17

Application of machine learning algorithms for demodulation in QKD system with quadrature modualtion

© B.E. Pervushin[1], A.V. Zinovev[2], D.N. Kirichenko[2], I.M. Filipov[2], R.K. Goncharov[2], E.O. Samsonov[2]

[1] Yandex LLC, Moscow, Russia
[2] ITMO University, St. Petersburg, Russia

e-mail: avzinovev15@yandex.ru

Received April 28, 2025
Revised June 27, 2025
Accepted June 28, 2025

The paper shows the application of machine learning algorithms for state demodulation in a continuous-variable quantum key distribution (CV-QKD) system with quadrature-amplitude modulation (QAM) with 16 states. When using classification algorithms, the average BER was 0.019, and — 0.022 for using clustering, which is 1.75 and 1.5 times lower than the standard LLR demodulation method.

Keywords: Quantum Key Distribution, Machine Learning.

DOI: 10.61011/EOS.2025.07.61906.7725-25

1. Introduction

Quantum Key Distribution (QKD) is used to used to exchange keys between two remote users for use in symmetric data encryption. It is based on three principles of quantum mechanics: Heisenberg's uncertainty principle, the no-cloning theorem, and quantum entanglement. All three principles ensure theoretically secure encryption even in the presence of sufficiently powerful quantum computers.

At the same time, machine learning (ML) algorithms are being increasingly developed and are already finding applications in different scientific and technical fields, including the area of QKD.

QKD is divided into two major paradigms: discrete variables (DV) and continuous variables (CV). CV protocols are subdivided into protocols with discrete modulation [1] and Gaussian modulation [2] according to the method of optical signal modulation and include coherent detection methods. DV protocols are those that satisfy one or more of the following conditions: use single-photon detectors, apply the single-photon paradigm, and quantum bit error rate (QBER) is estimated as a key parameter.

DV-QKD protocols differ fundamentally from CV protocols. First, the measured physical quantity itself can only take discrete sets of values because single photons are registered. On the other hand, CV protocols with discrete modulation typically use a discrete set of values to encode field quadratures, which in principle can take continuous sets of values.

Basic CV-QKD protocols with discrete modulation use phase-shift keying (PSK) and quadrature amplitude modulation (QAM) methods. Meanwhile, CV-QKD protocols with Gaussian modulation implement optical signal modulation in which both quadratures are statistically distributed over optical pulses according to a zero-mean Gaussian distribution.

In this work, a CV protocol with discrete modulation was chosen for testing, since, as with Gaussian modulation, its security is proven [3], and it has also been shown that the protocol with discrete modulation can achieve a high secret key generation rate [4].

Currently, research and development of machine learning and neural network algorithms for application in quantum key distribution are underway. Several usage scenarios exist in the QKD field:

1. Optimization of parameters and system calibration. Every QKD system has two sets of parameters: fixed and user-defined. Fixed parameters include losses in the optical channel, detection efficiency, and other parameters determined by equipment characteristics or channel features. User-defined parameters are adjustable and optimized to achieve the maximum secure key generation rate [5–12].

2. Classification and clustering of states. In 2019, a group from Central South University in Changsha published work [13] using the standard DBSCAN machine learning method for fast identification of modulation format in CV-QKD protocols. The following year, their colleagues implemented a multimetric classification algorithm using the standard K-nearest neighbors algorithm for CV-QKD with discrete modulation [14].

3. Calculation of secret key generation rate. A research group from Nanjing University (China) published in 2021 and 2022 their results [15–17] on using neural networks for fast calculation of the secure key rate in CV-QKD protocols.

4. Phase state recognition and calibration. Use of a small machine learning model to determine the phase state was demonstrated by Spanish scientists in 2021 [18]. The developed algorithm, based on a deep neural network model, performed phase compensation in a phase-encoded protocol. In 2020, a scientific group in Nanjing studied phase modulation stabilization using an LSTM algorithm based on the BB84 phase-encoding protocol [19].

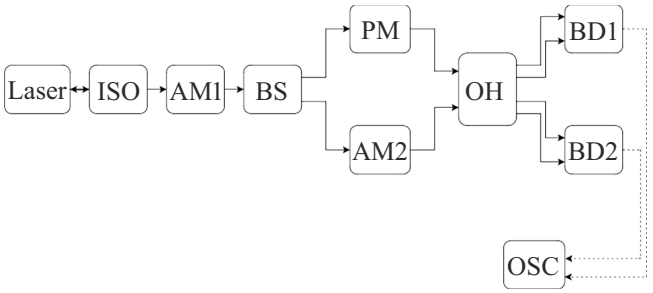

Figure 1. Experimental setup for implementing a CV-QKD protocol with discrete quadrature modulation. ISO isolator; AM1, AM2 amplitude modulators; BS beam splitter; PM phase modulator; OH optical hybrid; BD1, BD2 balanced detectors; OSC; oscilloscope.

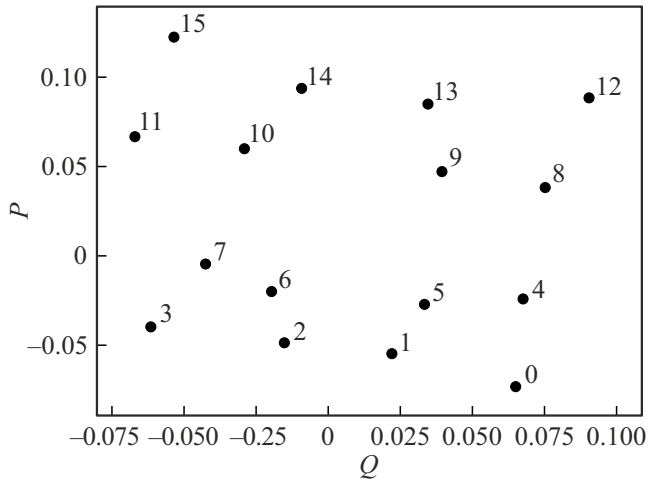

Figure 2. Constellation centers of experimental signals. Each point corresponds to the center of the distribution of the corresponding state in the quadrature modulation with 16 states.

In this article, an experiment is described on implementing a quantum key distribution system with quadrature amplitude modulation. Machine learning algorithms classification and clustering were used for demodulating the obtained data. Demodulation results were compared with a standard method using the logarithm of likelihood ratio.

2. Collection of experimental data

Due to the need to test algorithms on experimental data, an optical setup was assembled. It represents a Mach-Zehnder interferometer with signal pulses in one arm and a local oscillator in the other. The difference between the implemented setup and a standard QKD system setup is the absence of time and polarization multiplexing of signals, as well as the absence of state transmission through a channel, since this would overly complicate experimental realization.

In the setup shown in Fig. 1, radiation is generated by a single-mode laser. An optical isolator is used to protect the laser from back reflections. After the isolator, the signal reaches the first amplitude modulator, which creates the pulse mode. Then the radiation is split by a beam splitter. Half of the radiation goes into the interferometer arm with the amplitude modulator and is used as the signal radiation. The radiation in the other arm is phase modulated and used as the local oscillator. It is worth noting why the phase modulator and amplitude modulator are placed in different arms of the interferometer. In the vast majority of works, phase and amplitude are modulated specifically for the signal state, and an additional optical path in the local oscillator arm compensates for the delay time arising from the presence of extra amplitude and phase modulators in the signal arm. In this work, to simplify the setup, the phase and amplitude modulators were separated into the two arms, removing the need to balance interferometer arms. At the same time, the phase of the local oscillator is modulated relative to the signal phase, which can be accounted for by replacing the phase with an equal but opposite sign.

The optical hybrid is used to perform double homodyne detection. Using two balanced detectors, simultaneous detection of two signal quadratures is implemented. Output signals from the balanced detectors are proportional to the two quadratures of the signal state. The optical hybrid separates the signal and local oscillator, with the local oscillator in the two arms shifted in phase by 90 degrees, enabling measurement of two signal quadratures. Double homodyne detection allows determination of the position of each pulse in the phase plane. Signals from the balanced detectors go to the oscilloscope, where they are saved. Further processing is performed on a computer. The laser source power was 0 dBm at 1550 nm wavelength. A pulsed signal with a period of $0.5\,\mu$s and duty cycle 0.5 was applied to the radio-frequency input of the first amplitude modulator. The period was selected based on the fact that even a slight imbalance of the arms strongly affects interference in the optical hybrid, and also to achieve sufficient statistics while saving on the oscilloscope. The phase modulator and second amplitude modulator were driven by periodic signals defined by 16 states of quadrature modulation and one reference pulse. The reference pulse featured zero phase and maximum transmission at the second amplitude modulator. Such signals are applied to the second amplitude and phase modulators so that the output state distributions at the two balanced detectors closely resemble an ideal constellation.

As mentioned earlier, instability of arms is characteristic of fiber-optic interferometers, which leads to instability of the relative phase of the local oscillator and signal pulses. The implemented scheme is no exception, so to compensate for phase drift, a phase compensation method using two reference pulses described in article [20] was used.

As a result of the experiment, data presented in Figs. 2 and 3 were collected. For each class, $1.5 \cdot 10^4$ states were

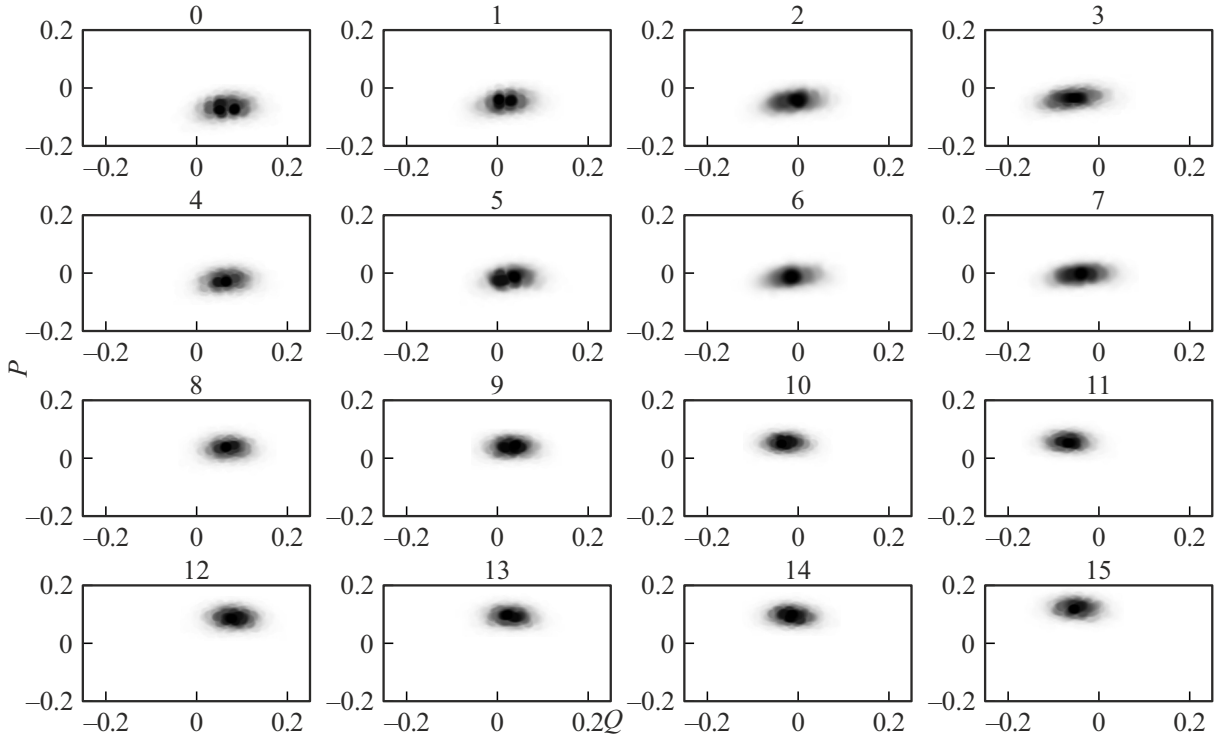

Figure 3. Experimentally obtained states on the phase plane. The axes show electrical signals from balanced detectors proportional to the corresponding quadratures of the signal.

recorded. The first figure shows centers of all states on one graph for comparison of their mutual arrangement, the second the distributions for each state on separate graphs for clearer consideration.

It can be seen that the experimentally obtained distribution centers replicate the pattern of an ideal constellation [13]. However, in this original form, the state clouds intersect. To reduce intersections, post-processing was carried out in which the square root of the quadrature signal values was calculated. Machine learning methods were used for demodulation of the obtained data.

3. Algorithm implementation

For comparison with the standard LLR demodulation algorithm (and because a QKD system is considered), it is preferable to consider bit error rate (BER) as the quality metric of the algorithms. To do this, a 4-bit string was assigned to each state. Encoding was used in which two neighboring states differ by one in Hamming distance, i.e., the corresponding bit strings differ in only one position. Such encoding is used to reduce bit errors during demodulation.

The LLR method is based on the use of conditional probabilities that, when detecting a signal with certain quadrature values, the k-th bit in its bit representation will be 0 or 1:

$$\mathrm{LLR}(k) \simeq \ln\left[\frac{\exp\left(-\left(|r-c^*(k,0)|^2/2\delta^2\right)\right)}{\exp\left(-\left(|r-c^*(k,1)|^2/2\delta^2\right)\right)}\right]$$

$$= \frac{1}{2\delta^2}\left(|r-c^*(k,1)|^2 - |r-c^*(k,0)|^2\right), \quad (1)$$

where r is the measured vector;$c^*(k,1), c^*(k,0)$ is the nearest state whose bit representation has a 1 or 0 at the k-th position respectively; δ^2 is the noise variance in the channel. The sign of the LLR for each bit determines its value. The described algorithm using the logarithm of likelihood ratio on the experimental data yields a bit error rate of 0.033.

To explore the applicability of machine learning algorithms for state demodulation in quadrature modulation systems, classification algorithms were selected: nearest neighbor method, support vector machine (SVM), and decision tree. For clustering, the k-means algorithm was chosen. DBSCAN and Agglomerative Clustering algorithms were also considered. DBSCAN does not require presetting the initial number of clusters, which can be useful for protocol development and increasing its security but may be impractical at low signal-to-noise ratio, where all clusters are too close for their separation by this algorithm. Agglomerative Clustering is, in turn, too slow and unsuitable for large data volumes and real-time operation.

To apply classification methods according to machine learning methodology, the overall dataset was split into

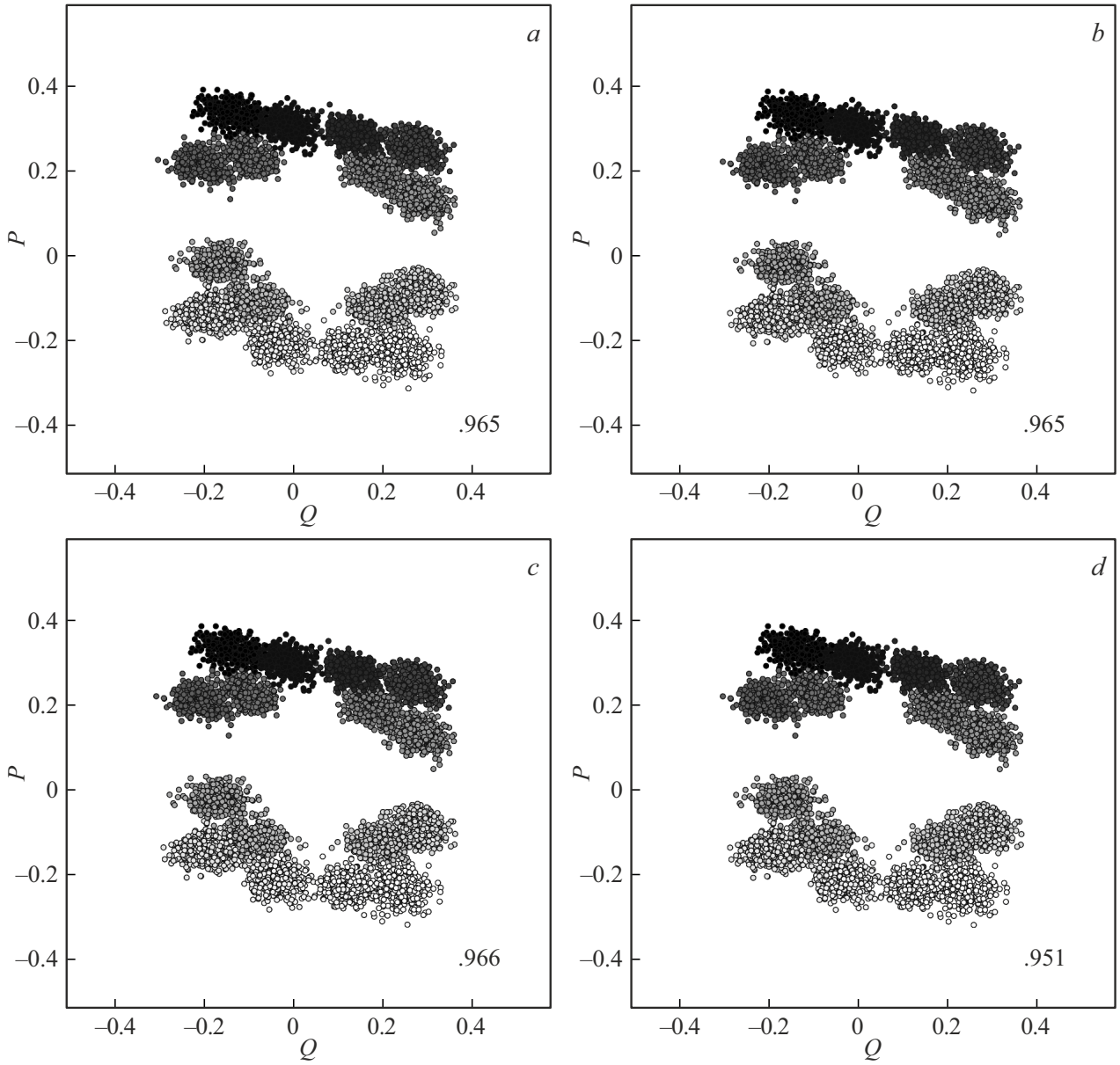

Figure 4. Graphical presentation of classification algorithm results for state demodulation: *a* – *k*-nearest neighbor method *b* -nonlinear support vector method (nonlinear SVM), *c* support vector machine (SVM) with Gaussian kernel, *d* decision tree. The graphs show the accuracy of the algorithms.

training and test samples in a 60 to 40% ratio. Classification algorithms were trained on the training sample, and on the test sample separation of states and determination of final algorithm accuracy were performed. Accuracy the ratio of correctly classified objects to their total number was used as the evaluation metric.

During algorithm training, corresponding hyperparameters were optimized. Cross-validation with 5 folds was used for hyperparameter optimization. The graph of classification algorithms application is presented in Fig. 4.

For the *k*-means algorithm, centers of the ideal constellation scaled similarly to the experimental data were used.

4. Comparison and analysis of bit error rate

For algorithm comparison, prediction time on the test sample was measured. The results for algorithm accuracy, bit error rate (BER), and testing time are presented in the table.

The results show that machine learning algorithms reduce the bit error rate by 1.74 times for classification algorithms and by 1.5 times for the *k*-means algorithm, indicating good potential of machine learning as demodulation algorithms. The support vector machine (SVM) has longer prediction

Results of applying algorithms for state demodulation

Algorithm	Accuracy	BER	Prediction time,, s
LLR	–	0.033	0.393
Nearest *k*-neighbor method	0.965	0.019	0.942
Nonlinear SVM SVM	0.965	0.019	42.11
SVM with Gaussian kernel	0.966	0.019	71.74
Decision tree	0.951	0.02	0.013
k-means	0.933	0.022	0.161

times, but in some system configurations, even small gains in bit error rate can outweigh algorithm runtime.

Results indicate that by using various machine learning algorithms, it is possible to select the most suitable algorithm for a particular QKD protocol and system. Moreover, some algorithms allow improved post-processing of sequences. For example, using the support vector method, it is possible to switch to erasure channels, i.e., to discard objects for which the algorithm is uncertain about classification correctness.

5. Conclusion

The work demonstrates the use of machine learning algorithms for state demodulation in a CV-QKD system with 16-state quadrature modulation. Using classification algorithms, the average BER was 0.019, and with clustering, 0.022, which is 1.75 and 1.5 times lower than the standard LLR demodulation method respectively. Further work will focus on implementing a complete quantum key distribution system with quadrature amplitude modulation and researching and applying ensemble methods and neural networks for state demodulation.

Funding

The study was supported by the Russian Science Foundation (project №. 24-11-00398).

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, T. Tsurumaru. Quantum Science and Technology, **2** (2), 024010 (2017).
[2] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel. Advanced Quantum Technologies, **1** (1), 1800011 (2018).
[3] C. Lupo Y. Ouyang. PRX Quantum, **3** (1), 010341 (2022).
[4] I.B. Djordjevic. IEEE Photonics Journal, **11** (4), 1–10 (2019).
[5] W. Wang H.-K. Lo. Physical Review A, **100** (6), 062334 (2019).
[6] F.-Y. Lu, Z.-Q. Yin, C. Wang, C.-H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo. JOSA B, **36** (3), B92–B98 (2019).
[7] H.-J. Ding, J.-Y. Liu, C.-M. Zhang, Q. Wang. Quantum Information Processing, **19**, 1–8 (2020).
[8] Y. Yi, Y. Rao, C. Huang, S. Zeng, Y. Yang, Q. He, X. Chen. IEEE 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 164–168 (2021).
[9] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, D. Simeonidou. IEEE 2018 European Conference on Optical Communication (ECOC), 1–3 (2018).
[10] Z.-A. Ren, Y.-P. Chen, J.-Y. Liu, H.-J. Ding, Q. Wang. IEEE Communications Letters, **25** (3), 940–944 (2020).
[11] W. Liu, P. Huang, J. Peng, J. Fan, G. Zeng. Physical Review A, **97** (2), 022316 (2018).
[12] D. Jin, Y. Guo, Y. Wang, Y. Li, D. Huang. Physical Review A, **104** (1), 012616 (2021).
[13] H. Zhang, P. Liu, Y. Guo, L. Zhang, D. Huang. JOSA B, **36** (3), B51–B58 (2019).
[14] Q. Liao, G. Xiao, H. Zhong, Y. Guo. New Journal of Physics, **22** (8), 083086 (2020).
[15] M.-G. Zhou, Z.-P. Liu, W.-B. Liu, C.-L. Li, J.-L. Bai, Y.-R. Xue, Y. Fu, H.-L. Yin, Z.-B. Chen. (2021). arXiv:2108.02578.2108.02578.
[16] Z.-P. Liu, M.-G. Zhou, W.-B. Liu, C.-L. Li, J. Gu, H.-L. Yin, Z.-B. Chen. Optics Express, **30** (9), 15024–15036 (2022).
[17] M.-G. Zhou, Z.-P. Liu, W.-B. Liu, C.-L. Li, J.-L. Bai, Y.-R. Xue, Y. Fu, H.-L. Yin, Z.-B. Chen. Scientific Reports, **12** (1), 8879 (2022).
[18] M. Ahmadian, M. Ruiz, J. Comellas, L. Velasco. Journal of Lightwave Technology, **40** (13), 4119–4128 (2022).
[19] J.-Y. Liu, H.-J. Ding, C.-M. Zhang, S.-P. Xie, Q. Wang. Phys. Rev. Appl., **12** (1), 014059 (2019).
[20] F.M. Goncharov, B.E. Pervushin, B.A. Nasedkin, R.K. Goncharov, D.A. Yashin, M.E. Gellert, D.V. Sulimov, P.A. Morozova, I.M. Filipov, I.A. Adam. Nanosystems: Physics, Chemistry, Mathematics, **14** (1), 59–68 (2023).

Translated by J.Savelyeva