Enhancing information transmission security with stochastic codes

Bohdan Zhurakovskyi[1,†], Sergei Otrokh[1,†], Mykhailo Poliakov[2,†], Oleksii Poliakov[2,†] and Pavlo Skladannyi[3,*,†]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," 37 Peremogy ave., 03056 Kyiv, Ukraine*
[2] *National University "Zaporizhzhia Polytechnic," 64 Zhukovsky str. 69063 Zaporizhzhia, Ukraine*
[3] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

All known algorithms of cryptographic systems, which have the property of interference resistance, are based on codes that detect and correct errors. This work proposes a study of stochastic codes for their potential use in cryptographic system algorithms. For stochastic codes, there is a "copy" decoding algorithm when two or more values of a code block of a stochastic code, including $(n, n–1)$ is a code with the detection of errors that are the same during their transmission, it is possible to carry out joint decoding of the extended code with bug fixes. Furthermore, the number of errors that can be corrected in a single block of the extended code is significantly higher than the total number of errors that can be corrected in each block. To simplify the comparative analysis, we converted the given value P_q to the probability of flipping the binary symbol P_0. We estimated this probability for different degrees of error grouping using the Portov model with the coefficient a.

Keywords

stochastic code, cryptographic protection, probabilities of distortion in the channel, error-correcting codes, error bursts, decoding mode

1. Introduction

The introduction of modern information technologies into the everyday life of society has caused problems in ensuring information security [1, 2]. One of the solutions to this problem is the widespread use of cryptography [3, 4]. At the moment, strict technological requirements are imposed on cryptographic algorithms not only in terms of stability but also in terms of speed [5].

The need to maintain the high performance of automated systems after protection mechanisms are implemented has led to increased speed requirements. Ease of hardware implementation is necessary to reduce the cost of encryption tools, which will contribute to their mass application and wider possibilities of embedding in portable equipment. Given the specific way that information is presented in digital devices, blockciphersare of particular interest.

Their problem oriented use in the devices and systems mentionedabovecanprovide effective protection against cyberthr eats. Thus, the development of problem-oriented encryption systems is an important and urgent task of applied cryptography [6]. Codes that detect and correct errors are the backbone of all known cryptographic systems that possess interference resistance properties [7].

The best-known public-key cryptosystem based on algebraic coding theory is McEliece's cryptosystem based on a class of error-correcting codes called Goppa codes. The basic idea is to create a Goppa code and disguise it as a regular linear code. There is a fast algorithm for decoding Goppa codes, but the general problem of finding codewords of this weight in a linear binary code is an NP-complete task [8].

Analysis of the crypto resistance of this algorithm indicates that to ensure reliable protection of information, the in imum parameter values required are $n = 1024$ and $k = 524$. The protected properties of the algorithm are contingent on the parameter t, which must be chosen such that $t>50$. This value is optimal for channels because the error probability is only 10^{-4} [8]. For reliable cryptographic protection, it is necessary to obtain the decoding complexity that would meet modern cryptographic standards (of the order of 250). To ensure there is required decoding complexity in the analyzed cryptosystem, it's necessary to use 750-800 columns in the check matrix of the Goppa code [9].

As can be seen from the above analysis, meeting the necessary limit requirements for system parameters ensures fairly reliable cryptographic protection of

CQPC-2024: Classic, Quantum, and Post-Quantum Cryptography, August 6, 2024, Kyiv, Ukraine

[*] Corresponding author.
[†] These authors contributed equally.

✉ zhurakovskybiyu@tk.kpi.ua (B. Zhurakovskyi); 2411197@ukr.net (S. Otrokh); polyakov@zntu.edu.ua (M. Poliakov); poliakov.job@gmail.com (O. Poliakov); p.skladannyi@kubg.edu.ua (P. Skladannyi)

0000-0003-3990-5205 (B. Zhurakovskyi); 0000-0001-9008-0902 (S. Otrokh); 0000-0002-7772-3122 (M. Poliakov); 0000-0002-9355-7056 (O. Poliakov); 0000-0002-7775-6039 (P. Skladannyi)

information. For instance, the durability of McEliece's system is.

Demonstrated by the fact that despite multiple tempts to cryptanalysis, none of them have been successful. Despite their interference resistance, several coding algorithms used for detecting and correcting errors introduce artificial information redundancy [10]. This can be a major drawback of interference-resistant codes. This circuit stance leads to a significant increase in the ciphered text compared to the original (in the McEliece system, by a fact or two). Furthermore, the public key in the MacEliece and Niederreiter systems is quite large by modern standards, at 219 bits [11].

Jam-resistant crypto-algorithms shave high requirements for hardware [12], speed [13], memory, and security. These requirements depend on the properties of the applied code algorithms that use artificial redundancy.

2. Statement of research problem

2.1. Self-resistant coding in transmission channels

The main works of C. Shannon [14], in which the tasks of interference-resistant information transmission with any predetermined accuracy of information transmission are formulated, proposes to use the principle of randomness of the used signals as a solution to these tasks. For interference-resistant information transmission, it is proposed to use random (n, k)-codes, formed by randomly selecting from $2n$ possible binary combinations of length n $2k$ combinations, each of which is identified with one of the information combinations of length k. Using this model of signals for transmission over a communication channel, C. Shannon proved a theorem about the possibility of transmitting information over a communication channel with a probability of error that depends on the parameters n and k, and which can be made arbitrarily small by choosing the appropriate values for these parameters. The proof of this theorem was of fundamental importance for the creation of the theory of interference-resistant coding, although it did not give constructive suggestions about the implementation of such a possibility [15].

In practice, a relatively small group of algebraic interference-resistant codes is used: Bowes-Choudhury-Hockingham (BCH) codes, Reed-Solomon (RS) codes, and convolutional codes. The most widely used cyclic codes with error detection, are a partial case of BCH codes and are used in standard X.25/2 protocols (LAP-B, LAP-M). RS codes with error correction in radio communication channels are being used. Convolutional codes are widely used in satellite communication channels, which are characterized by the independent nature of errors. Codes with error correction are not widely used due to the complexity of implementing error correction, and the high dependence of the probability of a decoding error on the law of error distribution.

In the works on information theory and interference-resistant coding, written in the 70s, codes with error correction were considered. First, codes based on C. Shannon's random codes, then algebraic codes. This is explained by the achievement of higher characteristics when transmitting information with error-correcting codes, compared to the currently widely used error-detecting codes. The transition from correction codes to error detection codes can be explained by several main reasons:

- Firstly, the greater computational complexity of implementing an error-correcting codec.
- Secondly, the need to match the type and parameters of the error-correcting code with the conditions of information transmission, that is the intensity and distribution law of errors in the used communication channel.
- Thirdly, the use of, as a rule, high-quality channels, a high degree of development of the necessary technical solutions for the implementation of the cyclic code in the developed microcircuits for connection with communication channels produced by several companies and the standardization of channel-level protocols, which include the implementation of the cyclic code [14].

Therefore, to consider the alternative of using codes with error correction, it is worth looking for significant reasons for such a transition. Let's formulate the properties of error-proof code with error correction that allow us to talk about such an alternative, and then consider a possible option for building and using such a code. So, such code should have the properties:

- The code has error detection and error correction modes, providing in both modes a guaranteed (predetermined) probability of decoding with an error in an arbitrary communication channel and a reliable rejection of decoding when the error cannot be corrected.
- The code has such a correcting ability and allows you to choose such parameters n and k that the information transmission algorithm that uses them is characterized by no worse probabilistic-temporal characteristics in comparison with the use of alternative codes.
- The code provides, in the error correction mode, the selection of a part of the correctly received symbols with a specified accuracy, even if the error multiplicity exceeds the code's correction ability.
- The code allows you to decode several copies (identical in terms of the information content of the code blocks) of the block with an efficiency that exceeds the efficiency of decoding the source code with the detection or correction of errors. This property can be used to work in parallel channels when multiple transmissions of a message on a single channel or in a channel with feedback when processing copies after receiving a repeated block.
- Code encoding and decoding procedures contain only modulo two operations.
- The coding method should have properties of the randomness of signals at the encoder output, which provide a joint solution to the problems of

ensuring interference resistance in C. Shannon's formulation.

The implementation of such a statement of the task will allow:

- To expand the spectrum of used communication channels according to the permissible level of channel quality due to the use of channels of reduced quality.
- Ensuring the guaranteed probability of the level specified by the consumer (10- 9, 10-18, 10-27) in case of any type of distortion in the communication channel.
- To remove the problem of accuracy (probability) of information when creating global hyper-informational spaces under the condition of information transmission via almost any communication channels.
- To ensure a return to C. Shannon's classic statement in solving the problems of interference resistance but within the framework of a single information transformation algorithm.

Interference-resistant coding is effective among the known methods of increasing the reliability of message reception, but its use in a complex interference environment caused by the active influence of radio-electronic warfare means is limited because in such conditions it can lead to an increase in the number of errors at the decoding stage (the effect of error multiplication) [16]. In this case, it is advisable to use the majority coding principle, which allows you to avoid the effect of multiplying errors.

The majority principle consists of the fact that an odd number of times the same message is sent to the channel, and on the receiving side, code combinations of the same name (or binary digits of the same name) are compared with each other. At reception, the code combination (or bit) that has been received the most number of times is chosen [17].

The disadvantage of majority coding is the redundancy of information, which increases in proportion to the number of repetitions of the same message (bit), therefore, when using it, it is necessary to take into account the time limits on the transmission of messages.

It is worth noting that for telemetry systems, monitoring of remote objects, control systems of unmanned aerial vehicles, and other special purpose systems, in addition to increasing the reliability of information reception, an especially important task is to ensure the information confidentiality of message transmission. One of the approaches that allows solving such tasks is the use of Combined Random Coding (CRC) [18].

The method of combined random coding, which is proposed in [19], involves the use of a combination of interference-resistant coding and a pseudo-random change of the ensemble of code combinations—stochastic coding of information. At the same time, high reliability of message transmission is ensured due to tamper-resistant coding, and information secrecy and protection against unauthorized access—due to coding, which refers to non-cryptographic methods of information protection. With CRC, the information-theoretic level of information protection is provided, which is determined by the level of uncertainty of the choice of an ensemble of code combinations corresponding to the transmitted message, for an attacker who carries out radio interception [20].

2.2. Construction and properties of error-correcting stochastic codes

In the 1980s, work was started on the creation of a new design of codes that fit into the structure of existing data transmission networks, to increase the technical and economic effect when transmitting information through communication channels of different quality [21]. The work resulted in the creation of designs and algorithms for coding and decoding *q* stochastic codes with error correction. These codes are based on the formation of binary codes for communication channels of varying quality [22].

The following estimates are valid for these codes, confirmed by theoretical studies and test statistics of practically implemented complexes [23]:

a) the code provides a predetermined probability (guaranteed probability of a decoding error) both when detecting and when correcting errors, related to the selected length of the *q*-symbol and the allowed number of corrected errors and relative to the maximum possible number of corrected errors *t* associated with the code distance of the original binary code *d*,

$$t = d - 2 \qquad (1)$$

This property can be used in duplex and simplex communication channels.

b) in a system with feedback [15], which employs a duplex data transmission channel, the error correcting code provides the following benefits (see the tables below):

- An increase in the relative (effective) speed of information transmission, in comparison with the use of error-detecting codes, in the entire range of possible channel quality (that is, always) [24].
- A higher probability of successful decoding of the code block in case of error correction, about the error detection mode; at the same time, the data transmission channel acquires the properties of a real-time channel ("tempo" channel) [25], where information is transmitted with a much smaller number of repetitions, which maximally satisfies the requirements for combining data transmission and speech in one channel (digital speech transmission is critical to repetitions) [26].

c) the encoder output signal has the character of "white noise," because not one randomly selected (*n, k*) code is used, but an ensemble of codes, where a code change occurs at each successive code block [27].

d) in the presence of two or more values in the receiver that are a priori the same before coding on the transmitting side of the code blocks (first transmission and repetition on request in the feedback system or multiple transmission of the block in single-channel and multi-channel simplex systems—"copies" of blocks) there are algorithms for decoding copies that make it possible to significantly increase the reliability of message delivery in conditions of intense interference in communication channels [27].

As a result, it is claimed that the considered construction of codes has a scope that coincides with the scope of the application of information systems and telecommunications technology in general.

Below are the main properties of error-correcting stochastic codes with a guaranteed probability of a decoding error [28].

The code base is selected $q = 2^{32}$, which means, the binary length of the q-symbol is 32 bits, and the number of such symbols in the block is n and k.

The probability of an error [29] in decoding stochastic q-codes does not depend on the type and nature of distortions and is mainly related to the value of q as in the error detection mode (n, n-1)—code (with one redundant symbol), and in error correction mode [30]. With the selected base q, the probability of an error after decoding does not exceed any type of twists

$$P_{errors} < q^{-1} = 2^{-32} < 10^{-9} \qquad (2)$$

The number of corrected errors t is related to the code distance d of the original binary code by the ratio $t = d$-2 and approximately corresponds to the number of corrected errors of the Reed-Solomon code with the same parameters n and k [31].

Note that these codes correct errors in a probabilistic sense. Specifically, errors are always corrected in multiples of 1 (when the 1 q-symbol is twisted), while errors in multiples of 2 or more are corrected with a controlled probability that depends on the code. It is important to note that decoding errors or failures are still possible, but in practical implementation, these probabilities can be reduced to desired values. The decoding and encoding of the stochastic codes use only binary operations with q-symbols [32, 33]. Since the number of decoding operations does not depend on q, as q increases, the number of operations per 1 bit of transmitted information decreases [34]. The number of decoding operations with error correction per block of q-code can be of the order of magnitude of b_n binary operations with length operands

$$L = -\log q, (L = 32), \qquad (3)$$

where the coefficient b = 5–10. In the calculation of 1 bit of transmitted information, the number of operations decreases by L times and has a value of less than 1 op/bit [35]. In the error detection mode for (n, n–1) q-code, the number of encoding and decoding operations is minimal and is n binary operations with operands of length L [36]. That is, for the code (16, 15) at q=232, the number of binary encoding (decoding) operations is 16 per block of length 16×32 = 512 bits.

The probability of successful decoding of the code block ($P_r(1)$) from the first transmission and the effective speed [37] can be calculated using the following formula:

$$R_{ef} = \frac{k * N_r}{n * N_t} \qquad (4)$$

where N_r and N_t are the number of received and transmitted blocks, respectively.

For stochastic codes, there is a "copy" decoding algorithm, when for two or more values of a code block of a stochastic code, including (n, n–1)—a code with the error detection that is the same during their transmission, it is possible to carry out joint decoding of the extended code with error correction [35, 36]. At the same time, the number of errors corrected in the block of the extended code significantly exceeds the number of errors corrected in total in each block [38, 39], for example, if the source code corrects t = 2 errors, then when the source block is repeated 2 times in an extended block, at least 6 twisted q-symbols are corrected, with three repetitions—at least 10 symbols, etc. At the same time, the guarantee of the reliability of the decoded information is preserved [40].

The copy decoding mode is most promising in simplex radio channels, particularly those with low-quality communication channels and intense radio interference. It is also effective in duplex channels that employ joint decoding of previously decoded and repeated blocks [41]. The temporal (or pace) characteristics of the code depend on two factors: the effective transmission speed R_{ef} and the probability of the block being successfully delivered in the first (or subsequent) transmission [42].

2.3. Comparative characteristics of stochastic codes with error correction, and obtained results of hardware and software tests

We conducted bench tests of stochastic codes using a software simulator of communication channel errors. The results of the set tests are presented in Tables 1, 2, and 3.

Table 1
The results of bench tests of stochastic codes obtained using a software simulator of communication channel errors

	Code			
	P$_q$	P$_0$		
		α = 0	α = 0,3	α = 0,5
Channel quality	1/2	0,02142	0,05942	0,11532
	1/4	0,00895	0,02511	0,04958
	1/8	0,00416	0,01173	0,02332
	1/16	0,0020	0,0057	0,0113
	1/32	0,0009	0,0028	0,0056
	1/64	0,0005	0,0014	0,0028
	1/128	0,00025	0,00069	0,00139

During the tests, different values of the probability of twisting in the q-symbol channel (P_q) were used. The values were chosen randomly and ranged from once every two symbols (1/2) to once every four symbols (1/4), and soon. To simplify the comparative analysis, we estimated the probability of twisting the binary symbol (P_0) for different degrees of error grouping based on the given value of P_q. We used the Purtov model with the coefficient "a" to estimate this probability. Specifically, we considered three different values of "a": 0 for independent errors, 0.3 for weak grouping in the leading channel, and 0.5 for strong grouping in the radio channel.

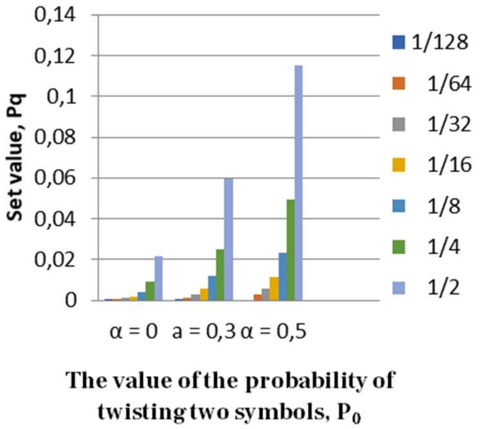

Figure 1: Channel quality for different degrees of error grouping with coefficient α

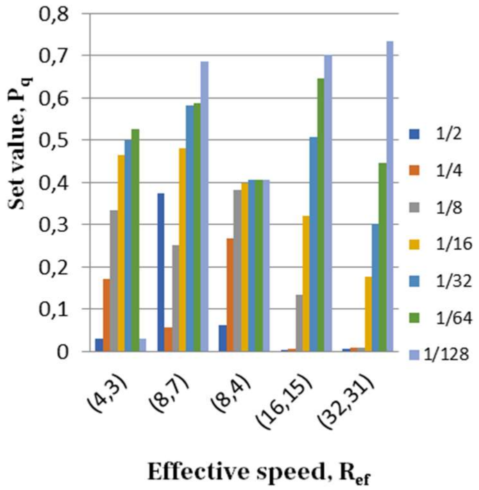

Figure2: Dependence of the effective speed (Ref) on the probability of distortion in the q symbol channel P_q for codes (4,3), (8,7), (8,4), (16,15), and (32,3)

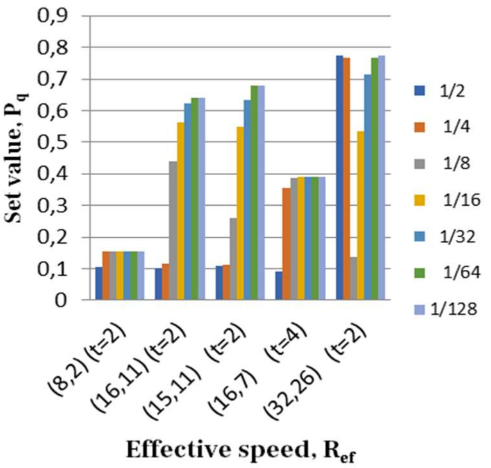

Figure 3: Dependence of the effective speed (Ref) on the probability of distortion in the q symbol channel P_q for codes (8,2), (16,11), (15,11), (16,7) and (32,26)

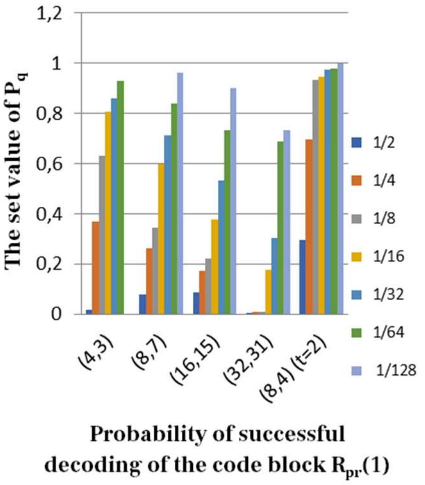

Figure 4: Dependence of the probability of reception of the block Pr (1) value of the probability of distortion in the channel of the q-symbol Pqfor codes (4,3), (8,7), (16,15), (32,3) and (8,4)

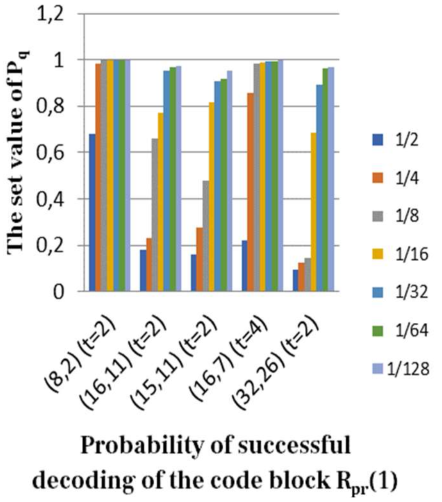

Figure 5: Dependence of the probability of reception of the blockPr (1) on the value of the probability of distortion in the channel of the q-symbol Pqfor codes (8,2), (16,11), (15,11), (16,7) and (32,26)

Table 2
Dependence of the effective speed (R_{ef}) on the probability of distortion in the q symbol channel (P_q)

Code	Channel quality							
	P_q	1/2	1/4	1/8	1/16	1/32	1/64	1/128
	Effective speed R_{ef}							
(4,3)		0.0319	0.1711	0.3339	0.4647	0.5009	0.526	0.0319
(8,7)		0.3740	0.0573	0.2524	0.4825	0.5817	0.588	0.6852
(16,15)		0.0048	0.0076	0.1336	0.3206	0.5073	0.646	0.7012
(32,31)		0.0057	0.0082	0.0096	0.1772	0.3026	0.446	0.7351
(8,4) (t = 2)		0.0635	0.2681	0.3815	0.3982	0.4062	0.406	0.4062
(8,2) (t = 2)		0.1051	0.1533	0.1559	0.1562	0.1562	0.156	0.1562
(16,11) (t = 2)		0.1024	0.1157	0.4383	0.5627	0.6215	0.641	0.6406
(15,11) (t = 2)		0.1085	0.1139	0.2597	0.5483	0.6345	0.680	0.6802
(16,7) (t = 4)		0.0925	0.3539	0.3869	0.3906	0.3906	0.391	0.3906

Table 3
Dependence of the probability of reception of the block P_r (1) value of the probability of distortion in the channel of the q symbol P_q

Code	Channel quality							
	P_q	1/2	1/4	1/8	1/16	1/32	1/64	1/128
	The probability of receiving a block P_r(1)							
(4,3)		0.0175	0.3684	0.6315	0.8070	0.8594	0.9298	0.962
(8,7)		0.0785	0.2634	0.3428	0.600	0.7142	0.8380	0.963
(16,15)		0.0874	0.1739	0.2222	0.3777	0.5333	0.7333	0.899
(32,31)		0.0038	0.0074	0.0096	0.1772	0.3026	0.6874	0.735
(8,4) (t = 2)		0.2970	0.695	0.9350	0.948	0.9735	0.9805	0.997
(8,2) (t = 2)		0.6816	0.9825	0.9961	0.9981	0.9984	0.9989	0.999
(16,11) (t = 2)		0.1818	0.2308	0.6615	0.7692	0.9538	0.9673	0.972
(15,11) (t = 2)		0.1598	0.2763	0.4769	0.8153	0.9076	0.9153	0.951
(16,7) (t = 4)		0.2190	0.8571	0.9810	0.9905	0.9917	0.9946	0.998

3. Conclusion

Our results demonstrate that codes with natural redundancy can be used in diverse information systems with strict security requirements, especially in noisy communication channels. Additionally, these codes are beneficial for hardware systems where minimizing size, cost, and energy consumption is important.

References

[1] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[2] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: 8th International Conference on "Mathematics. Information Technologies. Education:" Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[3] A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17. doi: 10.3390/cryptography8030038.

[4] S. Abramov, A. Bessalov, V. Sokolov, Properties of Isogeny Graph of Non-Cyclic Edwards Curves, in:

Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 234–239.

[5] M. Al-Bassam, et al., Fraud and Data Availability Proofs: Detecting Invalid Blocks in Light Clients, Financial Cryptography and Data Security: 25th International Conference, FC 2021, LNCS 12675 (2021) 279–298. doi: 10.1007/978-3-662-64331-0_15.

[6] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

[7] Y. Wu, Implementation of Parallel and Serial Concatenated Convolutional Codes, Dissertation Submitted to the Faculty of the Virginia Polytechnic Institute and State University (2000).

[8] V. Poltorak, et al., Remote Object Confidential Control Technology based on Elliptic Cryptography, in: Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 121–130.

[9] J. Ziv, Variable-to-Fixed Length Codes are Better than Fixed-to-Variable Length Codes for Markov Sources, IEEE Transactions on Information Theory 36(4) (1990) 861–863. doi: 10.1109/18.53746.

[10] R. E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, Reading, MA. (1984).

[11] C. Berrou, A. Glavieux, Near Optimum Error Correcting Coding and Decoding: Turbo-Codes, IEEE Trans. On Comm. 44(10) (1996) 1261–1271.

[12] S. Toliupa, et al., Formation of Shift Index Vectors of Ring Codes for Information Transmission Security, in: 21th International Scientific and Practical Conference "Information Technologies and Security", vol. 3241 (2021) 248–257.

[13] G. A. Radtke, et al., Robust Verification of Stochastic Simulation Codes, J. Comput. Phys. 451 (2022). doi: 10.1016/j.jcp.20 21.110855.

[14] C. Shannon, Communication Theory of Secrecy Systems, Bell Syst. Tech. J. 28(4) (1949) 656–715. doi: 10.1002/J.1538-7305.1949.TB00928.X.

[15] B. Zhurakovskiy, et al., Performance Analysis of Concatenated Coding for OFDM Under Selective Fading Conditions, in: 10th International Scientific Conference "Information Technology and Implementation," IT and I, vol. 3624 (2023) 403–413.

[16] B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, Cybersecurity Providing in Information and Telecommunication Systems, in: 3421 (2023) 67–76.

[17] O. Pliushch, B. Zhurakovskiy, M. Klymash, Robust Control Channel of Unmanned Aerial Vehicle, 5th IEEE International Conference on Advanced Information and Communication Technologies (2023) 37–40. doi: 10.1109/aict61584.2023. 10452677.

[18] I. Liminovych, et al., Protection System for Analysis of External Link Placing, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 179–188.

[19] B. Zhurakovskiy, N. Tsopa, Assessment Technique and Selection of Interconnecting Line of Information Networks, 3rd International Conference on Advanced Information and Communications Technologies (AICT) (2019). doi: 10.1109/aiact.2019.884 7726.

[20] V. Druzhynin, et al., Features of Processing Signals from Stationary Radiation Sources in Multi-Position Radio Monitoring Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 46–65.

[21] N. Onizawa, et al., Clockless Stochastic Decoding of Low-Density Parity-Check Codes, IEEE Workshop on Signal Processing Systems, Quebec City, QC (2012). doi: 10.1109/SiPS.2012.53.

[22] A. Hazem, et al., Low Energy High Speed Reed-Solomon Decoder Using Two Parallel Modified Evaluator Inversion less Berlekamp-Massey, Signals, Systems and Computers (ASILOMAR) IEEE (2010).

[23] N. Onizawa, et al., Lowering Error Floors in Stochastic Decoding of LDPC Codes Based on Wire-Delay Dependent Asynchronous Updating, IEEE 43rd International Symposium on Multiple-Valued Logic (2013) 254–259. doi: 10.1109/ismvl.2013.35.

[24] B. Zhurakovskyi, et al., Coding for Information Systems Security and Viability, in: Information Technologies and Security, vol. 2859 (2021) 71–84.

[25] C. Ceroici, V. C. Gaudet, FPGA Implementation of a Clockless Stochastic LDPC Decoder, IEEE Workshop on Signal Processing Systems (SiPS) (2014) 1–5. doi: 10.1109/SiPS.2014.6986088.

[26] J. Hagenauer, The Turbo Principle: Tutorial Introduction and State of the Art, in: Proc. of The Int. Symp. on Turbo Codes and Related Topics (1997).

[27] D. V. Sarwate, R. D. Morrison, Decoder Malfunction in BCH Decoders, Information Theory, IEEE Transactions on Information Theory 36(4) (1990) 884–889. doi: 10.1109/18.53752.

[28] X. Zuo, et al., Improving the Tolerance of Stochastic LDPC Decoders to Overclocking-

Induced Timing Errors: A Tutorial and a Design Example, IEEE Access 4 (2016) 1607–1629. doi: 10.1109/ACCESS.2016.2550179.

[29] P. Jung, J. Plechinger, Performance of Rate Compatible Punctured Turbo-codes for Mobile Radio Applications, Electronics Lettes 33(25) (1997) 2102–2103.

[30] B. Zhurakovskyi, N. Tsopa, Y. Batrak, Comparative Analysis of Modern Formats of Lossy Audio Compression, in: Cyber Hygiene, vol. 2654 (2020).

[31] G. Caire, E Biglieri, Parallel Concatenated Codes with Unequal Error Protection, IEEE Transactions on Communications 46(5) (1998) 565–567.

[32] P. Robertson, K. Villebrun, P. Hoeher, A Comparison of Optimal and Sub-optimal MAP Decoding Algorithms Operating in the Log Domain, in: Proc. IEEE Int. Conf. on Commun., Oberpfaffenhofen, Germany (1995) 1009–1013.

[33] J. Spinner, J. Freudenberger, Decoder Architecture for Generalised Concatenated Codes, IET Circuits, Devices and Systems, Published by Wiley and The Institution of Engineering and Technology (2015). doi: 10.1049/iet-cds.2014.0278.

[34] V. Tilavat, Y. Shukla, Simplification of Procedure for Decoding Reed–Solomon Codes Using Various Algorithms: An Introductory Survey, Int. J. Eng. Dev. Res. 2(1) (2014) 279–283.

[35] S. Lin, W. Chung, Y. Han, Novel Polynomial Basis and its Application to Reed-solomon Erasure Codes, 55th Annual Symposium on Foundations of Computer Science (2014) 316–325. doi: 10.1109/FOCS.2014.41.

[36] S. Otrokh, V. Kuzminykh, O. Hryshchenko, Method of Forming the Ring Codes, in: Information Technologies and Security, Vol. 2318 (2018) 188–198.

[37] M.-P. Beal, The Method of Poles: a Coding Method for Constrained Channels, IEEE Transactions on Information Theory 36(4) (1990) 763–772. doi: 10.1109/18. 53736.

[38] R. E. Blahut, Algebraic Codes for Data Transmission (2003). doi: 10.1017/CBO 9780511800467.

[39] T.-C. Lin, et al., A Future Simplification of Procedure for Decoding Nonsystematic Reed Solomon codes Using the Berlekamp-Massey Algorithm, IEEE Transactions on Communications 59(6) (2011). doi: 10.1109/tcomm.2011.050 211.100170.

[40] J. Freudenberger, J. Spinner, Mixed Serial/Parallel Hardware Implementa-tion of the Berlekamp-Massey Algorithm for BCH Decoding in Flash Controller Applications, Conference: Signals, Systems, and Electronics (ISSSE), International Symposium (2012). doi: 10.1109/issse.2012. 6374329.

[41] S.-J. Lin, W. Chung, Y. Han, Novel Polynomial Basis and Its Application to Reed-Solomon Erasure Codes, Computer Science, IEEE 55th Annual Symposium on Foundations of Computer Science. Conference Paper (26) (2014). doi: 10.1109/FOCS.2014.41.

[42] V. Moutoussamy, S. Nanty, B. Pauwels, Emulators for Stochastic Simulation Codes. ESAIM: Proceedings and Surveys 48 (2015) 116–155. doi: 10.1051/proc/201448005.