1. Dowling JP, Milburn GJ. Quantum technology: the second quantum revolution. *Phil. Trans. R. Soc. Lond.,* 2003, A361:1655-1674.
2. Lars J. *The Second Quantum Revolution.* Springer International Publishing, 2018, 339 p.
3. Horodecki R, Horodecki P, Horodecki M, Horodecki K. Quantum entanglement. *Rev. Mod. Phys.*, 2009, 81:865-942.
4. Bennett CH, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.,* 1993, 70:1895-1899.
5. Wootters W, Zurek W. A Single quantum cannot be cloned. *Nature,* 1982, 299:802-803.
6. Nielsen A, Chuang IL. *Quantum computation and quantum information*. Cambridge, Cambridge University Press, 2000, 676 p.
7. Holevo AS. Quantum Systems, Channels, Information: A Mathematical Introduction. *De Gruyter Studies in Mathematical Physics,* 2012, 16, 362 p, Berlin, Germany, ISBN 978-3-11-027325-0.
8. Kulik SP. Quantum cryptography. Part 1. *Photonics Russia*, 2010, 2:36-41.
9. Kulik SP. Quantum cryptography. Part 2. *Photonics Russia*, 2010, 3:56-60.
10. Kulik SP. Quantum cryptography. Part 2. *Photonics Russia*, 2010, 4:28-34.

11. Wolf R. Quantum Key Distribution: An Introduction with Exercises. *Lecture Notes in Physics*, Switzerland, Springer, 2021, 229 p.
12. Vernam GS. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Amer. Inst. Elec. Eng.*, 1926, 45:109-115.
13. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 1978, 21:120-126.
14. Lenstra AK. *Integer Factoring in Encyclopedia of Cryptography and Security*. Boston, Springer US, 2011, p 297.
15. Shor PW. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 1999, 41:303-332.
16. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 1984, p. 175-179.
17. Ekert AK. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.,* 1991, 67:661-663.
18. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 1992, 68:3121-3124.
19. Grosshans F, Grangier P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.,* 2002, 88:057902-1-4.
20. Lo H, Ma X, Chen K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.,* 2005, 94:230504-1-4.
21. Grosshans F, Assche GV, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. *Nature,* 2003, 421:238-241.
22. Schleich WP. *Quantum Optics in Phase Space*. Berlin, Wiley-VCH, 2001, 717 p.
23. Braunstein SL, Van Loock P. Quantum information with continuous variables. *Rev. Mod. Phys.*, 2005, 77:513-577.
24. Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security, and implementations. *Entropy,* 2015, 17(12):6072-6092.
25. Laudenbach F, Pacher C, Fung CHF, Poppe A, Peev M, Schrenk B, Hentschel M., Walther P, Hübel H. Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations. *Adv. Quantum Technol.,* 2018, 1:1800011-1-37.
26. Mironov YB, Kazantsev SY, Shakhovoy RA, Kolesnikov OV, Mashkovtseva LS, Zaitsev AI, Korobov AV. Analiz perspektiv razvitiya istochnikov odinochnykh fotonov v sistemakh kvantovogo raspredeleniya klyuchey. [Analysis of the prospects for the development of sources of single photons in quantum key distribution systems]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli*., 2021, 13(6):22-33 (in Russ.).
27. Mashkovtseva LS, Bolotov DV, Kazantsev SY, Kolesnikov OV, Mironov YB, Selyukov AS. Naukometricheskiy analiz publikatsiy po istochnikam odinochnykh fotonov dlya sistem svyazi s kvantovym raspredeleniem klyuchey. [Scientometric analysis of publications on sources of single photons for quantum key distribution systems]. *Nauchno-tekhnicheskaya informatsiya. Seriya 1: Organizatsiya i metodika informatsionnoy raboty*, 2022, 1:22-31 (in Russ.).
28. Zaitsev A, Zubilevich A, Kolesnikov O, Korobov A. Istochniki odinochnykh fotonov dlya infokommunikatsionnykh

sistem. [Sources of single photons for infocommunication systems]. *Pervaya milya*, 2022, 6(106):64-69 (in Russ.).

29. Cabrera B. Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors. *Appl. Phys. Lett.,* 1998, 73:735.
30. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber. *Phys. Rev. Lett.*, 2020, 125:010502-1-6.
31. Hosseinidehaj N, Babar Z, Malaney R, Ng SX, Hanzo L. Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook. *IEEE Communications Surveys and Tutorials,* 2019, 21:881-919.
32. Weedbrook C, Ottaviani C, Pirandola S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A*, 2014, 89:012309-1-8.
33. Qi B, Lougovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X*, 2015, 5:041009-1-12.
34. Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V, Gleim A. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis. *Scientific Reports,* 2020, 10:10034-1-9.
35. Leverrier A, Grangier P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.*, 2009, 102:180504-1-4.
36. Cerf NJ, Levy M, Assche GV. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A,* 2001, 63:052311-1-5.
37. Filip R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A*, 2008, 77:022310-1-5.
38. Chi YM, Qi B, Zhu W, Qian L, Lo HK, Youn SH, Lvovsky AI, Tian L. A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution. *New J. Phys.,* 2011, 13:013003-1-18.
39. Arbekov IM, Molotkov SN. Extraction of quantum randomness. *UFN,* 2021, 191:651-669.
40. Shakhovoy R. Digitization of a Random Signal from the Interference of Laser Pulses: Issue of Randomness Extraction for a Quantum Random Number Generator. *2023 Wave Electronics and its Application in Information and Telecommunication Systems,* St. Petersburg, 2023, p. 1-7.
41. Smithey DT, Beck M, Raymer MG, Faridani A. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: application to squeezed states and the vacuum. *Phys. Rev. Lett.,* 1993, 70:1244-1247.
42. Wigner EP. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.,* 1932, 40:749-759.
43. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV. The Wigner function negative value domains and energy function poles of the harmonic oscillator. *Journal of Computational Electronics,* 2021, 20:2148-2158.
44. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV, Afonin PV. The Wigner function negative value domains and energy function poles of the polynomial oscillator. *Physica A: Statistical Mechanics and its Applications,* 2022, 598:127339-1-15.

45. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV. Extended Wigner Function for the Harmonic Oscillator in the Phase Space. *Results in Physics,* 2020, 19:103546-1-8.
46. Dianov EM. Fiber lasers. *UFN,* 2004, 174:1139-1142.
47. Blakemore JS. Semiconducting and other major properties of gallium arsenide. *Journal of Applied Physics*, 1982, 53:123-181.
48. Assche GV, Cardinal J, Cerf NJ. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory,* 2004, 50:394-400.
49. Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 2008, 77:042325-1-8.
50. Richardson T, Urbanke R. *Modern Coding Theory*. New York, Cambridge University Press, 2008, 590 p.
51. Csiszár I, Korner J. Broadcast channels with confidential messages. *IEEE transactions on information theory,* 1978, 3:339-348.
52. Shannon CE. A mathematical theory of communication. *The Bell system technical journal,* 1948, 27(3):379-423.
53. Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 2009, 8(3):1301-1350.
54. Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A,* 2005, 461:207-235.
55. Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, Grangier P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A,* 2007, 76:042305.
56. Renner R. Security of quantum key distribution. *Int. J. Quantum Inf,* 2008, 6:1-127.
57. Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous variable quantum key distribution with real-time parameter monitoring and key distillation. *SPIE Photonex* (Birmingham, 2022). 2023, V. 12335.