Classification of Continuous-Variable Quantum Key Distribution Protocols

Subjects: Optics

Contributor: Roman Goncharov , Irina Vorontsova , Daniil Kirichenko , Ilya Filipov , Iurii Adam , Vladimir Chistiakov , Semyon Smirnov , Boris Nasedkin , Boris Pervushin , Daria Kargina , Eduard Samsonov , Vladimir Egorov

Quantum communications, in general, and quantum key distribution (QKD) as one of the internal directions, in particular, are some of the most actively developing areas of quantum technologies. QKD allows one to send a secure key between several legitimate users connected by so-called quantum and classical channels. Theoretically, the security of QKD is based on the principles of quantum mechanics, which guarantees security against any unforeseen technological developments, for example, in the field of quantum computing.

CV-QKD protocols schemes

1. General Approach to Quantum Key Distribution Protocol Description

As for a general classification of quantum key distribution (QKD) protocols, continuous-variable quantum key distribution (CV-QKD) included, two scenarios can be distinguished: “prepare-and-measure” (PM) and “entanglement-based” (EB) ones. In the PM scenario, Alice encodes classical information into quantum states (the preparation stage), then transmits them to Bob as optical signals. Subsequently, Bob makes a series of measurements for each of the received signals to restore the encoded information. EB scenario, in turn, implies that both Alice and Bob operate with modes of the entangled state. CV-QKD being the case, Alice generates a two-mode squeezed vacuum state and measures both quadratures of one of its modes. In turn, the second mode is sent to Bob to be projected onto a coherent state. In practice, most CV-QKD systems belong to the first of the above-mentioned approaches. Nevertheless, both for DV- and CV-QKD protocols, it is convenient to use the virtual entanglement method. The interchangeability of EB and PM approaches for the CV-QKD case is proved in the paper [1] for single-mode coherent states in the PM scheme and distribution of two-mode squeezed vacuum states in the EB scheme. The covariance matrices describing the two above-mentioned scenarios coincide up to a constant.

A similar relationship exists for DV-QKD protocols as well. For example, BB84 protocol can be reduced to the equivalent EB version, where Alice and Bob operate with an entangled pair of photons [2]. Additionally, it is possible to use entropic uncertainty relations uniting information leakage to Eve and classical conditional entropy between Alice and Bob. This approach is equivalent to a protocol where Alice randomly and equiprobably selects a basis, and then selects one of three states within the basis, also randomly and equiprobably, and sends them to the channel. The possibility of using entropic uncertainty relations for three-particle systems describing the general

quantum state “Alice–Bob–Eve” exists only by reducing the original PM protocol to a mathematically equivalent EB version [3].

The equivalence discussed cannot be called completely strict when considering a broader class of attacks [4], which implies the need for a security proof in the PM scenario [5][6][7]. However, security against collective attacks for finite keys has been proved for CV-QKD protocols both in PM and EB approaches separately [8][9][10].

If researchers address the protocol on squeezed states with the homodyne detection method [11], although the security proof against coherent attacks for finite-length keys was demonstrated, the secure key generation rate assessment turned out to be too pessimistic; that is, $\lim_{N\to\infty} K^{\varepsilon}(N) < K_{\text{call}}^{\text{asymp}}$.

The recently proposed de Finetti Gaussian reduction approach for CV-QKD protocols with Gaussian modulation [8] shows the possibility of achieving security against coherent attacks in realistic implementation using the protocol invariance considering a unitary group instead of a symmetric one. That is, the protocol part has been simplified in the terms of symmetrization. A mention should also be made of additional energy tests (measurements of the local number of photons on the users’ sides) in the context of the security described. Moreover, recent results show that certain parameters can provide a key distribution with a sufficient key rate, taking into account the finite key effects, confirmed by numerical modeling methods [4][12][13][14]. For real practical systems, a composable security is provided against collective attacks (without symmetrization and energy tests) by the current moment [15].

Noteworthy, here, an important motivation to account for in terms of a protocol choice is the need for a convenient and as “seamless” as possible integration of the CV-QKD system with existing telecommunication infrastructure. This implies the search for solutions that are simpler in the context of state generation (namely, single-mode coherent states), rather than two-mode squeezing. The latter option is, indeed, a frontier solution of great interest; however, the complexity of such states’ preparation forces us to reject this approach. Thus, the choice is made in favor of the PM scheme for the above-discussed mathematical equivalence to EB schemes.

2. Quantum Channel Implementation

There are two ways to implement a quantum channel for CV-QKD, as well as for DV-QKD: through optical fibers [15][16] and optical channels in free space [4][17]. The latter is attracting more and more attention because of the convenience of creating infrastructure in practice; unlike fiber channels, transmission through free space is devoid of all the disadvantages associated with transportation and difficulties in installing a physical fiber channel sensitive to mechanical influences and seismic features of the terrain (here, underground lines). This, undoubtedly, makes them more portable and flexible in the context of installation and operation. However, when working with free space, it is necessary to take into account not only the presence of diffraction losses, atmospheric extinction, and background thermal noise [18][19], but also the attenuation effect caused by guidance error and turbulence [20].

Fiber systems for secure key transmission, in turn, have already proven themselves in the context of QKD: such systems provide a high level of durability (the vulnerability of fiber-optic QKD communication systems is analyzed

in their study), low cost of implementation, and availability of installation and maintenance.

Additionally, though free space realizations of CV-QKD protocols carry a huge research potential and have their own advantages, researchers do not consider them as the main option here, for researchers aim at the integration of CV-QKD systems with existing telecommunication fiber optical networks.

3. Channel Configuration Schemes

For the case of DV-QKD, two schemes can be implemented: one-way and two-way schemes. Moreover, both schemes can implement the same protocol; for example, there are one-way schemes for BB84 protocols (for example, Ref. [21]) and two-way schemes using a QKD system of plug-and-play [22][23] type.

Similar schemes can be implemented in the CV-QKD case as well. In a typical one-way CV-QKD protocol, Alice prepares a quantum state and sends it to Bob via a quantum channel. The receiver performs coherent detection, followed by post-processing procedures performed by users.

One disadvantage of one-way schemes is the presence of phase and polarization distortions in the channel. To mitigate them, it is necessary that additional algorithms and modifications be used. Despite the fact there are questions about the stability of the system, for one-way CV-QKD schemes with Gaussian modulation, security against coherent attacks is justified [8][24].

In the two-way CV-QKD scheme [25][26][27], analogously to DV-QKD ones, Alice and Bob use a quantum channel twice to obtain a raw key. Initially, Bob prepares the so-called reference states and sends them to Alice through a quantum channel. Alice, in turn, encodes the information by applying unitary operations to the received reference states, and then sends them to Bob for measurement. In such CV-QKD schemes, various information encoding protocols can be used; the common ones are Gaussian modulation of coherent states, implying the use of amplitude and phase modulators, as well as double phase modulation, implying two phase modulators [23][28].

The main advantage of the two-way scheme is the potential stability of the QKD system, which is achieved by the auto-compensation of phase and polarization distortions of light passing through the same fiber in two directions. However, in the framework of world scientific practice, such QKD systems are only nascent [28][29], and have not yet been sufficiently studied. Moreover, two-way schemes can be limited in the implementation of a LO (preference is given to local LO, see Section 2.7) since the transmitted LO, like the signal, suffers twice as much losses in two passes. A practical security proof of two-way CV-QKD systems is also an actual task.

4. Types of Modulation

In the context of choosing the type of modulation of the CV-QKD system, it can be conditionally divided into two actively developing areas [30]: CV-QKD protocols with Gaussian [15][31][32][33][34][35][36] and discrete modulation [37][38][39][40][41][42][43][44][45].

At the same time, a critical disadvantage of this type of CV-QKD protocol is the incompleteness of their theoretical models. However, to date, active work are underway to fill this gap. There are a number of works demonstrating different approaches to proving security in the asymptotic regime [39][40][46] (i.e., for keys of infinite length) against an optimal attack (the convex optimization problem is solved). It is important to note that these works have already provided the basis for the composable security proof, including non-perfect homodyning and finite-key effects in the context of collective attacks [43]. A security proof using de Finetti for discrete modulation is still an open problem.

In addition, discrete modulation is inferior to the Gaussian one in terms of the secure key generation rate and the maximum distance at which a key distribution session is still possible: the results are demonstrated for various configurations of QAM and PSK (see Ref. [40]).

The unconditional security of CV-QKD protocols with Gaussian modulation, on the contrary, is strictly proved taking into account the finite key effects. Most recent experimental CV-QKD systems still operate with Gaussian modulated coherent states [15][17][24]. Nevertheless, one cannot fail to note the incipient growth in the popularity of discrete modulation schemes [42][44][45].

5. Quantum States

Continuing the classification, in CV-QKD implementations, coherent or squeezed states can be used. They, in turn, can be single-mode or two-mode. An increase in the number of modes is also possible, but the appropriate analysis due to the structure of the states themselves (for example, when using phase-modulated attenuated coherent states) is often reduced to considering the single-mode case [36][47][48][49], so it does not make much practical sense to single it out separately.

First CV-QKD protocols were proposed in 1999 in [50]. These protocols utilized coherent and two-mode squeezed states with discrete modulation and homodyne detection.

In the coherent state protocol, pulse modulation is used to encode information using two modulators, amplitude and phase, and then one of the signal quadratures is detected. If the session is recognized as secure, the measurement results for the second quadrature are used for subsequent key generation. In the protocol operating with two squeezed states generated using two different squeezed light sources, an entangled state is considered. After homodyne detection of the modes of the entangled state, it becomes possible to extract information about one of the initial states.

Later, CV-QKD protocols were proposed based on squeezed states with Gaussian modulation, where the states were modulated by quadratures according to a two-dimensional Gaussian distribution [11]. Initially, the protocol was described in the context of homodyne detection, but later heterodyne detection was also taken into account [51]. The CV-QKD protocol proposed in 2002 with Gaussian modulation of coherent states GG02 can now be considered the most well-known and widespread [31][52].

Discussing coherent states further, thermal states should also be mentioned separately. In essence, they are being noisy coherent states themselves and require equivalent mathematical description. Currently, research is underway in the field of CV-QKD using such states. The security analysis of CV-QKD protocols using thermal Gaussian states in the case of collective Gaussian attacks was carried out, for example, in the work [53], for cases of direct and reverse reconciliation with homodyne and heterodyne detection methods. The authors have shown that in the case of direct reconciliation with homodyning detection, it is possible to increase the key rate when taking into account the Alice's trusted noise, even with large values of the modulation variance of the initial thermal states. In addition, the authors determined the upper bound of entanglement stability in the case of CV-QKD for different wavelength values.

Regarding practical implementation of CV-QKD systems, it should be noted that CV-QKD protocols based on squeezed states may be superior to protocols based on coherent states. However, the assumption of infinite squeezing [51] should be used, which cannot be implemented experimentally. In addition, the generation of squeezed states is a much more complex task, than the generation of coherent ones (in fact, they are states of attenuated laser radiation), which becomes the most problematic part of the implementation of the CV-QKD protocol using squeezed states in practice [54].

References

1. Grosshans, F.; Cerf, N.J.; Wenger, J.; Tualle-Brouri, R.; Grangier, P. Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables. Quantum Inf. Comput. 2003, 3, 535–552.
2. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. Phys. Rev. Lett. 1992, 68, 557–559.
3. Molotkov, S.N. Quantum Key Distribution with Nonbinary Phase–Time Encoding That Admits an Exact Proof of Secrecy. J. Exp. Theor. Phys. 2019, 128, 700–706.
4. Pirandola, S. Limits and security of free-space quantum communications. Phys. Rev. Res. 2021, 3, 013279.
5. Kozubov, A.; Gaidash, A.; Miroshnichenko, G. Finite-key security for quantum key distribution systems utilizing weak coherent states. arXiv 2019, arXiv:1903.04371.
6. Gaidash, A.; Kozubov, A.; Miroshnichenko, G. Countermeasures for advanced unambiguous state discrimination attack on quantum key distribution protocol based on weak coherent states. Phys. Scr. 2019, 94, 125102.
7. Kozubov, A.; Gaidash, A.; Miroshnichenko, G. Quantum control attack: Towards joint estimation of protocol and hardware loopholes. Phys. Rev. A 2021, 104, 022603.

8. Leverrier, A. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. Phys. Rev. Lett. 2017, 118, 200501.
9. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. Phys. Rev. Lett. 2012, 109, 100502.
10. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Erratum: Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security Against Coherent Attacks. Phys. Rev. Lett. 2014, 112, 019902.
11. Cerf, N.J.; Lévy, M.; Assche, G.V. Quantum distribution of Gaussian keys using squeezed states. Phys. Rev. A 2001, 63, 052311.
12. Hosseinidehaj, N.; Walk, N.; Ralph, T.C. Optimal realistic attacks in continuous-variable quantum key distribution. Phys. Rev. A 2019, 99, 052336.
13. Hosseinidehaj, N.; Lance, A.M.; Symul, T.; Walk, N.; Ralph, T.C. Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection. Phys. Rev. A 2020, 101, 052335.
14. Pirandola, S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. Phys. Rev. Res. 2021, 3, 043014.
15. Jain, N.; Chin, H.M.; Mani, H.; Lupo, C.; Nikolic, D.S.; Kordts, A.; Pirandola, S.; Pedersen, T.B.; Kolb, M.; Ömer, B.; et al. Practical continuous-variable quantum key distribution with composable security. Nat. Commun. 2022, 13, 4740.
16. Hiskett, P.A.; Rosenberg, D.; Peterson, C.G.; Hughes, R.J.; Nam, S.; Lita, A.E.; Miller, A.J.; Nordholt, J.E. Long-distance quantum key distribution in optical fibre. New J. Phys. 2006, 8, 193.
17. Shen, S.Y.; Dai, M.W.; Zheng, X.T.; Sun, Q.Y.; Guo, G.C.; Han, Z.F. Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment. Phys. Rev. A 2019, 100, 012325.
18. Er-long, M.; Zheng-fu, H.; Shun-sheng, G.; Tao, Z.; Da-sheng, D.; Guang-can, G. Background noise of satellite-to-ground quantum key distribution. New J. Phys. 2005, 7, 215.
19. Liorni, C.; Kampermann, H.; Bruß, D. Satellite-based links for quantum key distribution: Beam effects and weather dependence. New J. Phys. 2019, 21.
20. Semenov, A.A.; Töppel, F.; Vasylyev, D.Y.; Gomonay, H.V.; Vogel, W. Homodyne detection for atmosphere channels. Phys. Rev. A 2012, 85, 013826.
21. Marand, C.; Townsend, P.D. Quantum key distribution over distances as long as 30 km. Opt. Lett. 1995, 20, 1695.

22. Stucki, D.; Gisin, N.; Guinnard, O.; Ribordy, G.; Zbinden, H. Quantum key distribution over 67 km with a plug&play system. New J. Phys. 2002, 4, 341.
23. Kawamoto, Y.; Hirano, T.; Namiki, R.; Ashikaga, M.; Shimoguchi, A.; Ohta, K. “Plug and play” systems for quantum cryptography with continuous variables. IQEC Int. Quantum Electron. Conf. Proc. 2005, 2005, 1612–1613.
24. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. Adv. Opt. Photonics 2020, 12, 1012.
25. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. Nat. Phys. 2008, 4, 726–730.
26. Ottaviani, C.; Pirandola, S. General immunity and superadditivity of two-way Gaussian quantum cryptography. Sci. Rep. 2016, 6, 22225.
27. Ghorai, S.; Diamanti, E.; Leverrier, A. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. Phys. Rev. A 2019, 99, 012311.
28. Huang, D.; Huang, P.; Wang, T.; Li, H.; Zhou, Y.; Zeng, G. Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. Phys. Rev. A 2016, 94, 032305.
29. Valivarthi, R.; Etcheverry, S.; Aldama, J.; Zwiehoff, F.; Pruneri, V. Plug-and-play continuous-variable quantum key distribution for metropolitan networks. Opt. Express 2020, 28, 14547.
30. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. Entropy 2015, 17, 6072–6092.
31. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett. 2002, 88, 057902.
32. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys. Rev. A 2011, 84, 062317.
33. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photonics 2013, 7, 378–381.
34. Jouguet, P.; Elkouss, D.; Kunz-Jacques, S. High-bit-rate continuous-variable quantum key distribution. Phys. Rev. A 2014, 90, 042329.
35. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci. Rep. 2016, 6, 19201.

36. Goncharov, R.; Samsonov, E.; Kiselev, A.D. Subcarrier wave quantum key distribution system with gaussian modulation. J. Phys. Conf. Ser. 2021, 2103, 012169.
37. Hirano, T.; Yamanaka, H.; Ashikaga, M.; Konishi, T.; Namiki, R. Quantum cryptography using pulsed homodyne detection. Phys. Rev. A 2003, 68, 042331.
38. Hirano, T.; Ichikawa, T.; Matsubara, T.; Ono, M.; Oguri, Y.; Namiki, R.; Kasai, K.; Matsumoto, R.; Tsurumaru, T. Implementation of continuous-variable quantum key distribution with discrete modulation. Quantum Sci. Technol. 2017, 2, 24010.
39. Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. Phys. Rev. X 2019, 9, 041064.
40. Denys, A.; Brown, P.; Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum 2021, 5, 540.
41. Lupo, C. Towards practical security of continuous-variable quantum key distribution. Phys. Rev. A 2020, 102, 022623.
42. Rios, C. Experimental Characterization of a Discrete Gaussian-Modulated Quantum Key Distribution System. Ph.D. Thesis, The University of Arizona, Tucson, AZ, USA, 2021.
43. Lupo, C.; Ouyang, Y. Quantum Key Distribution with Nonideal Heterodyne Detection: Composable Security of Discrete-Modulation Continuous-Variable Protocols. PRX Quantum 2022, 3, 010341.
44. Roumestan, F.; Ghazisaeidi, A.; Renaudier, J.; Vidarte, L.T.; Leverrier, A.; Diamanti, E.; Grangier, P. Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution. arXiv 2022, arXiv:2207.11702.
45. Pan, Y.; Wang, H.; Shao, Y.; Pi, Y.; Li, Y.; Liu, B.; Huang, W.; Xu, B. Experimental Demonstration of High-Rate Discrete-Modulated Continuous-Variable Quantum Key Distribution System. arXiv 2022, arXiv:2203.08470.
46. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. Phys. Rev. X 2019, 9, 021059.
47. 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. Sci. Rep. 2020, 10, 10034.
48. Fang, J.; Huang, P.; Zeng, G. Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation. Phys. Rev. A 2014, 89, 022315.
49. Shi, S.; Tian, L.; Wang, Y.; Zheng, Y.; Xie, C.; Peng, K. Demonstration of Channel Multiplexing Quantum Communication Exploiting Entangled Sideband Modes. Phys. Rev. Lett. 2020, 125, 070502.

50. Ralph, T.C. Continuous variable quantum cryptography. Phys. Rev. A 1999, 61, 010303.
51. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. Phys. Rev. Lett. 2009, 102, 130501.
52. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum Cryptography Without Switching. Phys. Rev. Lett. 2004, 93, 170504.
53. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-variable quantum key distribution using thermal states. Phys. Rev. A—At. Mol. Opt. Phys. 2012, 86.
54. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; 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.