National Research University Higher School of Economics

as a manuscript

Ivanov Fedor

Forward-error correction in problems of reliable and secure data transmission

–

Dissertation summary
for the purpose of obtaining academic degree
Doctor of Science in Applied Mathematics

Moscow – 2022

Relevance of the topic and problem statement

The active development of computer and information technologies, observed at the moment, leads to an increasingly rapid increase in the requirements for information transmission systems. The main requirements for modern telecommunication systems are: throughput (in terms of the amount of data transmitted per unit of time), reliability (the probability of correct recovering and processing of data) and the supported number of active system users. In addition, with the increasing digitalization of modern society, security issues are also becoming extremely relevant, that is, secure data transmission over (primarily) non-secured communication channels. Meeting of these requirements is impossible without forward-error-correcting methods.

In early telecommunication systems, algebraic codes (for example, BCH codes, Reed-Solomon codes, Reed-Muller codes, etc.) were used as forward-error correction codes. These codes were used jointly with their decoders up to half the code minimal distance (Bounded Distance Decoders - BDD). However, the coding theory based on algebraic codes with BDD is no longer able to satisfy all scenarios that are used in modern systems for processing, transmitting and storage of information.

At the same time, an active qualitative jump in the development of information technology, observed since the early 1990s, opened up the possibility of implementing long codes, the implementation of which had previously been difficult due to high complexity. It is the new available computing power that caused active research in the field of constructing long codes, for which effective polynomial decoding algorithms that practically implement maximum likelihood decoding exist.

In particular, in many cases Low-Density Parity-Check codes (LDPC codes) became in demand. Such classes of codes as turbo codes, polar codes, etc. were also developed. For these classes of codes, probabilistic decoding methods are used, the theory of which is far from its completion. The problem of the joint choice of codes and methods for their decoding becomes relevant. It should be especially noted that in probabilistic decoding such metrics as the structure of cycles in a bipartite code graph (Tanner graph), the structure of stopping sets, etc. play no less important role than such classical metrics as the minimum distance and the spectrum of weights for algebraic codes. Therefore, the task of constructing code designs that not only have good minimal distance and spectral properties, but also have a good structure of cycles in a graph, subcodes, etc., becomes relevant.

As noted above, one of the key requirements for modern telecommunication systems is the reliability of transmitted data. For example, systems that use in optical communication, allow the loss of one data packet out of 10^{15}. This means that in order to select a code-candidate for such systems, it is required to carry out at least $10^{16} - 10^{18}$ iterations of its simulation to obtain the required error probability per block 10^{-15}. It is obvious that this kind of simulation leads to significant time and overhead costs, and in some cases it is not feasible in practice. In this regard, the task of constructing sufficiently accurate analytical estimates that make it possible to evaluate the effectiveness of a given code without or with a minimum amount of simulation modeling becomes especially relevant.

The first chapter of the dissertation is devoted to the solution of the problem of constructing effective classes of LDPC codes, as well as the problem of developing a mathematical apparatus for studying the corrective properties of convolutional codes.

Another essential requirement is throughput of the system, which is directly related to the decoding time complexity. In other words, the task of minimizing the delay in the transmission of a packet of information becomes important for a number of applications. First of all, such applications are the industrial Internet of Things (IIoT), control systems, broadband transmission of video content, various applications of augmented and virtual reality, etc. Approaches to solving this problem in relation to polar codes are considered in the second chapter of the dissertation.

An additional requirement, which becomes more and more significant with the increase in the density of data transmission networks, is to enable a large number of devices/users of the system to transmit data to the base station with a given level of reliability and delay. An example of a system where the requirement for the number of active users is critical is the Internet of Things (IoT) (up to one million devices per square kilometer). It is clear that traditional "point-to-point" communication systems, which assume a single communication line between the transmitter and receiver, will be ineffective for such scenarios. In this regard, it became necessary to develop non-orthogonal non-coordinated multiple access methods that allow only synchronization of blocks. To analyze the effectiveness of a particular multiple access method, it is necessary to evaluate its throughput in terms of the amount of information that a given user can transmit in the network with a given restriction on the number of other users and some other system parameters. The solution to the problem of constructiong multiple access systems is given in the third chapter.

Finally, in recent years, the requirement to ensure the security of data transmission has become more and more critical. This is due to the fact that digital technologies are increasingly integrade in our lives, making many areas of human life, the normal functioning of organizations and entire sectors of the economy dependent on the normal functioning of a number of information systems and applications. It should be noted that at the moment the problem of security is not only not completely resolved, but in entire industries, such as the Internet of Things, there is no common understanding of how protection should be organized. In addition, a certain concern is also caused by the fact that the vast majority of traditional methods for protecting information transmitted over open communication channels can no longer be considered reliable, due to the perspective possibility of hacking them using a quantum computer. In this regard, it becomes relevant to develop such promising methods of cryptographic data protection, which would be quite easy to implement, but which would also not lend themselves to cryptanalysis using quantum algorithms. The development of post-quantum methods of cryptographic information protection based on the McEliece system was carried out in the fourth chapter of the work.

A significant contribution to solving the problems of constructing families of high-performance codes, developing effective methods for their encoding, decoding and researching their properties, developing multiple access methods, as well as researching and construction code—based cryptosystems, was made in our country by V. B. Afanassiev, A. M. Barg, L. A. Bassalygo, E. L. Bloch, S. V. Bezzateev, I. E. Bocharova, E. M. Gabidulin, I. I. Dumer, K. Sh. Zigangirov, V. A. Zinoviev, V. V. Zyablov, G. A. Kabatyansky, V. D. Kolesnik, E. A. Kruk, B. D. Kudryashov, E. T. Mironchikov, D. S. Osipov, M. S. Pinsker, Yu. Polyansky, P. S. Rybin, Yu. L. Sagalovich, V. M. Sidelnikov, V. R. Sidorenko, F. I. Solovieva, P. V. Trifonov, S. V. Fedorenko, A. A. Frolov, S. O. Shestakov, N. A. Shekhunova. Abroad — E. Arikan, M. Baldi, E. Berlekamp, R. Blahut, A. Vardy, S. Johnson, R. Gallagher, V. Guruswami, T. Kasami, R. Ketter, S. Koudekar, S. Kumar, R. McElice, J. Messi, T. Richardson, M. Sudan, I. Tal, T. Tanaka, R. Urbanke, M. Fossorie and many others.

The objective of the dissertation

The classical coding theory was developed in the direction of creating new classes of codes with good parameters (rate, spectrum, code distance) in relation to some bounds. The decoding algowithms, were created, focuse on the implementation of the error correction capabilities of these codes with the least possible complexity. Meanwhile, the development of the theory and technology of using codes (communications, data storage systems, information security systems) has led to the formulation of the problem of joint selection of codes and decoding methods focused on use in a specific applied task.

The objective of this dissertation is to construct and analyze signal-code constructions and algorithms for their decoding for non-metric channel models and data transmission scenarios.

The objects of research are linear codes, multiple access systems and information security systems based on linear codes, and the subject of research is methods for designing of linear codes and methods for their decoding, methods for constructing multiple access systems and estimating their capacities, as well as methods for constructing and analyzing information security systems based on error-correcting codes.

To achieve these goals, the following tasks are solved in the work:

1. Development of new designs of LDPC codes based on combinatorial constructions and permutation matrices that allow encoding and decoding these codes with moderate complexity, as well as estimating

the exponent of the error probability of some regular constructions of LDPC codes, with their fixed length .

2. Development of a mathematical apparatus for studying the correction properties of convolutional codes, which is based on the analysis of the properties of the spectrum of active distances, as well as the study of the properties of local erasures correction by convolutional codes.

3. Construction of high-performance and low-resource decoding schemes for polar codes, which are based on list decoding successive cancellation algorithms with information symbol inversion and fast list decoding of polar subcodes.

4. Development of effective methods of non-orthogonal multiple access, focused on the uncoordinated transmission of short data packets from devices to the base station, estimation of the throughput for the proposed transmission method, as well as the construction of code structures to resolve collisions that occur with the above transmission method.

5. Development of methods for ensuring secure data transmission in multiple access systems.

The degree of research topic elaboration

An analysis of the current stage of elaboration of the problems formulated above should take into account the requirements that are currently placed on information transmission systems. Compliance of the current progress in research with the practical requirements that are set for the developed systems for the transmission, processing and storage of information will make it possible to characterize the degree of elaboration of the problem.

Every year, information transmission systems become more and more complicated, which is dictated by both new scenarios that have appeared recently (data transmission within Internet of Things devices, video streaming, virtual and augmented reality, etc.), and increased volumes of transmitted data. But, the more complex and universal the system, the higher the requirements for it.

If we consider as an example the transmission of data over cellular communication networks of the 5-th generation (5G standard) [1], then we can distinguish 3 main transmission scenarios for which all the above problems are relevant:

- Massive Machine-to-Machine Communication (mMTC). This application is characterized by the ability to connect a very large number of simple low-power devices. The key requirement for this scenario is the support of a large number of simultaneously operating devices in the network (up to 1 million devices per 1 sq. km [43]) and the simplicity of the information transmission protocols used.
- Ultra-Reliable Low-Latency Communication (URLLC) — focuses

on providing a highly reliable data transmission with very low latency. The key requirement in this case is the data transfer delay, which should not exceed 1 ms. (10 times less than in LTE standart) [8], which also requires a sufficiently high probability of correct recovery of a data packet.

- Enhanced Mobile Broadband (eMBB) — focuses on supporting ever-increasing data rates and system performance [63]. The main requirement for this scenario is the data transfer throughput. In particular, it is 50 times higher than in the LTE standard [67].

The requirements formulated above define the key stack of technologies that are used in the implementation of the data transmission system used for a particular transmission scenario. And it is in the context of the requirements of each of the scenarios that one should analyze the applicability of a particular data transmission scheme, as well as the current status of its development.

In particular, if we speak about the transmission of large amounts of data between a small number of devices/users, then we can talk about the "point-to-point" transmission scenario, where data is transmitted along one line from the transmitter to the reciver. The key task that needs to be solved when transmitting information using the "point-to-point" scheme is to ensure the maximum transmission rate with a low error probability.

The code structures used in this type of transmission are Polar codes, LDPC codes, various concatenated structures both based on the above-mentioned codes and based on algebraic codes, convolutional codes, etc.

LDPC codes were first proposed by R. Gallagher in 1960 in his PhD thesis [32]. In the same work, the author proposed practically applicable algorithms for decoding of LDPC codes: the bit-flipping algorithm and the "belief propagation"algorithm. Due to the insufficient level of development of computer technology, LDPC codes did not find wide application immediately after their discovery and were forgotten until the end of the 1990s.

Active research of LDPC codes resumed in the late 1990s, when they were ”rediscovered” by D. McKay in his article [46]. Since then, LDPC codes have become one of the most popular areas for research in the field of error-correcting codes.

To date, some designs of LDPC codes (in particular, quasi-cyclic rate-adaptive LDPC codes [56], [45]) have involved the 5G standard as error-correcting codes for the link layer of the URLLC scenario (data transmission with high reliability and low latency) [45], [44], to 5G EMBB [33], [53]. Other practical applications of LDPC codes include the IEEE 802.11n/ac (WiFi) [62] standard, the DVB-S2 digital television standard [25] and many others. At the same time, it should be noted that the currently used code structures are obtained by optimizing some target functional (for example, the density evolution method or the P-EXIT chart method), which in turn indicates a lack of constructive methods for constructing highly efficient code structures with guaranteed properties.

Along with the construction of LDPC codes, an important and urgent task is to theorelically study the decoding error probability. This is due both to the fact that it is not always possible to simulate a long LDPC code to the required error probability, and to the fact that obtaining bounds on the error decoding probability allows one to estimate the effect of using LDPC codes as components of concatenated code structures.

There is a few papers where the non-asymptotic behavior of LDPC codes was considered. [52] explored the behavior of finite-length LDPC codes in the "start of the waterfall" region (signal-to-noise ratios where the frame-error-rate begins to decrease). In [31], [58], [68], various combinatorial techniques were used to describe decoding errors. This approach allowed the authors to obtain estimates for the average error probability per block and per bit when using iterative decoding algorithms. Most of the work discussed above deals only with the binary erasure channel and low complexity decoding algorithms (eg, bit-flipping or "belief propagation"). Only a small number of works are devoted to channels with errors.

Thus, analyzing the degree of elaboration of the problem of constructing, decoding and analyzing the efficiency of LDPC codes, it should be noted that although today a large number of constructions of long LDPC codes and algorithms for their decoding have been proposed, the development of algebraic and combinatorial methods for constructing LDPC codes that allow their efficient decoding by “belief propagation” algorithms, as well as problems of theoretical estimation of the correcting capacity of LDPC codes of finite lengths are still relevant.

Another class of codes that are used in modern telecommunications standards are Polar codes.

This class of codes was proposed by Arikan in [15]. The main result of this work is that it has been strictly proved that polar codes can reach the capacity of any symmetrical discrete memoryless channels with a binary input alphabet when decoded by the successive cancellation algorithm (SC), provided that the length of code tends to infinity.

The main disadvantage of SC decoding is the relatively low efficiency (in terms of error rate per block) for a fixed code length.

The main effort of researchers was aimed at finding more efficient decoding algorithms for polar codes that would allow realizing their potential corrective properties. In particular, [51; 61] proposed a list variant of SC. [10; 30; 35; 36; 38] have proposed a generalized decoding approach for polar codes, which makes it possible to reduce the number of decoding operations without significant degradation of performance. Another area of research is aimed at solving the problem of the space complexity of decoding. The bit-flipping SC algorithm was first introduced in [7], and a generalization of this algorithm for list decoding was proposed in [19].

Analyzing the degree of elaboration of the problem of constructing efficient and low-resource algorithms for decoding of Polar codes, it should be noted that basically the researchers solved two parallel problems — reducing the space complexity of list decoders by increasing the computational complexity (decoders based on bit-flipping) and reducing the computational complexity either due to the growth space (stack algorithms), or by fast decoding of the generalized nodes of the Polar code tree. At the same time, the problem of joint space-time optimization of polar code decoders is rather poorly developed.

In addition to block codes, there are also convolutional codes that are more efficient in some applications. Convolutional codes were proposed by P. Elias in 1955 [27]. In 1967, E. Viterbi proposed a relatively simple algorithm for decoding convolutional codes that realizes the maximum likelihood [65] approach and minimizes the probability of an error per block. In 1974, the BCJR [54] decoding algorithm was proposed to minimize the probability of a bit (symbol) error. Systematic Recursive Convolutional Codes are the main component of [18] Turbo Codes widely used today in telecommunication standards [13]. Usage of convolutional codes as components, and not as independent code structures, determines the direction of research, primarily related to the theoretical analysis of the correction capacity of these codes. The key mathematical apparatus in this case is Markov chains [4; 39; 66]. However, it should be noted that the use of this apparatus leads to rather rough estimates of the efficiency of convolutional codes. In this regard, the task of constructing a new mathematical apparatus for the theoretical analysis of the efficiency of convolutional codes, which, on the one hand, would give fairly accurate estimates, and, on the other hand, would be computationally efficient and realizable in practice, becomes relevant.

It is not always possible or efficient to organize a transmission system according to the ”point-to-point” scenario. In particular, for the scenario of mMTC discussed above, this would mean the presence of about 1 million single lines between user devices and the base station that receives information from these devices. In this and similar cases, a different paradigm is preferable: multiple access methods [3]. In this case, it is assumed that users use a single line (data transmission channel) to send information to the base station (another user or network node).

Depending on how the model of multiple access to a single frequency-time resource (data transmission channel) is organized, various methods of multiple access are distinguished. First of all, these methods are divided into orthogonal and non-orthogonal.

Orthogonal multiple access methods imply channel division between users: it can be frequency (FDMA) [49], time (TDMA) [50], frequency-time (TFDMA) [21] and code division (CDMA) [37]. Orthogonal multiple access methods are used in IEEE 802.16 (WiMAX) [2], IEEE 802.11ax (wireless LAN) [5], IEEE 802.20 [20], 4G LTE downlink [23] and others.

Non-orthogonal multiple access methods imply no sharing of channel resources between users. Instead of dividing resources, such systems resolve collisions that occur during the transmission of information from different users to the base station. It turns out that with this approach, it is possible to significantly increase the amount of transmitted traffic compared to orthogonal access methods with the same quality of service [22].

One of the earliest examples of a non-orthogonal multiple access system is the ALOHA [6] network. To date, there are many models of non-orthogonal multiple access, primarily differing in channel access methods and collision resolution algorithms. In particular, if the device has the ability to listen to the channel (carrier), then the Carrier Sense Multiple Access (CSMA) methods [9] are distinguished.

Non-orthogonal multiple access techniques have become an integral part of modern telecommunications standards. In particular, they are part of the link layer protocols in 5G (mMTC) [55], the new TV broadcasting standard in the US ATSC 3.0 [12], are used in uplink from devices to the base station in the 4G LTE standard [14] and others. It is obvious that in all future information transmission systems that must ensure the simultaneous operation of a large number of users, non-orthogonal multiple access methods will be used to access the radio resource.

Note that most of the well-known code structures that are used in classical multi-user channels, such as code division based (CDMA), [59] rate sharing, [40] interleaves, involve coordination of transmission between users. In addition, the parameters of such schemes, such as the separating sequence, code rates, Tanner graphs, etc., depend on the number of users in the system. Coordinated transmission and additional restrictions entail the complexity of the architecture of the multiple access network and communication protocols. Thus, classical multiple access systems turn out to be inapplicable for scenarios where short data packets are expected to be exchanged between a large number of users with limited computing resources (scenarios of mMTC and the Internet of Things). For these scenarios, it is required to develop special simple data exchange protocols that provide for the lack of coordination between devices.

It should also be noted that the development of multiple access systems must be accompanied by the development of asymmetric cryptography methods used to encrypt data in these systems. This is primarily due to the fact that when using a common communication channel, the user should not be able to read the information that another user sent to the base station. This prevents the transmission of the shared key that is used in symmetric encryption schemes and generally makes the use of symmetric ciphers difficult in this scenario. Therefore, to organize secure data transmission, an approach is more efficient when all users can use a single message encryption key, but only the base station has the ability to decrypt. Thus, we come to the methods of asymmetric cryptography.

Methods of error-correcting coding have long been used in cryptography. With their help, some of the first public-key cryptosystems [48] and digital signature systems [41] were built. However, in practice, code-based cryptosystems are used much less frequently than algebraic cryptosystems based on [60] factorization and [26] discrete logarithm problems. Although code cryptosystems outperform algebraic encryption/decryption in time [64], their use is largely limited by a number of objective and subjective factors.

Firstly, algebraic systems arose somewhat earlier than code-based systems and immediately went through numerous tests of their security. The latter circumstance is in the absence of evidence-based security of public-key cryptosystems a certain security guarantee.

Secondly, the first code-based cryptosystems (the McEliece system) were characterized by the presence of a public key that was significantly longer than for algebraic systems (for example, the RSA system).

Later, the research of code-based cryptosystems made it possible to significantly reduce the size of the public key [57], [11], and the development of new methods for solving the factorization problem [42] made it possible to increase the length of the public key of algebraic cryptosystems so that these values of public keys became comparable [16].

It should be noted that there is a common feature of all studies aimed at reducing the size of the public key in code-based cryptosystems. The essence of the improvements is that the original Goppa code is replaced by another class of codes that allow a more compact representation.

At the same time, the security of the McEliece cryptosystem and all such improvements is not based on the NP-hard problem of maximum likelihood decoding, since within the framework of the McEliece cryptosystem it is supposed to correct only errors with weight up to $d/2$, where d — minimum code distance. Such algorithms are called *decoding to half of the minimum distance* or *decoding HMD*. Note that it is not known whether decoding an HMD is NP-hard (or not). Some estimates of HMD decoding complexity can be found in [47], [24]. At the same time, there are no studies aimed at developing such cryptosystems in which the security of the scheme is determined not by low-weight error vector decoding (HMD), but by the complexity of maximum likelihood decoding.

Author's personal contribution

All results and provisions submitted for defense were obtained by the author personally.

Author has developed a concept for the synthesis of parity-check matrices for LDPC codes, that combines the use of some given algebraic structure with deterministic properties (minimal distance and properties associated with the structure of cycles in the Tanner graph) with circulant permutation matrices. Author analyzes the relationship between the minimum distance of such codes and the property of circulant matrices. Based on the obtained results, methods were proposed for choosing matrices of cyclic shifts that guarantee a strict increase of the minimum distance.

Analyzing the degree of elaboration of the problem of constructing efficient and low-resource algorithms for decoding of polar codes, the author proposed a new class of decoders that combine the approach with bit-flipping and fast list decoding of polar code subtrees.

Author proposes a new mathematical methodology for studying the error-correcting properties of convolutional codes, based on the spectrum of active distances, which made it possible to obtain analytical estimates of the distribution of error packet lengths at the output of the Viterbi decoder, as well as the error probability per block.

Author has developed a new model of data transmission in non-orthogonal multiple access systems based on a vector disjunctive channel and obtained an estimate of its capacity.

Author proposed a number of modifications of the original McEliece cryptosystem, the distinguishing feature of which is the reduction of the problem of decoding an encrypted message to the problem of decoding a linear code by maximum likelihood.

Personal contributions are also reflected in a sufficient number of publications in peer-reviewed and indexed publications in which the applicant is the main author.

Scientific novelty

In this dissertation, new constructions of LDPC codes are proposed. These code constructions are based on an approach that involves the simultaneous use of two constructions: a small matrix built by algebraic and/or combinatorial methods (base matrix) and permutation matrices that are used to obtain the required code length. In particular, Steiner triple systems, as well as repetition codes, are considered as algebraic constructions in this dissertation. Using this approach, it was possible to construct new families of high-rate (when using Steiner triple systems) and low-rate (when using a repetition code) codes that allow efficient storage and also show high efficiency (in terms of the error probability per block, depending on the signal-noise ratio) when they are decoded by the "belief propagation"algorithm. In addition, for regular LDPC codes, a new approach is proposed for estimating their error probability exponent during maximum likelihood decoding. This approach is based on the use of Hayman's theorem, which is used to find the roots of a polynomial by numerical methods.

A new mathematical apparatus for the study of convolutional codes is proposed. This approach is based on the concept of the spectrum of active distances. It is shown how the use of this apparatus allows estimating the distribution of error packet lengths at the output of the Viterbi decoder, as well as theoretically estimating the probability of an error per block when transmitting information through a binary symmetric channel without simulation of convolutional codes.

A new algorithm for decoding of Polar codes based on list decoding with bit-flipping and fast list decoding of some subcodes of Polar code is proposed. This algorithm is based on a new method for constructing a critical set (a set of information symbols, the inversion of which is most likely to lead to correct decoding), proposed in the dissertation work, a new method for constructing a critical set. It should be especially noted that this method of constructing a critical set is suitable for both vector (with subcode decoding) and symbolic decoding, and only the simplest operations are used in the calculations. The developed decoding algorithm is not inferior to the classical Tala-Vardi decoder, while its space and computational complexity is significantly lower.

A new method for organizing non-coordinated non-orthogonal multiple access is proposed, which is focused on the transmission of short data packets from multiple devices to a base station. For this method, estimates for the throughput are obtained, and it is also shown how the known constructions of interleaved binary codes and Reed-Solomon codes can be used to resolve collisions that occur during data transmission.

New designs of a public key cryptosystems have been developed. These constructions are based on the well-known McEliece cryptosystem which is based on the difficult task of decoding a linear code with an arbitrary structure. The approach to building this kind of cryptosystem is new — in contrast to existing approaches, the main idea of which is to replace the Goppa code with another code structure that allows to compactly describe the public key, the approach proposed in the thesis involves changing the structure of the public key. The main purpose of this change is to complicate the attack on information sets, which is considered one of the most effective for code-based cryptosystems. In the dissertation work, a number of cryptosystems based on the approach described above are proposed. In addition, a new scientific problem of searching for code structures for which it is possible to give a polynomial description of the set of correctable errors of weight greater than half the code distance is formulated. In addition, an efficient polynomial error correction algorithm from a given set is required.

All results obtained were new at the time of their publication.

Research methodology and methods

The dissertation research is based on the methodology of systems analysis and on the methods and theory of design telecommunication systems, theories of mathematical modeling, discrete mathematics, mathematical analysis, information theory, coding theory, probability theory and mathematical statistics.

Practical usefulness

The constructions of LDPC codes proposed in the thesis, decoding algorithms and constructions of critical set for Polar codes can be used in existing and future information transmission systems that use error-correcting codes. In particular, the use-cases may be: ultra-reliable low-latency communications (URLLC) or enhanced mobile broadband (eMBB). Both transmission scenarios are provided by the 5G mobile communication standard. In addition, the proposed algorithm for decoding of Polar codes, having a low delay, can claim to be implemented in promising communication standards for scenarios where the requirements for reliability and delay are decisive when choosing a code structure and its decoding algorithm.

The methods proposed in this work for evaluating the efficiency of LDPC codes and convolutional codes can be used in designing concatenated and generalized concatenated code structures in which the above schemes use as inner or outer codes. In particular, for generalized error locating codes (GEL codes currently used in some optical communication systems) [69], [28], [34] this will allow estimating the error probability for the entire scheme, without simulation.

The non-orthogonal multiple access methods proposed in the paper, as well as asymmetric cryptographic primitives, can be used to organize secure and reliable communication in information transmission systems where a large number of users does not allow efficient organization of orthogonal multiple access. An example of a concept involving a large number of devices and their non-orthogonal access to a joint communication channel is the Internet of Things, and the corresponding data transfer scenario is Massive Machine-to-Machine Communication (5G mMTC), which implies the presence of up to one million devices per square kilometer. In addition, the researchers note that the problem of security is one of the key risk factors for the widespread implementation of the Internet of Things [29], [17].

The following main results and provisions are submitted for defense:

1. The developed approach to the construction of LDPC codes, which is based on the joint use of some given algebraic structure (Steiner triple systems, repetition codes) with deterministic properties and permutation matrices, makes it possible to obtain ensembles of LDPC codes with a guaranteed minimum distance, which improves the performance of codes with a low probability of error.

2. The developed method for estimating the exponent of the error probability of regular LDPC codes, when decoding them by the maximum likelihood, makes it possible to build a lower bound on the probability of erroneous decoding of a given class of codes, thereby demonstrating their ”limiting” corrective properties.

3. The developed mathematical apparatus for studying the properties of convolutional codes, based on the spectrum of active distances, makes it possible to estimate the probability of erroneous decoding of convolutional codes in a binary symmetric channel for any input error probabilities without simulation.

4. The developed local erasure correction algorithm for convolutional codes, which reduces the erasure correction problem to solving a system of linear equations over a finite field, implements the potential correction properties of convolutional codes.

5. A fast algorithm for decoding polar codes based on the construction of a critical set of inversions of information symbols and fast list

decoding of some special subcodes of polar codes has the efficiency of a symbol-by-symbol list decoder, but at the same time has significantly less spatial and computational complexity.

6. The proposed method for organizing non-coordinated non-orthogonal multiple access in a disjunctive vector channel allows for non-coordinated transmission of short bursts of bits to a base station with a significantly higher bandwidth than slotted ALOHA.

7. Information protection methods based on the McEliece system, using modified public keys that make it difficult to analyze them using decoding by information sets, have significantly shorter public keys than in the original McEliece system.

Work approbation

The main results of the dissertation were reported at the following scientific conferences:

1. International conference IEEE International Conference on Communications (2018, Kanzas-City, USA). Topic - ”Signal-code construction based on interleaved reed-solomon codes for multiple access system over vector-disjunctive channel”;

2. International conference IEEE International Symposium on Information Theory and its Applications (2018, Singapore). Topic - ”Novel

signal-code construction for multiple access system over vector-disjunctive channel";

3. International conference IEEE International Symposium on Information Theory and its Applications (2020, online). Topic - "Theoretical Estimates of Burst Error Probability for Convolutional Codes";

4. International conference IEEE International Symposium on Information Theory and its Applications (2020, online). Topic - "Upper and Lower Estimates of Frame Error Rate for Convolutional Codes";

5. International conference 16th Canadian Workshop on Information Theory (2019, Gamilton, Canada). Topic - "On the performance of slotted vector-disjunctive channel";

6. International conference IEEE International Conference on Computer, Information and Telecommunication Systems (2019, Beijing, China). Topic - "On the Asymptotic Capacity of Slotted Multiple Access Channel";

7. International conference 1st International Workshop on Code-Based Cryptography (2020, online). Topic- "A new code-based cryptosystem";

8. International conference IEEE International Black Sea Conference on Communications and Networking (2018, Batumi, Georgia). Topic - "On the Maximal Achievable Rate for Signal-Code Construction

Based on Interleaved Reed-Solomon Codes for Multiple Access System Over Vector-Disjunctive Channel";

9. International conference IEEE International Black Sea Conference on Communications and Networking (2019, Sochi, Russia). Topic - "Signal-Code Construction Based on Codes on Gilbert-Varshamov Bound for Multiple Access System over Vector-Disjunctive Channel";

10. International conference 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (2019, Dublin, Ireland). Topic - "On the capacity estimation of a slotted multiuser communication channel";

11. International conference XVI International Symposium Problems of Redundancy in Information and Control Systems (2019, Moscow, Russia). Topic - "On the capacity estimation of a slotted multiuser communication channel with noise".

In addition, the main results of the dissertation were presented at the following seminars:

1. Seminar on coding theory. Institute for Information Transmission Problems Russian Academy of Sciences (Moscow, chaired by L.A. Bassalygo);

2. Seminar on coding theory and code-based cryptography. Skolkovo

Institute of Science and Technology (Skoltech) (Moscow, chaired by G.A. Kabatyansky);

3. Seminar ”Error-correcting codes and post-quantum cryptography” Institute of Electronics and Mathematics A. N. Tikhonov, National Research University Higher School of Economics (Moscow, chaired by - E. A. Krouk).

All proposed algorithms and methods were implemented in software, their behavior was studied by simulation methods, the results of which were compared with previously published ones.

List of published articles reflecting the main scientific findings of the dissertation

The author's publications in peer-reviewed scientific journals included in the international citation system Scopus:

1. Ivanov F., Miroshnik V., Krouk E. ”Improved Generalized Successive Cancellation List Flip Decoder of Polar Codes with Fast Decoding of Special Nodes” // Journal of Communications and Networks. — 2021. — V. 23. — P. 417—432.

2. A new code-based cryptosystem / F. Ivanov, E. Krouk, G. Kabatansky, N. Rumenko // Code-Based Cryptography Workshop. — Springer. 2020. — P. 41—49.

3. Ivanov F., Kreshchuk A., Zyablov V. On the local erasure correction

capacity of convolutional codes // 2018 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2018. — P. 296—300.

4. Ivanov F., Rybin P. Novel Signal-Code Construction for Multiple Access System over Vector-Disjunctive Channel // 2018 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2018. — C. 560—564.

5. Ivanov F., Rybin P. Signal-Code Construction Based on Interleaved Reed-Solomon Codes for Multiple Access System over Vector-Disjunctive Channel // 2018 IEEE International Conference on Communications Workshops (ICC Workshops). — IEEE. 2018. — P. 1—5.

6. Ivanov F., Rybin P. On the Asymptotic Capacity of Slotted Multiple Access Channel // 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). — IEEE. 2019. — P. 1—5.

7. Ivanov F., Rybin P., Afanassiev V. On the Performance of Slotted Vector-Disjunctive Channel // 2019 16th Canadian Workshop on Information Theory (CWIT). — IEEE. 2019. — P. 1—5.

8. On the Capacity Estimation of a Slotted Multiuser Communication Channel / F. Ivanov, A. Kreschuk, V. Afanassiev // 2019 11th International Congress on Ultra Modern Telecommunications and

Control Systems and Workshops (ICUMT). — IEEE. 2019. — P. 1—5.

9. On the Capacity Estimation of a Slotted Multiuser Communication Channel with Noise / F. Ivanov, A. Kreschuk, V. Afanassiev, P. Rybin // 2019 XVI International Symposium"Problems of Redundancy in Information and Control Systems"(REDUNDANCY). — IEEE. 2019. — P. 27—31.

10. Rybin P., Ivanov F. On estimation of the error exponent for finite length regular graph-based ldpc codes // Journal of Communications Technology and Electronics. — 2018. — V. 63, no. 12. — P. 1518—1523.

11. Smeshko A., Ivanov F. Signal-Code Construction Based on Codes on Gilbert-Varshamov Bound for Multiple Access System over Vector Disjunctive Channel // 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). — IEEE. 2019. — P. 1—3.

12. Smeshko A., Ivanov F., Zyablov V. Theoretical Estimates of Burst Error Probability for Convolutional Codes // 2020 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2020. — P. 136—140.

13. Smeshko A., Ivanov F., Zyablov V. Upper and Lower Estimates of

Frame Error Rate for Convolutional Codes // 2020 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2020. — P. 160—164.

14. Ivanov F. I. A Special Class of Quasi-Cyclic Low-Density Parity-Check Codes Based on Repetition Codes and Permutation Matrices // Problems of Information Transmission. — 2017. — V. 53, №3. — P. 229—241.

15. Ivanov F. I., Zyablov V. V. Low-Density Parity-Check Codes Based on Steiner Triple Systems and Permutation Matrices. // Problems of Information Transmission. — 2013. — V. 49, №4. — P. 333—347.

16. Ivanov F. I., Zyablov V. V., Krouk E. A., Sidorenko V. R. On New Problems in Asymmetric Cryptography Based on Error-Correcting Codes. // Problems of Information Transmission. — 2022. — V. 58, №2. — P. 92— 111.

17. Smeshko A. A., Ivanov F. I., Zyablov V. V. Theoretical and Experimental Upper and Lower Estimates for the Efficiency of Convolutional Codes in a Binary Symmetric Channel. // Problems of Information Transmission. — 2022. — V. 58, №2. — P. 24—40.

Author's publications in other journals:

18. Estimate of the Capacity of a Multiuser Vector Disjunctive Channel for Arbitrary Input Distributions / V. S. Dyrenkov, N. M. Shevel,

F. I. Ivanov, A. A. Kreschuk // Information Processes. — 2020. — V. 20, №2. — P. 133—141.

General conclusions of the research

1. The proposed constructions of LDPC codes based on the general approach - the joint use of some given algebraic structure with deterministic properties (minimal distance and properties associated with the structure of cycles in the corresponding Tanner graph) and permutation matrices used to obtain codes of the required length, allow us to obtain long codes with a given estimated minimum distance, which suggests a fairly low ”error-floor” level. At the same time, the correction capacity of the obtained codes are not inferior to LDPC codes, which are based on optimization by the density evolution method or P-EXIT charts. At the same time, the algebraic approach used in the construction of codes makes it possible to optimize the procedures for storing of parity-check matrices.

2. The approach proposed in the research, which makes it possible to estimate the error probability exponent of regular LDPC codes when decoding these codes by the maximum likelihood, allows us to conclude that, despite the widespread practical use of LDPC codes in applications, their potential correction capacity characteristics are inferior to arbitrary binary codes.

3. The mathematical apparatus proposed in the research for studying the error correction capacity of convolutional codes, based on the spectrum of active distances, made it possible to obtain analytical estimates of the distribution of error packet lengths in the output of the Viterbi decoder, as well as the error probabilities per block. On the basis of the study, it can be concluded that the analytical method proposed in the dissertation work for estimating the performance of convolutional codes makes it possible to obtain accurate values of the error probability per block at low input error probabilities, for which it is difficult to obtain results by simulation. In this case, the proposed method has linear complexity in the code length and does not depend on the error probability of the channel.

4. Based on the analysis of the new criterion for constructing a critical set proposed for Polar codes, which is used as part of a list decoder based on bit-flipping, a class of metrics was obtained that allow both symbolic and vector calculations. In particular, it was shown how the obtained method for constructing a critical set can be extended to the case of generalized list decoding of Polar codes, where at each stage, instead of symbolic decision, a decision is made immediately on a group of symbols that form an easily decodable subcode of Polar code. Studies of the generalized bit-flipping list decoder developed on the basis of the proposed metric have shown that both the symbolic and generalized decoders based on the new

metric are not inferior in their performance to the best Polar code decoders to date, while having significantly less implementation complexity.

5. Studies of a new data transmission model in non-orthogonal multiple access systems based on a vector disjunctive channel and estimation of its capacity have shown that the efficiency of the proposed transmission model is significantly higher than that of the slotted ALOHA model.

6. The problem of resolving collisions that arise when transmitting data from a group of users to a base station in the proposed channel model was formulated. Studies of the properties of codes that can be used to resolve collisions have revealed the advantages of using interleaved binary and non-binary codes compared to classical binary and non-binary codes without interleaving. At the same time, the error-correction capacity of the proposed code structures are significantly inferior to the potential one of codes that lie on the limit of the capacity of a disjunctive vector channel.

7. A number of modifications of the original McEliece cryptosystem were proposed, the main feature and distinguishing feature of which is that, in contrast to the classical approach, where the Goppa code is replaced by another class of codes that allow a compact description of the public key, in this dissertation it is proposed

to modify the the structure of the public and private keys, which leads to the fact that in order to extract information about the encrypted message, it is necessary to solve the decoding problem in code coset, which, in other words, is equivalent to searching for an error vector that has not the smallest possible weight. An analysis of the properties of the developed cryptosystems showed that the most effective method of attacking the classical McEliece cryptosystem - information set decoding — is inapplicable to them. In view of this, it is possible to significantly reduce the length of the public key while maintaining a given level of security of the cryptosystem.

References

1. 5G: A tutorial overview of standards, trials, challenges, deployment, and practice / M. Shafi [и др.] // IEEE journal on selected areas in communications. — 2017. — Т. 35, № 6. — С. 1201—1221.
2. A survey on mobile WiMAX [wireless broadband access] / B. Li [и др.] // IEEE Communications magazine. — 2007. — Т. 45, № 12. — С. 70—75.
3. A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends / Z. Ding [и др.] // IEEE Journal on Selected Areas in Communications. — 2017. — Т. 35, № 10. — С. 2181—2195.
4. A technique to evaluate an exact formula for the bit error rate of convolutional codes in case of finite length words / F. Chiaraluce [и др.] // TENCON'97 Brisbane-Australia. Proceedings of IEEE TENCON'97. IEEE Region 10 Annual Conference. Speech and Image Technologies for Computing and Telecommunications (Cat. No. 97CH36162). Т. 1. — IEEE. 1997. — С. 113—116.
5. A tutorial on IEEE 802.11 ax high efficiency WLANs / E. Khorov [и др.] // IEEE Communications Surveys & Tutorials. — 2018. — Т. 21, № 1. — С. 197—216.

6. *Abramson N.* The ALOHA system: Another alternative for computer communications // Proceedings of the November 17-19, 1970, fall joint computer conference. — 1970. — С. 281—285.

7. *Afisiadis O.*, *Balatsoukas-Stimming A.*, *Burg A.* A low-complexity improved successive cancellation decoder for polar codes // 2014 48th Asilomar Conference on Signals, Systems and Computers. — IEEE. 2014. — С. 2116—2120.

8. *Ahamed M. M.*, *Faruque S.* 5G backhaul: requirements, challenges, and emerging technologies // Broadband Communications Networks: Recent Advances and Lessons from Practice. — 2018. — Т. 43.

9. *Akyildiz I. F.*, *Wang X.* A survey on wireless mesh networks // IEEE Communications magazine. — 2005. — Т. 43, № 9. — S23—S30.

10. *Alamdar-Yazdi A.*, *Kschischang F. R.* A simplified successive-cancellation decoder for polar codes // IEEE communications letters. — 2011. — Т. 15, № 12. — С. 1378—1380.

11. Algebraic cryptanalysis of McEliece variants with compact keys / J.-C. Faugere [и др.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2010. — С. 279—298.

12. An overview of the ATSC 3.0 physical layer specification / L. Fay [и др.] // IEEE Transactions on Broadcasting. — 2016. — Т. 62, № 1. — С. 159—171.

13. An overview of turbo codes and their applications / C. Berrou [и др.] // The European Conference on Wireless Technology, 2005. — IEEE. 2005. — С. 1—9.

14. Application of non-orthogonal multiple access in LTE and 5G networks / Z. Ding [и др.] // IEEE Communications Magazine. — 2017. — Т. 55, № 2. — С. 185—191.

15. *Arikan E.* Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels // IEEE Transactions on Information Theory. — 2009. — Т. 55, № 7. — С. 3051—3073.

16. *Barker E.*, *Dang Q.* Nist special publication 800-57 part 1, revision 4 // NIST, Tech. Rep. — 2016. — Т. 16.

17. *Bekara C.* Security issues and challenges for the IoT-based smart grid // Procedia Computer Science. — 2014. — Т. 34. — С. 532—537.

18. *Berrou C.*, *Glavieux A.* Near optimum error correcting coding and decoding: Turbo-codes // IEEE Transactions on communications. — 1996. — Т. 44, № 10. — С. 1261—1271.

19. Bit-flip algorithm for successive cancellation list decoder of polar codes / F. Cheng [и др.] // IEEE Access. — 2019. — Т. 7. — С. 58346—58352.

20. *Bolton W.*, *Xiao Y.*, *Guizani M.* IEEE 802.20: mobile broadband wireless access // IEEE Wireless Communications. — 2007. — Т. 14, № 1. — С. 84—95.

21. *Buranapanichkit D.*, *Andreopoulos Y.* Distributed time-frequency division multiple access protocol for wireless sensor networks // IEEE wireless communications letters. — 2012. — Т. 1, № 5. — С. 440—443.

22. *Cover T.* An achievable rate region for the broadcast channel // IEEE Transactions on Information Theory. — 1975. — Т. 21, № 4. — С. 399—404.

23. *Dahlman E.*, *Parkvall S.*, *Skold J.* 4G: LTE/LTE-advanced for mobile broadband. — Academic press, 2013.

24. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding / A. Becker [и др.] // Annual international conference on the theory and applications of cryptographic techniques. — Springer. 2012. — С. 520—536.

25. *Dielissen J.*, *Hekstra A.*, *Berg V.* Low cost LDPC decoder for DVB-S2 // Proceedings of the Design Automation & Test in Europe Conference. Т. 2. — IEEE. 2006. — С. 1—6.

26. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE transactions on information theory. — 1985. — Т. 31, № 4. — С. 469—472.

27. *Elias P.* Coding for noisy channels // IRE Conv. Rec. — 1955. — Т. 3. — С. 37—46.

28. Encoding and decoding methods using generalized concatenated codes (GCC) / X. Yang [и др.]. — Авг. 2010. — US Patent 7,782,232.

29. Evaluating critical security issues of the IoT world: Present and future challenges / M. Frustaci [и др.] // IEEE Internet of things journal. — 2017. — Т. 5, № 4. — С. 2483—2495.

30. Fast polar decoders: Algorithm and implementation / G. Sarkis [и др.] // IEEE Journal on Selected Areas in Communications. — 2014. — Т. 32, № 5. — С. 946—957.

31. Finite-length analysis of low-density parity-check codes on the binary erasure channel / C. Di [и др.] // IEEE Transactions on Information theory. — 2002. — Т. 48, № 6. — С. 1570—1579.

32. *Gallager R.* Low-density parity-check codes // IRE Transactions on information theory. — 1962. — Т. 8, № 1. — С. 21—28.

33. *Gamage H.*, *Rajatheva N.*, *Latva-Aho M.* Channel coding for enhanced mobile broadband communication in 5G systems // 2017 European conference on networks and communications (EuCNC). — IEEE. 2017. — С. 1—6.

34. Gel codeword structure encoding and decoding method, apparatus, and related device / A. E. Maevskii [и др.]. — Дек. 2020. — US Patent 10,879,937.

35. *Giard P.*, *Burg A.* Fast-SSC-flip decoding of polar codes // 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). — IEEE. 2018. — С. 73—77.

36. *Hanif M.*, *Ardakani M.* Fast successive-cancellation decoding of polar codes: Identification and decoding of new nodes // IEEE Communications Letters. — 2017. — Т. 21, № 11. — С. 2360—2363.

37. *Hara S.*, *Prasad R.* Overview of multicarrier CDMA // IEEE communications Magazine. — 1997. — Т. 35, № 12. — С. 126—133.

38. *Hashemi S. A.*, *Condo C.*, *Gross W. J.* Simplified successive-cancellation list decoding of polar codes // 2016 IEEE International Symposium on Information Theory (ISIT). — IEEE. 2016. — С. 815—819.

39. *Herro M.*, *Hu L.*, *Nowack J.* Bit error probability calculations for convolutional codes with short constraint lengths on very noisy channels // IEEE Transactions on Communications. — 1988. — Т. 36, № 7. — С. 885—888. — DOI: 10.1109/26.2819.

40. Interleave division multiple-access / L. Ping [и др.] // IEEE transactions on wireless communications. — 2006. — Т. 5, № 4. — С. 938—947.

41. *Kabatianskii G.*, *Krouk E.*, *Smeets B.* A digital signature scheme based on random error-correcting codes // IMA International Conference on Cryptography and Coding. — Springer. 1997. — С. 161—167.

42. *Kocher P. C.* Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Annual International Cryptology Conference. — Springer. 1996. — С. 104—113.

43. *Li S.*, *Da Xu L.*, *Zhao S.* 5G Internet of Things: A survey // Journal of Industrial Information Integration. — 2018. — Т. 10. — С. 1—9.

44. Low-complexity LDPC decoder for 5G URLLC / J.-C. Liu [и др.] // 2018 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia). — IEEE. 2018. — С. 43—46.

45. Low-rate PBRL-LDPC codes for URLLC in 5G / X. Wu [и др.] // IEEE Wireless Communications Letters. — 2018. — Т. 7, № 5. — С. 800—803.

46. *MacKay D. J.* Good error-correcting codes based on very sparse matrices // IEEE transactions on Information Theory. — 1999. — Т. 45, № 2. — С. 399—431.

47. *May A.*, *Meurer A.*, *Thomae E.* Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$ // International Conference on the Theory and Application of Cryptology and Information Security. — Springer. 2011. — С. 107—124.

48. *McEliece R. J.* A public-key cryptosystem based on algebraic // Coding Thv. — 1978. — Т. 4244. — С. 114—116.

49. *Myung H. G.*, *Lim J.*, *Goodman D. J.* Single carrier FDMA for uplink wireless transmission // IEEE Vehicular Technology Magazine. — 2006. — Т. 1, № 3. — С. 30—38.

50. *Nelson R.*, *Kleinrock L.* Spatial TDMA: A collision-free multihop channel access protocol // IEEE Transactions on communications. — 1985. — Т. 33, № 9. — С. 934—944.

51. *Niu K.*, *Chen K.* CRC-aided decoding of polar codes // IEEE Communications Letters. — 2012. — Т. 16, № 10. — С. 1668—1671.

52. *Noor-A-Rahim M.*, *Nguyen K. D.*, *Lechner G.* Finite length analysis of LDPC codes // 2014 IEEE Wireless Communications and Networking Conference (WCNC). — IEEE. 2014. — С. 206—211.

53. On the performance of polar codes for 5G eMBB control channel / S. A. Hashemi [и др.] // 2017 51st Asilomar Conference on Signals, Systems, and Computers. — IEEE. 2017. — С. 1764—1768.

54. Optimal decoding of linear codes for minimizing symbol error rate (corresp.) / L. Bahl [и др.] // IEEE Transactions on information theory. — 1974. — Т. 20, № 2. — С. 284—287.

55. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges / S. R. Islam [и др.] // IEEE Communications Surveys & Tutorials. — 2016. — Т. 19, № 2. — С. 721—742.

56. Protograph-based raptor-like LDPC codes / T.-Y. Chen [и др.] // IEEE Transactions on Communications. — 2015. — Т. 63, № 5. — С. 1522—1532.

57. Reducing key length of the McEliece cryptosystem / T. P. Berger [и др.] // International Conference on Cryptology in Africa. — Springer. 2009. — С. 77—97.

58. *Richardson T.*, *Urbanke R.* Finite-length density evolution and the distribution of the number of iterations for the binary erasure channel // unpublished.[Online]. Available: http://lthcwww. epfl. ch/RiU02. ps. — 2003.

59. *Rimoldi B.*, *Urbanke R.* A rate-splitting approach to the Gaussian multiple-access channel // IEEE Transactions on Information Theory. — 1996. — Т. 42, № 2. — С. 364—375.

60. *Rivest R. L.*, *Shamir A.*, *Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. — 1978. — Т. 21, № 2. — С. 120—126.

61. *Tal I.*, *Vardy A.* List decoding of polar codes // Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on. — IEEE. 2011. — С. 1—5.

62. *Tsatsaragkos I.*, *Paliouras V.* A reconfigurable LDPC decoder optimized for 802.11 n/ac applications // IEEE Transactions on Very Large

Scale Integration (VLSI) Systems. — 2017. — Т. 26, № 1. — С. 182—195.

63. Use cases and scenarios of 5G integrated satellite-terrestrial networks for enhanced mobile broadband: The SaT5G approach / K. Liolis [и др.] // International Journal of Satellite Communications and Networking. — 2019. — Т. 37, № 2. — С. 91—112.

64. *Véron P.* Code based cryptography and steganography // International Conference on Algebraic Informatics. — Springer. 2013. — С. 9—46.

65. *Viterbi A.* Error bounds for convolutional codes and an asymptotically optimum decoding algorithm // IEEE transactions on Information Theory. — 1967. — Т. 13, № 2. — С. 260—269.

66. *Yoshikawa H.* Theoretical analysis of bit error probability for punctured convolutional codes // 2012 International Symposium on Information Theory and its Applications. — 2012. — С. 658—661.

67. *Yuan Y.*, *Zhao X.* 5G: Vision, scenarios and enabling technologies // ZTE communications. — 2015. — Т. 13, № 1. — С. 3—10.

68. *Zhang J.*, *Orlitsky A.* Finite-length analysis of LDPC codes with large left degrees // Proceedings IEEE International Symposium on Information Theory, — IEEE. 2002. — С. 3.

69. *Zhilin I.*, *Kreshchuk A.*, *Zyablov V.* Generalized error-locating codes and minimization of redundancy for specified input and output

error probabilities // Journal of Communications Technology and Electronics. — 2015. — T. 60, № 6. — C. 695—706.