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

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

Keywords – mobile system, ideal ring bundle, Barker code, barker-like code.

During the construction of simple perfect bundle, it turned out that not all values n have an ideal ring bundle (IRB). For example, all attempts to construct IKB for $N = 7$ and $N = 11$ have failed, although for the rest of the values n within the first ten simple perfect rings exist. A similar picture is observed when considering multiple perfect bundles. In particular, it follows from the definition of the concept of a multiple ideal ring bundle that is $S_N - 1 = \frac{N(N-1)}{R}$ an integer, from which one of the necessary conditions for the existence R of -multiple IRBs is determined:

$$N(N-1) \equiv 0 \pmod{R} \quad (1)$$

The existence, construction and list of combinatorial objects of type 1KB is, in fact, a problem, the solution of which is the subject of studying combinatorial analysis as the theoretical basis of discrete mathematics. Therefore, the necessary and sufficient conditions for the existence of IRB should be established on the basis of the provisions of combinatorial analysis.

There are a lot of algorithms for constructing IRBs, namely: classical methods of construction based on difference sets, an algorithm based on Galois fields, however, algorithms of selective branching and asymmetric movements have become more common for constructing IRBs on a computer.

The algorithm is based on the use of the combinatorial properties of the IRB and implements the principle of growing bundles of natural numbers according to certain rules. Its essence is to compile a sequence of numbers chosen in the order of increasing their values while meeting the necessary conditions that satisfy the formation of ideal bundle with given parameters. The conditions for the formation of knits follow directly from the combinatorial properties of these sequences.

* науковий керівник

It is necessary to build an interference-resistant system capable of providing protection in two main directions:

- from interference - the system must have the highest possible correction ability for successful data transmission over a wireless network, where, as is known, various types of interference may occur;
- from unauthorized access - the algorithm on the basis of which this system is built must be sufficiently complex and non-obvious to make it impossible to decode the data in some way.

Therefore, before proceeding with the software implementation, it is necessary to assess the technical feasibility of implementing an interference-resistant system based on IRB, and for that it is necessary to compare it with the best similar systems known today. Most experts consider this a system based on Bose – Choudhury - Hockingham (BCH) codes. During the comparison, such indicators as the speed of the encoding-decoding process, degree of redundancy, correction ability, algorithmic complexity, etc. are taken into account.

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 [1].

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

* науковий керівник

[1] S. Matsuyuki and A. Tsuneda, "A Study on Aperiodic Auto-Correlation Properties of Concatenated Codes by Barker Sequences and NFSR Sequences", in 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2018, pp. 664-666. doi: 10.1109/ICTC.2018.8539367.

[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.

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

Methods of increasing the power of interference-resistant barker-like codes

Abstract – It is known that the power of any multi-position interference-resistant sequence, in particular a Barker-like sequence, is determined by the number of its digits and increases accordingly with the increase in the length of the code sequence [4]. One of the well-known methods of increasing the power of barker-like interference-resistant sequences based on IRB is to use next to the combinations of the basic cyclic code of combinations, where all symbols in the corresponding digits are changed to the opposite.

Keywords – BCH code, ideal ring bundle, Barker code, barker-like code.

* науковий керівник