Method of data control in the residue classes

Victor Krasnobayev [0000-0001-5192-9918], Alexandr Kuznetsov [0000-0003-2331-6326],

Anna Kononchenko [0000-0002-8101-6500], Tetiana Kuznetsova [0000-0001-6154-7139]

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine

v.a.krasnobaev@gmail.com, kuznetsov@karazin.ua, akononpro@gmail.com, kuznetsova.tatiana17@gmail.com

Abstract. Methods of data control in the residue classes are considered in the article. The main advantage of non-positional notation in the residue classes lays in the possibility of an organization of the process of quick implementation of modular arithmetic operations of addition, subtraction and multiplication. The base of the method is the procedure of generating and using the positional indication of non-positional code. That allows increasing efficiency of the procedure of data control granted by the residue classes.

Keywords. Methods of data control, the system of the residue classes, the positional indications of the non-positional code, computer systems and components.

1 Introduction

It is well known, that the main advantage of non-positional notation in the residue classes (NRC) is laid in the possibility of quick process of organization of modular arithmetic operations of addition, subtraction and multiplication [1, 2].

However, in computer systems for common purpose it is needed to perform so-called non-modular (position) operations except the above listed arithmetic operations. The following operations belong to these:

- Arithmetic and algebraic congruence of numbers and its absolute values;
- Sign of number definition;
- Definition of existing of overflow of bit grid of computer system (CS);
- Rounding of value of result of operation;
- Computing the absolute value;
- Division and multiplication of fraction
- Translation of data from code of NRC to positional notation and back;
- Expanding of original NRC (it is an informational process in which familiar remainders $\{a_i\}$, that correspond to basis $\{m_i\}$, define value of remainders with the same code structure by other additional basis);

- Control, diagnostic and correction mistakes of NRC data, etc.

Generally, all positional operations come down to the procedure of definition of an index of j numerical $\left[jm_i,\ (j+1)m_i\right)$ interval of entering (detecting) of number $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$. It is appropriate to use so-called positional indications of non-positional code (PINC) to define an index of j numerical interval of detecting A. The following indications are the most frequently used in NRC (within existing PINCs) [3, 4]:

- Indications based on the procedure of number's translating from NRC to PINC;
- Indications based on the procedure of nulevization (reduction to zero polynomial) (definition of the value of y_{n+1});
- Indications based on the procedure of expanding given system of basis of NRC;
- Rank r of number A, etc.

There are disadvantages of the above-mentioned PINC. At first, it is technical and time complexity of PINC generating (developing) for given code structure $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$. At second, it is no mean time of implementation having applied the existing positional indications, non-modular operations in NRC, specifically, operations of control, diagnostic of correction of data mistakes [3, 4].

It becomes obvious that the research of developing methods of generating new PINC in NRC is important; because of them, we can use operatively non-modular operations. It should be pointed out, population (sequence) of defined modular and non-modular operations, which are implemented by PINC, can realize any non-modular operation.

Beforehand we will consider the general requirements to PINC, on base of which in article will be developed method of increasing of operational efficiency of data control:

- To define exactly correctness and incorrectness of number A in NRC (to define fact of detecting/not detecting of number A in an informational numerical $[0,M]$ interval, where $M=\prod_{i=1}^{n} m_i$) by used (chosen, developed, generated) PINC;
- Simplicity of generating PINC for given code structure of data $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$;
- Simplicity of using of generated indication for data control in NRC (in general case for implementing positional operations);
- Indication has to have clear and understandable physical meaning;
- Indication must be analytically described by simple mathematical relator;
- It is possible to technically implement process of data control in NRC by using PINC;
- Using the chosen indication of non-positional code has to provide the given fidelity of data control in NRC;

- PINC using has to provide the possibility of exception from the control procedure, diagnostic and correction of mistakes in NRC the most difficult positional operations.

It is reasonable to develop and research the method of data control in NRC on the base of PINC using, resulting from the above-mentioned information.

2 Method of generating of positional indication of non-positional code structure of data in NRC

Looking upon method of generating of PINC (Fig. 1).

The indication n_A forms proceeding from representation of initial code structure $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$, which is represented as NRC with basis $\{m_i\}$, $i=\overline{1,n+1}$, in the way of creating of so-called uniserial code (UC).

In standard form, UC

$$K_N^{(n_A)}=\left\{Z_{N-1}^{(A)}\ Z_{N-1}^{(A)}\ ...\ Z_1^{(A)}\ Z_0^{(A)}\right\}$$

represents sequence of binary bits, which contains ones and a zero, index of which is at n_A place (the count is performed from right to left, from digit bit $Z_0^{(A)}$ to digit bit $Z_{N-1}^{(A)}$). Indication of PINC n_A defines an index of j numerical interval $\left[jm_i,\ (j+1)m_i\right)$ of detecting of number $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$. Mathematically PINC n_A represents a positive integer, which points out the location of zero binary bit in the record of UC $K_N^{(n_A)}$ $\left(Z_{n_A}^{(A)}=0\right)$.

The procedure of generating UC $K_N^{(n_A)}$ lies in the following. A constant

$$KH_{m_i}^{(A)}=\left(a_1',...,a_{i-1}',a_i,a_{i+1}',...,a_{n+1}'\right)$$

defines in the block of constants of nuvelization (BCN). It is performed by the definition of remainder a_i of number $A=(a_1,...,a_{i-1},\ a_i,a_{i+1},...,a_n,a_{n+1})$ for chosen integer m_i of NRC.

Further, using the chosen constant of nuvelization $KH_{m_i}^{(A)}$, we displace number A on the left edge of the interval $\left[jm_i,\ (j+1)m_i\right)$ by implementing operation

$$A_{m_i}=A-KH_{m_i}^{(A)}=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_{n+1})-\left(a_1',a_2',...,a_{i-1}',a_i,a_{i+1}',...,a_{n+1}'\right)=$$
$$=\left[a_1^{(1)},a_2^{(1)},...,a_{i-1}^{(1)},0,a_{i+1}^{(1)},...,a_{n+1}^{(1)}\right].$$

1.	Choice informational $\{m_i\}$, $i=\overline{1,n}$ and control $m_k = m_{n+1}$ ($m_i < m_{i+1}$) basis of residue classes for representing data $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1})$, GCD $(m_i,m_j)=1$, $i \neq j$.
2.	Choice of basis $m_i \in \{m_i\}$, $(j=\overline{1,n+1})$, by which defines an index of j numerical interval $\left[jm_i,\ (j+1)m_i\right)$ of detecting number A.
3.	Defining the constant of reducing to zero polynomial $KH_{m_i}^{(A)}=(a_1^{'},a_2^{'},...,a_{i-1}^{'},a_i,a_{i+1}^{'},...,a_n^{'},a_{n+1}^{'})$ by value of remainder a_i (by module m_i) of number A.
4.	Defining the value $A_{m_i}=A-KH_{m_i}^{(A)}=\left(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n,a_{n+1}\right)-$ $-\left(a_1^{'},a_2^{'},...,a_{i-1}^{'},a_i,a_{i+1}^{'},...,a_n,a_{n+1}\right)=\left[a_1^{(1)},a_2^{(1)},...,a_{i-1}^{(1)},0,a_{i+1}^{(1)},...,a_n^{(1)},a_{n+1}^{(1)}\right].$
5.	Defining UC $K_N^{(n_A)}=\left\{Z_{N-1}^{(A)}\ Z_{N-2}^{(A)}\ ...\ Z_0^{(A)}\right\}$, $K_{N_i}^{(n_A)}=\left\{Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)}\ ...\ Z_0^{(A)}\right\}$. $N=\prod_{\substack{K=1\\K\neq i}}^{n+1} m_K$, $N_i=]M/m_i[$, $M=\prod_{i=1}^{n} m_i$. $A_{m_i}-K_A\cdot m_i=Z_{K_A}^{(A)}$. $\begin{cases} A_{m_i}-0\cdot m_i=Z_0^{(A)}, \\ A_{m_i}-1\cdot m_i=Z_1^{(A)}, \\ \quad\cdots \\ A_{m_i}-(N-2)\cdot m_i=Z_{N-2}^{(A)}, \\ A_{m_i}-(N-1)\cdot m_i=Z_{N-1}^{(A)}. \end{cases}$ $\begin{cases} A_{m_i}-0\cdot m_i=Z_0^{(A)}, \\ A_{m_i}-1\cdot m_i=Z_1^{(A)}, \\ \quad\cdots \\ A_{m_i}-(N_i-2)\cdot m_i=Z_{N_i-2}^{(A)}, \\ A_{m_i}-(N_i-1)\cdot m_i=Z_{N_i-1}^{(A)}. \end{cases}$
6	Defining PINC n_A of number A, which means numerical value of n_A for which $Z_{K_A}^{(A)}=Z_{n_A}^{(A)}=0$, which means $A_{m_i}-n_A\cdot m_i=0$. Herewith $Z_l^{(A)}=1, (A_{m_i}-l\cdot m_i\neq 0; l\neq n_A)$.

Fig. 1. The method of generating PINC in NRC

It is obvious, that number A is aliquot to value of module m_i of NRC.

It is known, that an indication of the correctness of number A in NRC defines by it's entering or not entering in its numerical informational interval $[0, M)$. If number A is out of the interval $(A \geq M)$, A is considered as garbling (wrong). In this case, PINC n_A has to define the fact of entering or not entering initial number A in the interval $[0, M)$. We have to implement operation

$$A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)} \tag{1}$$

to define the fact of detecting number in numerical informational interval [0, M).

The operation (1) is carried out simultaneously using the population of N constants

$$K_A \cdot m_i \left(K_A = \overline{0, N-1}\right),$$

where $N = \prod_{\substack{K=1 \\ K \neq i}}^{n+1} m_K$:

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ A_{m_i} - 2 \cdot m_i = Z_2^{(A)}, \\ \quad \dots \\ A_{m_i} - (N-2) \cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(A)}. \end{cases} \tag{2}$$

In this case, UC represents in the view

$$K_N^{(n_A)} = \left\{ Z_{N-1}^{(A)}\ Z_{N-2}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\} \tag{3}$$

The only value n_A from (1) exists in total (2) analytical rations. For n_A there is

$$Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0 \quad (K_A = n_A),$$

which means

$$A_{m_i} - n_A \cdot m_i = 0.$$

The rest of values (2) equal

$$Z_l^{(A)} = 1 \ \ (A_{m_i} - l \cdot m_i \neq 0;\ l \neq n_A).$$

In the general case, the amount of N binary bits in the record UC $K_N^{(n_A)}$ equal to value

$$N = \prod_{\substack{K=1 \\ K \neq i}}^{n+1} m_K \ .$$

It should be pointed out, that there is no necessity to have the whole sequence of values $Z_{K_A}^{(A)}$ from (3) to define only the fact of the garbling of number $(A \geq M)$. It is enough to have UC $K_{N_i}^{(n_A)}$ with length only $N_i =]M / m_i[$ of binary bits (where value $]M / m_i[$ describes the lesser integer of number M / m_i).

In this case values of variables of numerical intervals $\left[jm_i, \ (j+1)m_i \right)$, which are out of informational interval $[0, \ M)$, make no matter for establishing the fact of correctness control of number A.

3 Method of operational data control in NRC on base of using positional indication of non-positional code

The procedure of generating of positional indication of non-positional code (fig. 1) laid in the base of method of operational data control in residue classes. In that way, the essence of the method of data control in residue classes lies in the following. For the controlled code structure $A=(a_1,...,a_{i-1}, \ a_i, a_{i+1},...,a_n, a_{n+1})$, which is represented in residue classes, developed (defined) PINC n_A by generating UC

$$K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)} \ Z_{N_i-2}^{(A)} \ ... \ Z_1^{(A)} \ Z_0^{(A)} \right\}$$

in view of sequence of N_i binary bits. Choosing of basis m_i of NRC is performed by special-purpose in accordance with defined measures. The constant of nuvelization

$$KH_{m_i}^{(A)} = \left(a_1', a_2', ..., a_i, ..., a_n', a_{n+1}' \right)$$

is selected depending on a result of the value of remainder a_i of number A. Further implementation operation is carried out:

$$A_{m_i} = A - KH_{m_i}^{(A)} = (a_1, a_2, ..., a_i, ..., a_n, a_{n+1}) - \left(a_1', a_2', ..., a_i, ..., a_n', a_{n+1}' \right) =$$
$$= \left[a_1^{(1)}, a_2^{(1)}, ..., 0, ..., a_n^{(1)}, a_{n+1}^{(1)} \right].$$

Using Ni constants $K_A \cdot m_i$ $\left(K_A = \overline{0, N_i - 1} \right)$ simultaneously the operations of subtractions $A_{m_i} - K_A \cdot m_i$ are carried out, in the result of which appears the values of binary bits $Z_{K_A}^{(A)}$, so the UC $K_{N_i}^{(n_A)}$ forms.

The values of PINC n_A defined from the equation $A_{m_i} - n_A \cdot m_i = 0$.

If $n_A > N_i$, number A is considered as a wrong. In the opposite case ($n_A \le N_i$) number A is correct. In common view, method of data control is represented on Fig. 2.

Algorithm of defining UC $$K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\}$$ of number $$A = \left(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1}\right).$$

↓

Method of generating of PINC n_A: $$A_{m_i} - n_A \cdot m_i = 0, Z_{n_A}^{(A)} = 0;\ Z_l^{(A)} = 1, A_{m_i} - l \cdot m_i = 1; l \ne n_A.$$

↓

Data control $A = \left(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1}\right)$ in NRC.
If $n_A > N_i$, then number $\tilde{A}$ is wrong (garbled).
If $n_A \le N_i$, then number A is right (ungarbled).

Fig. 2. Method of data control in NRC

Examine now the examples of implementing of method of control for specific NRC, which is given with basis $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ and $m_k = m_{n+1} = m_5 = 11$. The NRC provides the data handling in single-byte (1=1) bit grid of CS. Herewith

$$M = \prod_{i=1}^{4} m_i = 420,\ M_0 = Mm_{n+1} = 4620;$$

$$N_i = N_{n+1} = \left]M / m_i\right[= \left]M / m_{n+1}\right[= \left]420/11\right[= \left]38{,}18\right[= 39.$$

Contents of the block of constants of nuvelization (BCN) concerning basis $m_k = m_{n+1} = 11$ are given in Table 1.

Example 1. Perform control of data that represented in view $A = (01, 00, 000, 010, 0001)$.

Constant of nuvelization

$$KH_{m_{n+1}}^{(A)} = (01, 01, 001, 001, 0001)$$

is selected by values of remainders $a_K = a_{n+1} = a_5 = 0001$ of number A in BCN CS (Table 1). Then we define value

Table 1. Constants $KH^{(A)}_{m_{n+1}}$ of nulevization BCN

Remainder $a_k = a_{n+1}$	Constant of nuvelization				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_k = m_5 = 11$
	a'_1	a'_2	a'_3	a'_4	a_5
0000	00	00	000	000	0000
0001	01	01	001	001	0001
0010	10	10	010	010	0010
0011	00	11	011	011	0011
0100	01	00	100	100	0100
0101	10	01	000	101	0101
0110	00	10	001	110	0110
0111	01	11	010	000	0111
1000	10	00	011	001	1000
1001	00	01	100	010	1001
1010	01	10	000	011	1010

$$A_{m_{n+1}} = A - KH^{(A)}_{m_{n+1}} = (00,11,100,001,0000) .$$

By implementation of ratio (2) we form UC

$$K^{(n_A)}_{N_i} = K^{(9)}_{39} = \{11...110111111111\} .$$

Resulting from the view of UC and using formula

$$A_{m_{n+1}} - n_A \cdot m_{n+1} = 0 ,$$

we define that $n_A = 9$

$$(A_{m_{n+1}} - n_A \cdot m_{n+1} = 99 - 9 \cdot 11 = 0),$$

meaning $Z^{(A)}_{n_A} = Z^{(A)}_9$.

Because of $N_i = 39 > n_A = 9$ it means that there is no mistake in data.

Check: $A = 100 < M = 420$ (number A is right).

Example 2. Perform control of data $A = (00,10,000,010,1010)$.

The constant

$$KH^{(A)}_{m_{n+1}} = (01,10,000,011,1010)$$

is selected by value of $a_5 = 1010$ in BCN (Table 1).

We deduce that

$$A_{m_{n+1}} = A - KH^{(A)}_{m_{n+1}} = (10,00,000,110,0000)\ .$$

Because

$$A_{m_{n+1}} - n_A \cdot m_{n+1} = 440 - 44 \cdot 11 = 0$$

then UC has view $K^{(n_A)}_{N_i} = K^{(40)}_{39} = \{11...11...11\}$ and $n_A = 40$.

Because of $N_i = 39 < n_A = 40$ it means that there is a mistake in data.

Check: $A = 450 > M = 420$ (number A is wrong).

Example 3. Perform control of data $A = (01,11,010,000,1001)$. .

The constant

$$KH^{(A)}_{m_{n+1}} = (00,01,100,010,1001)$$

is selected by value of $a_5 = 1001$ in BCN (Table 1). We deduce that

$$A_{m_{n+1}} = A - KH^{(A)}_{m_{n+1}} = (01,10,011,101,0000)\ .$$

Because

$$A_{m_{n+1}} - n_A \cdot m_{n+1} = 418 - 38 \cdot 11 = 0$$

then UC has view

$$K^{(n_A)}_{N_i} = K^{(38)}_{39} = \{011...11...11\}$$

and $n_A = 38$.

Because $n_A = 38 < N_i = 39$ of it means that number A is right (ungarbled). Though the check $A = 427 > M = 420$ shows us that number A is wrong (Fig. 3).

The represented method can be used for improving promising computer systems and their components and in the other practically important applications [5-9]. In particular, mathematical transformation in the system of the residue classes can be successfully adopted for optimization of calculations of cryptographic methods of data protection [10-15, 24-27], also in code theories and complicated discrete signals [16-21], in authentication and steganography [22, 23].

4 Conclusions

Thus, the method of data control in the system of residue classes is presented in the article. The procedure of forming and using of position indication of non-positional code is the base for a method of operational control of data in a residue class. Use of PINC allows to increase efficiency of the procedure of data control provided to NRC.

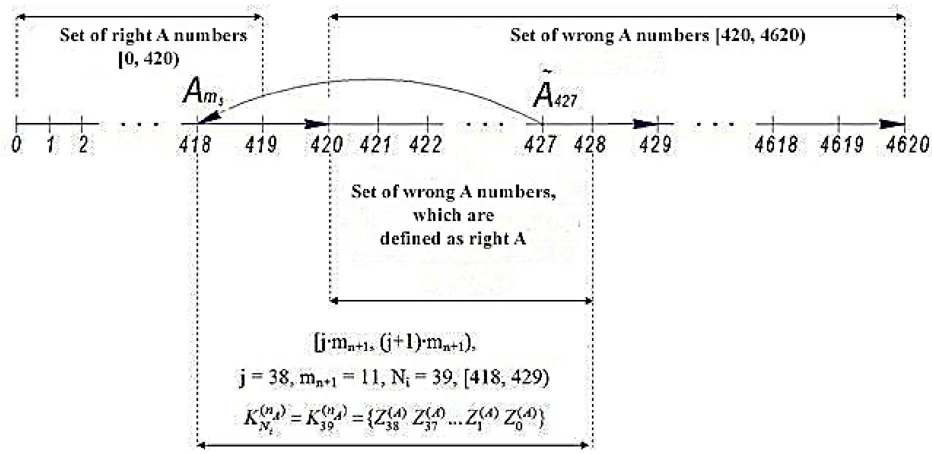

Fig. 3. Example of implementing operation of data control in NRC for $m_{n+1} = m_5 = 11$

It should be pointed out, that any non-modular operation can be implemented by set (sequence) of defined modular and non-modular operations, which are implemented by PINC. Using PINC in the method provides the possibility of exception of the most complicated positional operations from the procedure of control, diagnostic and correction of mistakes in NRC.

References

1. Akushsky, I.Y., Yuditsky, D.I.: Machine modular arithmetic. M.: Sov. Radio (in Russian) (1968)
2. Kolyada, A.A., Pak, I.T.: Modular structures of pipeline processing of digital information. Minsk: University (in Russian) (1992)
3. Krasnobayev, V., Kuznetsov, A., Koshman, S., Moroz, S.: Improved Method of Determining the Alternative Set of Numbers in Residue Number System. In: Recent Developments in Data Science and Intelligent Analysis of Information. ICDSIAI 2018. Advances in Intelligent Systems and Computing, Springer, Cham, 2018, vol. 836, pp. 319–328. (2019) doi:10.1007/978-3-319-97885-7_31
4. Krasnobayev, V.A., Yanko, A.S., Koshman, S.A.: A Method for arithmetic comparison of data represented in a residue number system. Cybernetics and Systems Analysis, 2016, vol. 52(1), pp. 145–150. (2016) doi:10.1007/s10559-016-9809-2
5. Xiao, H., Wu, D.: A Component Model for Network Processor Based System. In: 2007 IEEE/ACS International Conference on Computer Systems and Applications, Amman, 2007, pp. 47–50. (2007) doi:10.1109/AICCSA.2007.370863
6. Andrushkevych, A., Gorbenko, Y., Kuznetsov, O., Oliynykov, R., Rodinko, M.: A Prospective Lightweight Block Cipher for Green IT Engineering. In: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control, Springer, Cham, 2019, vol. 171, pp. 95–112. (2019) doi:10.1007/978-3-030-00253-4_5

7. Kuznetsov, O., Potii, O., Perepelitsyn, A., Ivanenko, D., Poluyanenko, N.: Lightweight Stream Ciphers for Green IT Engineering. In: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control, Springer, Cham, 2019, vol. 171, pp. 113–137. (2019) doi:10.1007/978-3-030-00253-4_6
8. Wang, A., Zhang, A., Chen, S.: Study On simulation and design of data links human computer interface. In: 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 4066–4069. (2011) doi:10.1109/CSSS.2011.5974893
9. Irfan, S., Ghosh, S.: Optimization of information retrieval using evolutionary computation: A survey. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 328–333. (2017) doi:10.1109/CCAA.2017.8229837
10. Moskovchenko, I., Pastukhov, M., Kuznetsov, A., Kuznetsova, T., Prokopenko, V., Kropyvnytskyi, V.: Heuristic Methods of Hill Climbing of Cryptographic Boolean Functions. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 1–6. (2018) doi:10.1109/INFOCOMMST.2018.8632017
11. Kuznetsov, A., Kavun, S., Panchenko, V., Prokopovych-Tkachenko, D., Kurinniy, F., Shoiko, V.: Periodic Properties of Cryptographically Strong Pseudorandom Sequences. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129–134. (2018) doi:10.1109/INFOCOMMST.2018.8632021
12. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O.: Experimental Studies of the Modern Symmetric Stream Ciphers. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 125–128. (2018) doi:10.1109/INFOCOMMST.2018.8632058
13. Rodinko, M., Oliynykov, R.: An Approach to Search for Multi-Round Differential Characteristics of Cypress-256. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 659–662. (2018) doi:10.1109/INFOCOMMST.2018.8631904
14. Ivanov, O., Ruzhentsev, V., Oliynykov, R.: Comparison of Modern Network Attacks on TLS Protocol. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 565–570. (2018) doi:10.1109/INFOCOMMST.2018.8632026
15. Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M.: Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. In: 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5027–5033. (2018) doi:10.1109/BigData.2018.8622621
16. Kuznetsov, A., Serhiienko, R., Prokopovych-Tkachenko, D.: Construction of cascade codes in the frequency domain. In: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 20187, pp. 131–136. (2017) doi:10.1109/INFOCOMMST.2017.8246366
17. Kuznetsov, A., Kiyan, A., Uvarova, A., Serhiienko, R., Smirnov, V.: New Code Based Fuzzy Extractor for Biometric Cryptography. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 119–124. (2018) doi:10.1109/INFOCOMMST.2018.8632040
18. Gorbenko, I.D., Zamula, A.A.: Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems. Telecommunications and Radio En-

gineering, 2017, vol. 76(12), pp. 1079–1100. (2017) doi:10.1615/TelecomRadEng.v76.i12.50
19. Kuznetsov, .A, Pushkar'ov, A., Kiyan, A., Kuznetsova, T.: Code-based electronic digital signature. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331–336. (2018) doi:10.1109/DESSERT.2018.8409154
20. Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.: Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications. Telecommunications and Radio Engineering, 2016, vol. 75(2), pp. 169–178. (2016) doi:10.1615/TelecomRadEng.v76.i17.40
21. Gorbenko, I.D., Zamula, A.A., Semenko, A.E., Morozov, V.L.: Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols. Telecommunications and Radio Engineering, 2017, vol. 76(17), pp. 1523–1533. (2017) doi:10.1615/TelecomRadEng.v76.i17.40
22. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Mikheev, I., Belozertsev, I.: Hiding data in the structure of the FAT family file system. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 337–342. (2018) doi:10.1109/DESSERT.2018.8409155
23. Gorbenko, Y., Svatovskiy, I., Shevtsov, O.: Post-quantum message authentication cryptography based on error-correcting codes. In: 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 51–54. (2016) doi:10.1109/INFOCOMMST.2016.7905333
24. Kavun, S.: Conceptual fundamentals of a theory of mathematical interpretation. Int. J. Computing Science and Mathematics, 2015, vol. 6(2), pp. 107–121. (2015) doi:10.1504/IJCSM.2015.069459
25. Kavun, S.: Indicative-geometric method for estimation of any business entity. Int. J. Data Analysis Techniques and Strategies, 2016, vol. 8(2), pp. 87–107. (2016) doi: 10.1504/IJDATS.2016.077486
26. Zamula, A., Kavun, S.: Complex systems modeling with intelligent control elements. Int. J. Model. Simul. Sci. Comput., 2017, vol. 08(01). (2017) doi:10.1142/S179396231750009X
27. Kavun, S., Zamula, A., Mikheev, I.: Calculation of expense for local computer networks. In: Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International, Kharkiv, Ukraine, 2017, pp. 146–151. (2017) doi:10.1109/INFOCOMMST.2017.8246369