NANOSYSTEMS:
PHYSICS, CHEMISTRY, MATHEMATICS

Guselnikov M.S., et al. *Nanosystems: Phys. Chem. Math.*, 2025, **16** (3), 311–316.
http://nanojournal.ifmo.ru
DOI 10.17586/2220-8054-2025-16-3-311-316

Original article

Properties of multi-moded phase-randomized coherent states

Mikhail S. Guselnikov[1,a], Andrei A. Gaidash[1,2,b], George P. Miroshnichenko[1,c], Anton V. Kozubov[1,2,d]

[1]ITMO University, Saint Petersburg, Russia
[2]Steklov Mathematical Institute of Russian Academy of Sciences, Moscow, Russia

[a]msguselnikov@itmo.ru, [b]andrewdgk@gmail.com, [c]gpmirosh@gmail.com, [d]avkozubov@itmo.ru

Corresponding author: Gaidash A.A., andrewdgk@gmail.com

ABSTRACT Phase-randomized coherent states are widely used in various applications of quantum optics. They are best known to be the core part of decoy-state quantum key distribution protocols with phase-coding. From the perspective of future development of quantum protocol architecture, it is important to determine whether phase randomization can be applied at an arbitrary stage of an optical scheme without affecting the informational properties of the quantum system. In this paper, using the superoperator formalism, we have shown that phase randomization of a two-mode coherent state commutes with linear optical transformations. This implies that phase randomization can be applied virtually at any point within the optical setup. We further demonstrate that the Holevo bound for such a state coincides with that of regular coherent states, bearing in mind that the Holevo bound quantifies only the maximum amount of information accessible to an eavesdropper. Advantages of phase-randomized coherent states compare to regular ones in particular cases of eavesdropper's strategies should be considered separately. Also, these findings indicate that phase randomization can be directly applied to a subcarrier wave quantum key distribution type of systems, opening prospects for its future development.

KEYWORDS coherent states, phase randomization, phase-averaged coherent states, quantum key distribution, Holevo bound, subcarrier wave quantum key distribution.

ACKNOWLEDGEMENTS Contribution to the work of A. A. Gaidash and A. V. Kozubov was financially supported by Russian Science Foundation (project 20-71-10072) and performed at Steklov Mathematical Institute of Russian Academy of Sciences.

FOR CITATION Guselnikov M.S., Gaidash A.A., Miroshnichenko G.P., Kozubov A.V. Properties of multi-moded phase-randomized coherent states. *Nanosystems: Phys. Chem. Math.*, 2025, **16** (3), 311–316.

1. Introduction

Phase-randomized or phase-averaged coherent states (PHAVs) are peculiar quantum optical states: a mixture of Fock states with Poissonian distribution. In particular, they are known to be utilized in the study of generalized Hong-Ou-Mandel effect [1]. However, they are best known in the context of quantum key distribution (QKD) protocols based on weak coherent states. Especially, two-moded ones are widely used in protocols with phase-coding, implying utilization of Mach-Zehnder interferometer [2, 3], or other interferometric schemes [4–8]. Compare to single photons, attenuated laser radiation - treated as weak coherent states - can contain more than one photon, which may compromise the security of such protocols for quantum communication, and PHAVs have proven to be an effective tool for enhancing the security of weak coherent state QKD protocols [9], leading to the development of decoy-state QKD protocols [10]. Since then, PHAVs have become critically important in quantum communication. Their properties have been extensively studied, revealing the non-Gaussian nature of their Wigner functions, simple methods of generation, and a growing range of applications [11–17].

Practical decoy-state QKD protocols with phase-coding utilize multi-mode (precisely, two-mode) PHAVs. The main difference compare to single-mode PHAVs is that multi-mode ones may contain relative phase. And, unlike single-mode PHAVs, the informational properties of multimode PHAVs remain incompletely characterized. In this paper, we focus on exploration in regards to the order of optical transformations including phase-randomization taken place in QKD optical schemes, and how this order might affect the informational aspects. In other words, our goal is to elaborate on whether phase randomization in two-mode systems commutes with linear optical transformations and what consequences of the ordering choice are.

2. Commutation of phase-randomization with transformations of linear optics

First, consider a density matrix ρ of a two-mode phase-randomized state constructed from coherent states $|\alpha\rangle$ and $|\beta\rangle$, where $\alpha = |\alpha|e^{i\theta}$ and $\beta = |\beta|e^{i(\theta+\phi)}$ are complex amplitudes of coherent states, respectively,

$$\rho(\phi) = \int |\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta| \frac{d\theta}{2\pi}. \tag{1}$$

Density matrix above can be expressed in terms of superoperator notation:

$$\begin{gathered}
\rho(\phi) = N \int e^{\overleftarrow{(\alpha a_1^\dagger + \beta a_2^\dagger)} + \overrightarrow{(\alpha^* a_1 + \beta^* a_2)}} |0\rangle\langle 0| \frac{d\theta}{2\pi} = \\
N \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{\overleftarrow{(|\alpha| a_1^\dagger + |\beta| e^{i\phi} a_2^\dagger)^{n-k}} \overrightarrow{(|\alpha| a_1 + |\beta| e^{-i\phi} a_2))^k} \delta_{n-2k,0}}{(n-k)!k!} |0\rangle\langle 0| = \\
= N \sum_{n=0}^{\infty} \frac{\overleftarrow{\left((|\alpha| a_1^\dagger + |\beta| e^{i\phi} a_2^\dagger)\right.} \overrightarrow{\left.(|\alpha| a_1 + |\beta| e^{-i\phi} a_2))\right)^n}}{n!n!} |0\rangle\langle 0| = \\
= N \sum_{n} \frac{(\mathcal{K}_{R(\phi)}^{(+)})^n}{n!n!} |0\rangle\langle 0|, \quad R(\phi) = \begin{pmatrix} |\alpha|^2 & |\alpha\beta| e^{-i\phi} \\ |\alpha\beta| e^{i\phi} & |\beta|^2 \end{pmatrix},
\end{gathered} \tag{2}$$

where we have integrated over the common phase θ of the two coherent states; $a_i^\dagger (a_i)$ is the creation (annihilation) operator of the i^{th} mode, $N = e^{-|\alpha|^2 - |\beta|^2}$ is normalization constant, also $\mathcal{K}_{R(\phi)}^{(+)} = \sum_{ij} R(\phi)_{ij} \overleftarrow{\hat{a}_i^\dagger} \overrightarrow{\hat{a}_j}$ introduced in [18], $\overleftarrow{A} B = AB$ and $\overrightarrow{A} B = BA$ is left- and right-action notation for superoprators, $(\,\cdot\,)^*$ denotes complex conjugation and $(\,\cdot\,)^\dagger$ denotes the Hermitian conjugation, δ_{ij} is the Kronecker delta-symbol. Obtained superoperator form provides some explicit insights on the properties of the state, that will be discussed further.

We discuss additional transformations applied to the state, that may take place before or after the phase randomization. Expression of the state in the superoperator notation (2) explicitly shows that any transformation that maps a set of creation (annihilation) operators to a different set of creation (annihilation) operators, in particular, of the form $a_i^\dagger \to \sum_j M_{ij} a_j^\dagger$ for a given matrix M_{ij}, preserves the state to be phase-randomized. Basically, these are transformations that describe actions of linear optics devices. Note, it may even change the number of considered modes. The same holds true for the coherent state before the phase randomization, i.e. the same transformation preserves the state to be coherent. We may conclude, then, that this type of transformations should be commutative with phase-randomization. Consider sequential actions of the transformation (M) and phase-randomization (PR) and vice versa to show that they are indeed commutative:

$$\begin{gathered}
\otimes_j |\alpha_j\rangle = N_0 e^{\sum_j \overleftarrow{\alpha_j a_j^\dagger}} |0\rangle \quad \xrightarrow{PR} \quad N_0^2 \sum_{n=0}^{\infty} \frac{\left(\left(\sum_j \overleftarrow{\alpha_j a_j^\dagger}\right)\left(\sum_j \overrightarrow{\alpha_j^* a_j}\right)\right)^n}{n!n!} |0\rangle\langle 0| \\
\downarrow M \\
N_0^2 \sum_{n=0}^{\infty} \frac{\left(\left(\sum_{jk} \overleftarrow{|\alpha_j| e^{i\phi_j} M_{jk} a_k^\dagger}\right)\left(\sum_{jk} \overrightarrow{|\alpha_j| e^{-i\phi_j} M_{jk}^\dagger a_k}\right)\right)^n}{n!n!} |0\rangle\langle 0| \\
\uparrow PR \\
\otimes_j |\alpha_j\rangle = N_0 e^{\sum_j \overleftarrow{\alpha_j a_j^\dagger}} |0\rangle \quad \xrightarrow{M} \quad N_0 e^{\sum_{jk} \overleftarrow{\alpha_j M_{kj} a_k^\dagger}} |0\rangle
\end{gathered} \tag{3}$$

where N_0 is normalization constant. Thus, phase randomization and transformation provided by elements of linear optics are commutative operations.

3. Consequences of the ordering choice for a QKD

As mentioned in the introduction, phase-randomized states are employed in QKD, especially in decoy-states schemes. The essential parts of such QKD schemes are beamsplitters as well as phase modulators (as a part of Mach-Zehnder interferometer scheme), where the latter can be described by the following transformation: $e^{i\phi a^\dagger a} a^\dagger e^{-i\phi a^\dagger a} = a^\dagger e^{i\phi}$, that also agrees with the provided point above in regard to commutativity. The main idea of phase randomization in the decoy state method is to separate the single-photon fraction of the received mixture of Fock states. Thus, practically, the phase randomization process, according to the conclusions made above, can be applied to the state at any point of the optical scheme, even at the receiver's side, and, at the first glance, that may lead to a new design of protocols. Indeed, from the

point of view of legitimate user only, it does not affect the performance of QKD setup. However, and we shall emphasize that, position of phase-randomization obviously may impact the information accessible to an eavesdropper.

In order to elaborate on the latter issue, we shall estimate the difference of regular coherent states and phase-randomized coherent states in regard to provided to eavesdropper information. Thus, we propose to compare the Holevo bound for these two types of states as rather simple example without necessity of considering special cases, that is given by

$$\chi = S(\rho) - \sum_i p_i S(\rho(\phi_i)), \tag{4}$$

where $\rho = \sum_i p_i \rho(\phi_i)$ is the density matrix of an ensemble, $S(\rho) = -\mathbf{Tr}(\rho \log_2 \rho)$ is von Neumann entropy. Further two phases $\phi_0 = 0$ and $\phi_1 = \pi$ within one informational basis will be considered. Also, their probabilities of choosing are equal, i.e. $p_0 = p_1 = \frac{1}{2}$. For coherent states, Holevo bound is well known and is given by

$$\chi_{CS} = h\Big(\frac{1 - e^{-2|\beta|^2}}{2}\Big), \tag{5}$$

$$h(x) = -x \log_2(x) - (1-x)\log_2(1-x), \tag{6}$$

where the latter is the binary entropy function. As for the phase-randomized states, von Neumann entropy can be estimated by eigenvalues λ_i of the density matrix: $S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i$. Eigenvalues of $\rho(\phi)$ can be easily calculated by introduced in [18] superoperator algebra: adjoint action of $\mathcal{N}_{iV}^{(-)} = i \sum_{nm} V_{nm} (\overleftarrow{\hat{a}_n^\dagger \hat{a}_m} - \overrightarrow{\hat{a}_n^\dagger \hat{a}_m})$ provides unitary rotation of the matrix $R(\phi)$ in $\mathcal{K}_{R(\phi)}^{(+)}$ and thus can be diagonalized, i.e.

$$e^{\mathcal{N}_{iV}^{(-)}} \mathcal{K}_{R(\phi)}^{(+)} e^{-\mathcal{N}_{iV}^{(-)}} = \mathcal{K}_{e^{iV} R(\phi) e^{-iV}}^{(+)} = \mathcal{K}_{UR(\phi)U^\dagger}^{(+)}, \tag{7}$$

where U is given by

$$U = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}} \begin{pmatrix} -|\beta| e^{i\phi} & |\alpha| \\ |\alpha| e^{i\phi} & |\beta| \end{pmatrix}. \tag{8}$$

According to (7), R has two eigenvalues: 0 and $|\alpha|^2 + |\beta|^2$, so $\rho(\phi)$ can be expressed in its diagonalized form as follows:

$$\rho_{\text{diag}}(\phi) = N \sum_{n=0}^{\infty} \frac{(|\alpha|^2 + |\beta|^2)^n}{n!} |n\rangle\langle n| \otimes |n\rangle\langle n|. \tag{9}$$

Since

$$\big[g(n)|n\rangle\langle n| \otimes |n\rangle\langle n|, g(k)|k\rangle\langle k| \otimes |k\rangle\langle k|\big] = 0, \tag{10}$$

$$g(n) = \frac{(|\alpha|^2 + |\beta|^2)^n}{n!}, \tag{11}$$

where $[\,\cdot\,,\,\cdot\,]$ stands for commutator, operators under the sum can be diagonalized by the same eigenoperators, and non-zero eigenvalue of $\rho(\phi)$ can be determined as

$$\lambda = N \sum_n \frac{(|\alpha|^2 + |\beta|^2)^n}{n!} = 1. \tag{12}$$

Both $\rho(0)$ and $\rho(\pi)$ have the same non-zero eigenvalue: $\lambda = 1$. Thus, they do not contribute to the Holevo bound quantity. However, for the ensemble density matrix $\rho = \frac{1}{2}(\rho(0) + \rho(\pi))$ introduced superoperator algebra cannot be directly applied, since superoperators of $(\mathcal{K}_{R(0)}^{(+)})^n + (\mathcal{K}_{R(\pi)}^{(+)})^n$ cannot be simultaneously diagonalized. So, firstly, we express the density matrix in the Fock basis in its general form as follows:

$$\rho = N \sum_{n=0}^{\infty} \sum_{k,p=0}^{n} \frac{|\alpha|^{2n-(k+p)} |\beta|^{k+p} (1 + (-1)^{k-p})}{2\sqrt{(n-k)!(n-p)!k!p!}} |n-k\rangle\langle n-p| \otimes |k\rangle\langle p|. \tag{13}$$

Note, that

$$\Big[A(n,k,p), A(m,k',p')\Big] = 0, \tag{14}$$

$$A(n,k,p) = \sum_{k,p=0}^{n} f(n,k,p)|n-k\rangle\langle n-p| \otimes |k\rangle\langle p|, \tag{15}$$

$$f(n,k,p) = \frac{|\alpha|^{2n-(k+p)}|\beta|^{k+p}(1+(-1)^{k-p})}{2\sqrt{(n-k)!(n-p)!k!p!}}, \tag{16}$$

as well, so operators $A(n,k,p)$ under the sum for different values of n in ρ share the same eigenoperators, and thus they can be diagonalized simultaneously. Therefore eigenvalues of ρ are determined by the sum of eigenvalues of $A(n,k,p)$ for all values of n. Characteristic equation for each $A(n,k,p)$ is given by

$$\lambda^{n-1}\Bigg((-1)^{n+1}\lambda^2 + \Big(\frac{(-|\alpha|^2-|\beta|^2)^n}{n!}\Big)\lambda + \\ + \frac{(-1)^{n+1}|\alpha\beta|^2}{n!n!}\sum_{m=0}^{n-1}\Bigg(\binom{2n}{2m+1}\frac{|\alpha|^{4(n-m-1)}|\beta|^{4m}}{2}\Bigg)\Bigg) = 0, \tag{17}$$

and there are only two non-zero eigenvalues, thus

$$\lambda_{\pm} = N\sum_{n=0}^{\infty}\lambda_{n,\pm} = N\sum_{n=0}^{\infty}\frac{(|\alpha|^2+|\beta|^2)^n \pm (|\alpha|^2-|\beta|^2)^n}{2(n!)} = \frac{1\pm e^{-2|\beta|^2}}{2}, \tag{18}$$

and, respectively, the Holevo bound for two-mode phase-randomized coherent state χ_{PR} is equal to the Holevo bound for regular coherent states χ_{CS}. Dependence of the Holevo bound on $|\beta|$ is shown in Fig. 1.

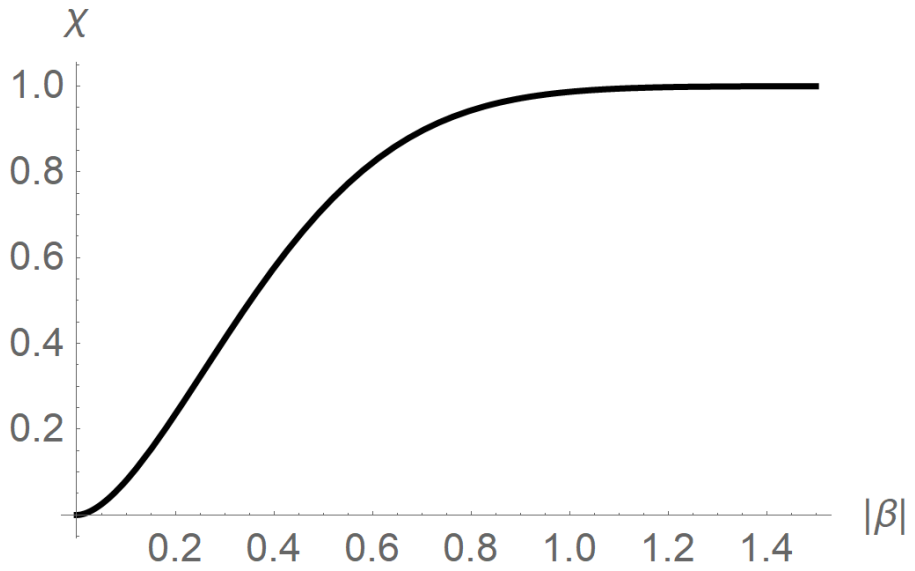

FIG. 1. Dependence of the Holevo bound χ for PHAV ensemble state $\rho = \frac{1}{2}(\rho(0)+\rho(\pi))$, where $\rho(\phi)$ is defined in Eq. (2), on the absolute value of the amplitude of the coherent state $|\beta|$ as it shown in Eq. (6)

At this point, we have shown that the phase randomization of two-mode coherent state do not influence the maximum of accessible for an eavesdropper information. Unfortunately, consideration of special cases of eavesdropper's interactions with the states, whether they are regular coherent or PHAV ones, is obligatory for a security analysis. For instance, in case of unambiguous state discrimination (USD) [19–23], an eavesdropper can easily construct positive operator-valued measure (POVM) for a set of linearly independent pure states, such as a set of coherent states. However, mixed states may introduce linear dependency, and in this case USD POVM cannot be constructed.

4. Implementation to subcarrier wave quantum key distribution

Another thing to note is that, from the observations, it immediately follows that multi-moded phase-randomized coherent state can be created by applying multi-mode (generalized) beamsplitter to a single-mode phase-randomized coherent state. Therefore, phase modulation with harmonic signal, as it is employed in subcarrier wave (SCW) QKD

[23–27], also produce multi-moded phase-randomized coherent state, since the provided transformation of annihilation (creation) operator is given by

$$a_i = \sum_{j=-S}^{S} D_{ij}^{S}(\mu, \nu, \eta) a_j, \tag{19}$$

where $D_{ij}^{S}(\mu, \nu, \eta)$ is the Wigner D-function with S being a number of interaction modes, μ, ν, and η are some angles that define axes of rotation [28]. Considering the stated above, it appears that the decoy-state method may be directly applied to an SCW QKD protocol as well, providing a new variation of the protocol. However, in order to make a final decision on that and elaborate full decoy-state protocol for an SCW setup, a few points should be addressed prior in regards. The first one is accurate selection of single-photon fraction of the signal, that may be non-trivial problem for a milti-mode states with high (approaching to infinity) amount of modes, and parameter estimation, such as quantum bit error of detection events that have originated from single-photon signals. The second is required analysis of discrete phase-randomization, as it was provided recently for the original decoy-state protocol. Estimation of closeness between full phase-randomized states and the discrete phase-randomized [29–31] ones and conclusion regarding the necessary amount of discrete phases for them to be close enough in case of SCW setup are essential for practical implementations.

5. Conclusion

In this paper, we have investigated two-mode PHAVs from the point of view of the superoperator formalism, that provide useful insights on its properties. In particular, observations demonstrate preservation of state's type (phase-randomized) under a linear optical transformation. Therefore, this approach clearly shows that the phase randomization transformation commutes with one provided by linear optics. In context of QKD applications, phase randomization can be applied at any point within the optical scheme, at least, from the point of view of legitimate users.

At the same time, utilization of phase-randomization may significantly influence accessible to an eavesdropper information. Hence, we have estimated the Holevo bound for ensemble of two-mode phase-randomized coherent states ($\rho = \frac{1}{2}(\rho(0) + \rho(\pi))$) and found it matches with the Holevo bound for regular coherent states with the same phase difference within the ensemble. However, the Holevo bound quantifies the maximum of accessible to an eavesdropper information and consideration of particular attacks may vary the outcome. For instance, USD probabilities are heavily affected by the type of considered states to be measured, especially for pure and mixed states. Therefore, additional estimations for particular cases may be considered for a full informational characterization of PHAVs.

Also, if phase-randomization commutes with transformation provided by linear optics, it appears, that phase-randomization may be directly applied to SCW QKD type of systems. It may open prospects to a new kind of SCW QKD protocol with PHAVs.

References

[1] Zhang Y., Wei K., Xu F. Generalized Hong-Ou-Mandel quantum interference with phase-randomized weak coherent states. *Physical Review A*, 2020, **101**(3), P. 033823.

[2] Bennett C., Bessette F., Brassard G.,Salvail L., and Smolin J. Experimental quantum cryptography. *Journal of cryptology*, 1992, **5**(3).

[3] Gobby C., Yuan Z., and Shields A. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 2004, **84**, P. 3762.

[4] Bogdanski J., Ahrens J., Bourennane M. Sagnac quantum key distribution and secret sharing. *In Quantum Communications Realized II, SPIE*, 2009, **7236**, P. 120–127.

[5] Mo X., Zhu B., Han Z., Gui Y., Guo G. Faraday-Michelson system for quantum cryptography. textitOptics letters, 2005, textbf30(19), P. 2632–2634.

[6] Brougham T., Barnett S., McCusker K., Kwiat P., Gauthier D. Security of high-dimensional quantum key distribution protocols using Franson interferometers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 2013, **46**(10), P. 104010.

[7] Vorontsova I., Goncharov R., Kynev S., Kiselev F., Egorov V. Measurement-device-independent continuous variable quantum key distribution protocol operation in optical transport networks. *Nanosystems: Physics, Chemistry, Mathematics*, 2023, **14**(3), P. 342–348.

[8] Latypov I.Z., Chistiakov V.V., Fadeev M.A., Sulimov D.V., Khalturinsky A.K., Kynev S.M., Egorov V.I. Hybrid quantum communication protocol for fiber and atmosphere channel. *Nanosystems: Physics, Chemistry, Mathematics*, 2024, **15**(5), P. 654–657.

[9] Lo H.-K., Preskill J. Phase randomization improves the security of quantum key distribution. *arXiv preprint quant-ph/0504209*, 2005.

[10] Lo H.K., Ma X., and Chen K. Decoy state quantum key distribution. *Physical review letters*, 2005, **94**(23), P. 230504.

[11] Allevi A., Bondani M., Marian P., Marian T., and Olivares S. Characterization of phase-averaged coherent states. *Journal of the Optical Society of America B*, 2013, **30**(10), P. 2621–2627.

[12] Allevi A., Olivares S., Bondani M. Manipulating the non-Gaussianity of phase-randomized coherent state. *Optics Express*, 2012, **20**(22), P. 24850–24855.

[13] Wang Q., Wang X.B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. *Scientific reports*, 2014, **4**(1), P. 4612.

[14] Valente P., Lezama A. Probing single-photon state tomography using phase-randomized coherent states. *Journal of the Optical Society of America B*, 2017, **34**(5), P. 924–929.

[15] Moschandreou E., Garcia J.I., Rollick B.J., Qi B., Pooser R., and Siopsis G. Experimental study of Hong-Ou-Mandel interference using independent phase randomized weak coherent states. *Journal of Lightwave Technology*, 2018, **36**(17), P. 3752–3759.

[16] Glerean F., Rigoni E.M., Jarc G., Mathengattil S.Y., Montanaro A., Giusti F., et.al. Ultrafast pump-probe phase-randomized tomography. *Light: Science and Applications*, 2018, **14**(1), P. 115.

[17] Zhao Y., Qi B., and Lo H.K. Experimental quantum key distribution with active phase randomization. *Applied physics letters*, 2007, **90**(4), P. 044106.
[18] Gaidash A., Kozubov A., Kiselev A., and Miroshnichenko G. Algebraic approach for investigation of a multi-mode quantum system dynamics. *arXiv preprint arXiv:2207.01383*, 2022.
[19] Ivanovic A.D. How to differentiate between non-orthogonal states. *Physics Letters A*, 1987, **123**(6), P. 257–259.
[20] Peres A., Terno D.R. Optimal distinction between non- orthogonal quantum states. *Journal of Physics A: Mathematical and General*, 1998, **31**(34), P. 7105.
[21] Chefles A. Unambiguous discrimination between linearly inde- pendent quantum states. *Physics Letters A*, 1998, **239**(6), P. 339–347.
[22] Kozubov A., Gaidash A., and Miroshnichenko G. Quantum control attack: Towards joint estimation of protocol and hardware loopholes. *Physical Review A*, 2021, **104**(2), P. 022603.
[23] Gaidash A., Miroshnichenko G., and Kozubov A. Sub-carrier wave quantum key distribution with leaky and flawed devices. *Journal of the Optical Society of America B*, 2022, **39**(2), P. 577–585.
[24] Miroshnichenko G., Kozubov A., Gaidash A., Gleim A.V., and Horoshko D.V. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Optics express*, 2018, **26**(9), P. 11292–11308.
[25] Sajeed Sh., Chaiwongkhot P., Huang A., Qin H., Egorov V., Kozubov A., Gaidash A., Chistiakov V., Vasiliev V., Gleim A., et al. An approach for security evaluation and certification of a complete quantum communication system. *Scientific Reports*, 2021, **11**(1), P. 1–16.
[26] Chistiakov V., Kozubov A., Gaidash A., Gleim A., and Miroshnichenko G. Feasibility of twin-field quantum key distribution based on multi-mode coherent phase-coded states. *Optics express*, 2019, **27**(25), P. 36551–36561.
[27] Samsonov E., Goncharov R., Gaidash A., Kozubov A., Egorov V., and Gleim A. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis. *Scientific Reports*, 2020, **10**(1), P. 1–9.
[28] Miroshnichenko G., Kiselev A., Trifanov A., Gleim A. Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model. *Journal of the optical society of America B*, (2017), **34**(6), P. 1177–1190.
[29] Cao Zh., Zhang Zh., Lo H.-K., and Ma X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New Journal of Physics*, 2015, **17**(5), P. 053014.
[30] Wang R.-Q., Yin Zh.-Q., Jin X.-H., Wang R., Wang Sh., Chen W., Guo G.-C., and Han Zh.-Fu. Finite-key analysis for quantum key distribution with discrete-phase randomization. *Entropy*, 2023, **25**(2), P. 258.
[31] Nahar Sh., Upadhyaya T., and Lütkenhaus N. Imperfect phase randomization and generalized decoy-state quantum key distribution. *Physical Review Applied*, 2023, **20**(6), P. 064031.

Submitted 21 April 2025; revised 11 May 2025; accepted 12 May 2025

Information about the authors:

Mikhail S. Guselnikov – ITMO University, 3b Kadetskaya Line, 199034 Saint Petersburg, Russia; ORCID 0000-0002-0809-8431; msguselnikov@itmo.ru

Andrei A. Gaidash – ITMO University, 3b Kadetskaya Line, 199034 Saint Petersburg, Russia; Steklov Mathematical Institute of Russian Academy of Sciences, 8 Gubkina Street, 119991 Moscow, Russia; ORCID 0000-0001-9870-9285; andrewdgk@gmail.com

George P. Miroshnichenko – ITMO University, 3b Kadetskaya Line, 199034 Saint Petersburg, Russia; ORCID 0000-0002-4265-8818; gpmirosh@gmail.com

Anton V. Kozubov – ITMO University, 3b Kadetskaya Line, 199034 Saint Petersburg, Russia; Steklov Mathematical Institute of Russian Academy of Sciences, 8 Gubkina Street, 119991 Moscow, Russia; ORCID 0000-0002-4468-5406; avkozubov@itmo.ru

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