of such operations as finding primitive irreducible polynomials $GF(p^{\alpha})$ over the field minimum length.

References

[1] AMN Aljalai, C. Feng, VCM Leung, R. Ward, "Improving the energy efficiency of dft-s-ofdm in uplink massive mimo with barker codes", in 2020 International Conference on Computing, Networking and Communications (ICNC), 2020, pp. 731–735. doi: 10.1109/ICNC47757.2020.9049829.

[2] M. Kellman, F. Rivest, A. Pechacek, L. Sohn, M. Lustig, "Barker-coded nodepore resistive pulse sensing with built-in coincidence correction", in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp. 1053–1057. doi: 10.1109/ICASSP.2017.7952317.

[3] R. Lakshmi, D. Trivikramarao, S. Subhani, VS Ghali, "Barker coded thermal wave imaging for anomaly detection", in 2018 Conference on Signal Processing And Communication Engineering Systems (SPACES), 2018, pp. 198–201. doi: 10.1109/SPACES.2018.8316345.

Oleksandr Meshcheulov, Oleg Riznyk*

student of CS Department, Ukrainian National Forestry University, Lviv, Ukraine, meshcheulov@nltu.edu.ua.

*associate professor of CS Department, Ukrainian National Forestry University, Lviv, Ukraine. https://orcid.org/0000-0002-3815-043X, riznykoleg@nltu.edu.ua.

Methods for information coding in mobile systems

Abstract – Naturally, there is a need to protect information from unauthorized access, theft, destruction, distortion and other criminal acts. The concept of information vulnerability is introduced, which describes the effectiveness of selected methods for information protection. With the development and complication of methods and forms of automation of information processing processes, its vulnerability increases. The spectrum of problems expands significantly when the user starts working with wireless networks, because errors may occur during data transmission over these communication channels. Their reasons may be different, but

* науковий керівник

the result is the same - the data is distorted and cannot be used on the receiving side for further processing.

Keywords – balanced incomplete block, ideal ring bundle, interference-resistant code, mobile system.

Knits make it possible to ensure a sufficiently high correction ability of such a system due to its unique combinatorial properties, and the dissimilarity of the encoding-decoding process compared to existing cryptographic methods that use the properties of polynomials makes the protection even stronger.

The basis of the construction of interference-resistant codes, as is known, is the principle of introducing redundancy, which makes it possible to detect and correct errors by imposing additional requirements on the transmitted signals, followed by their verification [8].

The synthesis of interference-resistant codes on the basis of ideal ring bundle (IRB) became possible due to the fact that an ideal ring with parameters N and R corresponds to a cyclic balanced incomplete block (BIB) scheme on a set of elements $\{b_j\} = \{j\}$, $j = \overline{1, 2, \ldots, S_N}$, which is one of the main types of block diagrams.

Cyclic IRB code is a block code, that is, the number of bits in one block is a constant value. How many bits can be encoded in one block: $n = \log_2(S_N + 1) = \log_2 16 = 4$.

After constructing the code combinations, let's find out the possibilities of this code, namely determine the minimum code distance, correction and correction ability. It is easy to find that each of S_N $(S_N - 1)/2$ of different pairs of code combinations contains exactly R single N symbols in digits of the same name, which follows from the properties of the IRB. The remaining $N - R$ symbols of the same and as many other code combinations differ from the symbols contained in the digits of the same name. Therefore, the minimum code distance for this code is defined as:

$$d_{\min} = 2(N - R) \tag{1}$$

* науковий керівник

The number of errors that can be detected t_d and the number of errors that can be corrected t_c using the correction code are related to the minimum code distance by dependencies, and are, respectively:

$$t_d \le d_{\min} - 1 \tag{2}$$

$$t_c \le \frac{d_{\min} - 1}{2} \tag{3}$$

The interference-resistant system of barker-like sequences based on IRB is able to encode 4 the bits of the data array into a sequence of length 15 and at the same time correct to 3 the positions of the sequence (or 20%), while the cryptographic system based on BCH codes with the same length of the sequence and the number of information bits allows editing to the 4 positions of (or $26,67\%$).

In terms of corrective ability, BCH codes show better results, although globally 3 or 4 per block length 15 is not critical, because for most software the threshold of correctability is 10%.

The second most important parameter that determines the feasibility of implementing a particular development is the speed of the encoding and decoding process. It was experimentally established that both coding systems give approximately the same results when encoding a data array, however, the process of decoding data using IRB is performed more than twice as fast as BCH.

Conclusion. Codes based on IRB are based on well-studied properties of bundle, which have a complex structure for reproduction by attackers. In addition, we use different IRBs, we sort the construction results according to different parameters. BCH-based codes based on Galois fields are theoretically more complex, as the number of operations for their construction increases, and the number of polynomial options is limited and they are all already known.

References

[1] O. Riznyk, O. Povshuk, Y. Kynash and I. Yurchak, "Composing method of anti-interference codes based on non-equidistant structures", in 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS

* науковий керівник

Design (MEMSTECH), Lviv , 2017, pp. 15-17. doi: 10.1109/MEMSTECH.2017.7937522.

[2] I. Tsmots, V. Rabyk, O. Riznyk, Y. Kynash, "Method of synthesis and practical realization of quasi-barker codes", in 2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), 2019, vol. 2, pp. 76–79. doi: 10.1109/STC-CSIT.2019.8929882.

[3] I. Tsmots, O. Riznyk, V. Rabyk, Y. Kynash, N. Kustra, M. Logoida, "Implementation of fpga-based barker's-like codes", in Lytvynenko, V., Babichev, S., Wo´jcik , W., Vynokurova, O., Vyshemyrskaya, S., Radetskaya, S. (eds.) Lecture Notes in Computational Intelligence and Decision Making, 2020, pp. 203–214. Springer International Publishing, Cham. doi: 10.1007/978-3-030-26474-1 15.

[4] I. Tsmots, O. Riznyk, V. Rabyk, Y. Kynash, N. Kustra, M. Logoida, "Implementation of fpga-based barker's-like codes", in Lytvynenko, V., Babichev, S., Wo´jcik , W., Vynokurova, O., Vyshemyrskaya, S., Radetskaya, S. (eds.) Lecture Notes in Computational Intelligence and Decision Making, 2020, pp. 203–214. Springer International Publishing, Cham. doi: 10.1007/978-3-030-26474-1 15.

Oleg Talanchuk, Oleg Riznyk*

*associate professor of IT Department, Ukrainian National Forestry University, Lviv, Ukraine. https://orcid.org/0000-0002-3815-043X.
riznykoleg@nltu.edu.ua.
student of IT Department, Ukrainian National Forestry University, Lviv, Ukraine, talanchuk@nltu.edu.ua.

Information encoding methods based on ideal ring bundle

Abstract – Naturally, there is a need to protect information from unauthorized access, theft, destruction, distortion and other criminal acts. The concept of information vulnerability is introduced, which describes the effectiveness of selected methods for information protection. With the development and complication of methods and forms of automation of information processing processes, its vulnerability increases.

* науковий керівник