UDC 004.056

Faure E. V.[1], Shcherba A. I.[2], Kharin A. A.[3]

[1]PhD, Associate Professor, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine
[2]PhD, Associate Professor, Head of Department of Applied Mathematics, Cherkasy State Technological University, Cherkasy, Ukraine
[3]Post-graduate student of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine

FACTORIAL CODE WITH A GIVEN NUMBER OF INVERSIONS

Context. Factorial coding with data recovery by permutation provides complex information protection from unauthorized reading and errors in communication channel and has the property of self-synchronization. At the same time, such coding does not allow to detect all low-weight errors that leads to a relatively small increase of reliability.

The purpose of this work is to develop and study the method of factorial coding with a given number of inversions aimed at increasing the reliability of information transmission, by introducing additional redundancy by choosing a class of permutations that satisfy the given criterion.

Method. The main idea of the proposed method is to introduce artificial redundancy by reducing the cardinality of used permutations. Such an approach makes it possible to select from a whole set of permutations a class that possesses the necessary, pre-assigned properties. It was suggested to use the correspondence of the number of permutation inversions to a given class of residues as a sign of belonging to the permutation class in use. A theoretical evaluation of code parameters was performed.

Results. Signal-code constructions for the factorial code with a given number of inversions under the order of permutations $M = 8$ are constructed. For each of the possible classes, the cardinality, code rate, estimates of the probability of undetected error and the relative transmission rate for systems with decision feedback and independent bit errors were investigated. It is shown that the code parameters are not invariant with respect to the selected class of residues for a given modulus. The structural schemes of encoding and decoding devices are developed.

Conclusions. The method of factorial coding with data recovery by permutation has been developed. The use of permutations with a number of inversions that belongs to the selected class of residues allowed increasing the reliability of transmission in exchange for the loss of code rate.

Keywords: factorial coding, permutation, inversion, redundancy, class of residues, reliability of transmission, relative transmission rate.

NOMENCLATURE

FCDR – Factorial Code with Data Recovery by Permutation;

FCGNI – Factorial Code with a Given Number of Inversions;

DF – decision feedback;

SCC – signal-code construction;

$A(x)$ – data word in a binary form;

$B_M(q,R)$ – class of permutations with inversion numbers belonging to the class of residues $\overline{R}_q$;

$f_j(i)$ – number of i-bit errors that can transform the j-th permutation of SCC into any other permutation of the same construction;

$i_M(q,R)$ – amount of information carried by one permutation of the class $B_M(q,R)$;

k – number of binary symbols in information block;

$k_M(q,R)$ – length of binary data word to be converted into a permutation of the class $B_M(q,R)$;

l_r – number of bits for encoding a single symbol of permutation;

M – permutation order;

n – number of bits in a data block;

$N_M(\omega)$ – number of different permutations of the order with a number of inversions equal to ω;

$P_{ud}(FCGNI, p_0)$ – probability of FCGNI undetected errors;

p_0 – bit error probability;

Q – probability of codeword error-free reception;

$R_{FCDR}(x)$ – FCDR codeword in a binary form;

$\overline{R}_q$ – residue class modulo q;

r_{FCDR} – number of bits in FCDR codeword;

α – code redundancy factor (by cardinality);

ν_0 – relative transmission rate;

ν_1 – code rate;

ν_2 – dynamic component of transmission rate loss due to retransmission of data in error;

$W_M(q,R)$ – permutations class cardinality;

ω – number of inversions in permutation.

INTRODUCTION

Rapid growth of modern society computerization level leads to the need to ensure the joint work of many computers including in open communication networks. Particularly acute is the need to ensure safe operation in open computer

DOI 10.15588/1607-3274-2018-2-16

networks in the exchange of financial information, as well as information of national importance, such as information from the state's law enforcement agencies. All this leads to the need for complex information security that provides for the following tasks:

– the task of protection against information unauthorized reading (through its encryption);

– the task of ensuring information integrity that includes:

– information protection against errors due to noise in communication channels;

– protection against obtrusion of false information.

All these tasks are solved in existing computer and telecommunication systems and networks. However, each of them is solved independently from each other, by different means created at different times, and based on an individual mathematical basis. A consequence of this approach is an increase of the introduced redundancy. This entails a reduction of data channel bandwidth and leads to an increase of the load of computational basis used to realize the assigned tasks.

Therefore, the development of methods and tools for complex information security based on a single procedure for its processing that ensure a high level of protection and transmission reliability is an actual problem.

To date, a relatively large volume of extensive research on factorial coding methods has been performed from the viewpoint of providing complex information protection. The analysis of works [1–9] reveals the properties of factorial codes and allows planning further research in this scientific direction. In particular, the paper [5] is of exceptional interest. It examined the factorial code with data recovery by permutation (FCDR).

The most important property of FCDR is its ability to provide complex data protection at acceptable values of transmission rate loss. At the same time, FCDR does not detect an even number of bit errors that lead to the transformation of one permutation into another. In channels of acceptable quality (where $\lambda = np_0 \le 1$), the probability of FCDR erroneous decoding is determined by the intensity of low-weight errors. As shown in [1], this probability decreases rapidly with increasing of error weight. Therefore, eliminating low-weight errors from the set of FCDR non-detectable errors will reduce the undetected error probability.

The purpose of this work is to increase the reliability of information transmission when using FCDR. This purpose can be achieved by introducing additional redundancy by choosing a class of permutations that satisfy the given criterion.

1 PROBLEM STATEMENT

Suppose that the information from the source goes to the encoder input in blocks $A(x)$ of k bits. In this case, the cardinality of information words set is 2^k. FCDR realizes a bijective transformation of the set of information words $A(x)$ into an allowed set of permutations of order M $\left(M! \ge 2^k\right)$. Reducing the cardinality of information words of used permutations while preserving their order M makes it possible to choose from $M!$ permutations only those that satisfy the preassigned set of properties.

The task of developing a method of information coding based on factorial coding with data recovering by permutation consists in determining the effective criterion for choosing the class of used permutations, which allows one to vary flexibly the parameters of reliability of information transmission, and also in the analysis of the structure of allowed set of permutations and its influence on undetected error probability and relative transmission rate.

2 REVIEW OF THE LITERATURE

According to [5], the permutation π after the symbols encoding by a uniform binary code is represented as a data block $R_{FCDR}(x)$ of r_{FCDR} bits, where

$$r_{FCDR} = l_r \cdot M, \tag{1}$$

l_r is a number of bits for encoding a single symbol of permutation.

For uniform binary code

$$l_r = \lceil \log_2 M \rceil, \tag{2}$$

where $\lceil a \rceil$ is the smallest integer greater than or equal to a (function 'ceiling' [10] of a).

The length of FCDR code combination n_{FCDR} corresponds to the number of bits in the representation of the permutation π of the order M in a binary form: $n_{FCDR} = r_{FCDR}$.

A necessary (but not sufficient) condition for the bijectivity of the mapping between the set $\{A(x)\}$ and the set of allowed permutations $\{\pi\}$ is the condition of choosing an order M according to the inequality $M! \ge 2^k$. Since $M! = 2^k$ is possible only for $k = 1$, for practical applications we shall proceed from the condition $M! > 2^k$. It follows that

– the maximum length of a binary information word to be converted into a permutation of the order M is given by

$$k_{\max} = \lfloor \log_2 M! \rfloor; \tag{3}$$

– $M! - 2^k$ permutations are not used by the source, and FCDR is a redundant code. Code redundancy factor (by cardinality) is defined in [6] as:

$$\alpha = M! / 2^k. \tag{4}$$

When the value of the number of bits of the information word is chosen according to (3), the minimum redundancy factor (by cardinality) is provided for the given M. In this case,

$$1 < \alpha < 2. \tag{5}$$

An error-detecting factorial code that satisfies the condition (5) will be called a factorial code with natural redundancy. The value of redundancy factor (by cardinality) is $\alpha_{nat} = M! / 2^{k_{\max}}$.

It was shown in [6] that equality (4) implies that the decrease in the length of the information word per Δk bits for a fixed M leads to the increase in the redundancy factor (by cardinality) by a factor of $2^{\Delta k}$. A code with $k < k_{\max}$ for a given M will be called a factorial code with introduced redundancy. In this case, the value of redundancy factor (by cardinality) is $\alpha_{intr} = 2^{\Delta k}$, where $\Delta k = k_{\max} - k$.

As a result of research performed in [5, 8], it is shown that FCDR provides protection against unauthorized reading of data if the law of transformation of source words into permutation is kept in secret. Meanwhile, the protection of information from errors in communication channel is provided by the properties of permutations. The most important of these properties is that the permutation π of order M is a sequence of symbols of the set $\{0;1;2;\ldots;M-1\}$. The position of the symbols in permutation is determined by the information word. In addition, every symbol in the permutation is used only once. Checking the occurrence of each of the symbols only once at the receiving station ensures that all odd number of bit errors and part of even number of bit errors are detected in the received block [5]. This check will be referred to as the data block validation.

The advantage of FCDR is also that it has the property of self-synchronization. This eliminates the need for a combination of frame synchronization to be entered in the data block.

The disadvantage of FCDR is that this code does not detect even number of bit errors, which lead to the transformation of one permutation into another.

In [6] it is shown that if for a given k the value of M is calculated according to the condition $(M-1)! < 2^k < M!$, then inequality $\alpha > 2$ can take place. Then it is possible to insert additional check bits into information part before forming the checksum. This allows to increase the transmission reliability while maintaining the permutation order and the code rate. On the other hand, if the value of M is given in a data transmission system and $k = k_{\max} = \lfloor \log_2 M! \rfloor$, the transmission reliability can be increased due to artificially introduced redundancy. This redundancy is provided by reducing the size of the data block at the encoder input and introducing additional check bits. The results presented in [6] for $k \le 1024$ and $p_0 = 10^{-3}$ indicate an increase in the energy gain due to the application of the proposed method by up to 1.6 dB. At the same time, the method proposed in [6] does not allow to detect some errors, including 2-bit errors, that lead to the transformation of one permutation into another (permutation of the permutation symbols).

3 MATERIALS AND METHODS

The proposed coding method provides the artificial redundancy by reducing the cardinality of used permutations. Consequently, the size of the source word also decreases (in comparison with its maximum possible value): $k = k_{\max} - \Delta k$, $\Delta k > 0$. We consider it obvious that an increase in redundancy should lead to an increase in the transmission reliability.

All the decisions made in this work are oriented to the creation of data transmission systems operating over a communication channel with independent bit errors. Primarily, this applies to block transmission systems where error correction is performed by retransmission of data in error (binary symmetric decision feedback (DF) systems). Such systems include most general and special purpose systems operating over wired telephone channels, radio relay, microwave, satellite and fiber-optic communication channels.

The main idea of the work is to use a number of inversions in permutation as a sign of its belonging to an allowed set. So, if we use only even (odd) permutations to transfer source words, then:

– the cardinality of the allowed set of source words will be halved (exactly half of the permutations of the set of $M!$ permutations is even (odd));

– the decoder will detect all the errors that lead to the transformation of a permutation into another permutation and change its parity. Accordingly, the decoder will not detect errors that lead to the transformation of a permutation into another permutation and do not change its parity.

Note that the transformation of one permutation into another is equivalent to a permutation of its symbols and can be represented as a product of transpositions. Therefore, the transformation of one FCDR codeword into another can be represented as a finite number of consecutive transpositions. Each transposition applied to a permutation changes its parity. Therefore, the consistent application of an odd number of transpositions changes the parity of a permutation. The consistent application of an even number of transpositions does not change the parity of a permutation. This means that the use of only even (odd) permutations allows to detect errors that lead to a transformation equivalent to an odd number of consecutive transpositions over the codeword.

Note also that if the source uses only even (odd) permutations, the decoder will detect all 2-bit errors in a FCDR codeword. This is because a 2-bit error is not detected by FCDR if and only if it generates a transposition of symbols in the codeword. Since the transposition changes the parity of a permutation, it will be detected by the decoder. In this case, an undetected decoding error can be estimated using the expression (2) from [5], where instead of the estimate $f_{per}(2) \le l_r \cdot M/2$ it should be used $f_{per}(2) = 0$.

Thus, it is possible to increase the transmission reliability of systems with FCDR by reducing the cardinality of permitted permutations and detecting their transpositions in the process of transportation.

In turn, reducing the cardinality of the set of permutations – information carriers – by half leads to a need to reduce the block length by one bit and, accordingly, to reduce the code rate. Therefore, the use of permutations for information transferring, in which a number of inversions satisfies the specified requirements, allows exchanging the code rate for the transmission reliability.

In view of the foregoing, the proposed code will be called a factorial code with a given number of inversions (FCGNI). We define the rule for choosing an allowed set of permutations based on the number of inversions. For this, we consider the theoretical basis for constructing FCGNI.

A number of inversions $\omega = inv(\pi)$ in the permutation π of the order M satisfies the condition $0 \le \omega \le 0.5 \cdot M \cdot (M-1)$. Each number ω of possible inversions corresponds to a frequency number $N_M(\omega)$. Due to the definition of frequency numbers, the next expression is valid:

$$\sum_{\omega=0}^{0.5M(M-1)} N_M(\omega) = M!,$$

and besides $N_M(0) = N_M(0.5M(M-1)) = 1$.

In addition, the frequency number $N_M(\omega) = 0$ for $\omega < 0$ and $\omega > 0.5M(M-1)$.

It is shown in [11] that the distribution of inversions on all permutations of a fixed length coincides with the distribution of their major index. That is, the number $N_M(\omega)$ of permutations of order M with ω inversions is the same as the number of permutations of order M with major index equal to ω. These numbers are known as Mahonian numbers. A stronger result is valid: the number of permutations of order M with major index k and ω inversions is the same as the number of permutations of order M with major index ω and k inversions, that is, the two statistics are equidistributed.

According to [12, 13], the following recurrence relation is valid:

$$N_{M+1}(\omega) = N_M(\omega - M) + N_M(\omega + 1 - M) + \\ + \ldots + N_M(\omega) = \sum_{i=\omega-M}^{\omega} N_M(i), \quad (6)$$

wherein $N_0(\omega) = 0$ if $\omega \ge 1$.

In accordance with [12, 14, 15], the frequency numbers are coefficients in the expansion $\prod_{i=0}^{M-1} \left(1 + x + \ldots + x^i\right)$, i.e.

$$\prod_{i=0}^{M-1} \left(1 + x + \ldots + x^i\right) = \sum_{\omega=0}^{0.5M(M-1)} N_M(\omega) \cdot x^{\omega}.$$

Online Encyclopedia of Integer Sequences (OEIS) [16] contains the sequence of McMahon numbers $N_M(\omega)$ for $M \in [1,50]$.

Properties of frequency numbers $N_M(\omega)$.

1. For $M \ge 2$ and $\omega : 2 \le \omega \le C_M^2 - 1$ all the frequency numbers $N_M(\omega) \ge M - 1$.

2. The symmetry property for $M \ge 2$: $N_M(\omega) = N_M\left(C_M^2 - \omega\right)$, $N_M(1) = M - 1$.

3. $\sum_{\omega=0}^{0.5M(M-1)} (-1)^{\omega} N_M(\omega) = 0$.

4. $\sum_{\omega=0}^{0,5M(M-1)} \omega N_M(\omega) = \frac{1}{2} C_M^2 M! = \sum_{\pi} inv(\pi)$.

5. If $\omega_1 < \omega_2 \le \left[0,5 \cdot C_M^2\right]$, then $N_M(\omega_1) < N_M(\omega_2)$.

6. If the number C_M^2 is even, i.e. $C_M^2 = 2l$, then $\max_{\omega} N_M(\omega) = N_M(l)$. If the number C_M^2 is odd, i.e. $C_M^2 = 2l + 1$, then $\max_{\omega} N_M(\omega) = N_M(l) = N_M(l+1)$.

6. The recurrence formula (6) can be reduced to the following form:

$$N_{M+1}(\omega) = N_{M+1}(\omega - 1) + N_M(\omega) - N_M(\omega - 1 - M). \quad (7)$$

Remark. If $\omega < M + 1$, formula (7) has the form $N_{M+1}(\omega) = N_{M+1}(\omega - 1) + N_M(\omega)$, which corresponds to the expressions (I) from [12] and (9) from [17].

We define the residue modulo q of a number of inversions in a permutation of the order M: $R = |\omega|_q$, where $2 \le q \le 0,5 \cdot M \cdot (M-1)$ and $0 \le R \le q - 1$.

The set of various permutations π of the order M with a number of inversions of the residue class $\overline{R}_q$ forms a subset (class) of permutations $B_M(q,R) = \left\{\pi : |inv(\pi)|_q = R\right\}$. Depending on values of q and R, cardinalities $W_M(q,R)$ of classes $B_M(q,R)$ are calculated as follows:

$$W_M(q,R) = \sum_{j=0}^{\left[(0.5 \cdot M \cdot (M-1) - R)/q\right]} N_M(\omega = jq + R). \quad (8)$$

It was shown in [17] that if $q \le M$, then the cardinalities of classes $B_M(q,R)$ are invariant with respect to R and are equal to

$$W_M(q,R) = M!/q. \quad (9)$$

Note that the cardinalities $W_M(q,R)$ of the classes $B_M(q,R)$ can differ significantly for the constant modulus q value. Therefore, in order to maximize the code rate, it is necessary to use the permutation classes of maximum

cardinality for information transmission. In this case, the amount of information carried by one permutation will be equal to

$$i_M(q,R) = \log_2\left(W_M(q,R)\right), \quad (10)$$

and

$$k_M(q,R) \le \lfloor i_M(q,R) \rfloor. \quad (11)$$

At the same time, it does not follow from this that the use of the permutation class $B_M(q,R)$ of maximum cardinality provides the greatest energy efficiency. By energy efficiency, we mean the difference in signal levels at the input of the FCGNI receiver and some other receiver of information, providing the same probability of error-free reception.

All classes $B_M(q,R)$ for $q \le M$ have an equal cardinality. On other hand, the cardinalities of classes $B_M(q,R)$ where $M < q \le 0.5 \cdot M \cdot (M-1)$ are not equal and should be subject to experimental evaluation.

The above theoretical basis of information factorial coding determines the way of FCGNI constructing – selecting for information transmission only those permutations, which numbers of inversions belong to a selected class of residues $\overline{R}_q$. As shown above, if $q = 2$, the code detects all 2-bit errors and a part of errors with higher weight. Selecting a modulus q other than two $\left(2 < q \le 0.5 \cdot M \cdot (M-1)\right)$ will result in a different distribution of detectable and undetectable errors. This requires an informed choice of class $B_M(q,R)$. Note that if $q : |q|_2 = 0$, the code will detect all odd permutations and a part of even permutations.

We will accept $K = k_M(q,R)$. Then the probability of undetected error

$$P_{ud}(FCGNI, p_0) = 2^{-K} \sum_{j=1}^{2^K} \sum_{i=2}^{n} f_j(i)\, p_0^i (1-p_0)^{n-i}. \quad (12)$$

An integral indicator of data transmission quality is a relative transmission rate ν_0 [18]. It is calculated for a DF system as follows:

$$\nu_0 = \nu_1 \nu_2, \quad (13)$$

where $\nu_1 = k/n$.

According to [18], for the simplest DF system

$$\nu_2 = Q + P_{ud}(FCGNI, p_0),$$

where $Q = (1-p_0)^n$.

The structural scheme of the FCGNI encoder is shown in Fig. 1.

From a data source, an information word of k bits is entered in the buffer register 1. Then a source word is transmitted to the block 2 for forming a permutation with a number of inversions of a given class of residues. This permutation, after encoding its symbols with a binary code, is transmitted through the modulator 3 to a receiving station via a communication channel.

Generation of a permutation with a number of inversions of a given class of residues can be performed, for example, by creating a table that consists of 2^k rows. In each of them one of the permutations with a number of inversions $\omega : |\omega|_q = R$ is written.

The number of different tables that can be constructed is equal to

$$\mu(M,q,R,k) = C^{2^k}_{W_M(q,R)} \cdot k!. \quad (15)$$

At the same time, it is created a table that links permutations with information words for decoder. If these tables are kept secret, then the prerequisites for information encryption are created, and the expression (15) determines the key space cardinality. With this approach, the transmitting part of the system with FCGNI is a ROM where tables are stored. A table is selected by a session key. A permutation is selected by a k-bit source word that defines an address of a cell storing this permutation.

The structural scheme of the FCGNI decoder is shown in Fig. 2.

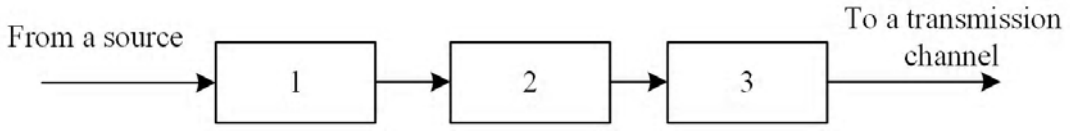

Figure 1 – The structural scheme of the FCGNI encoder

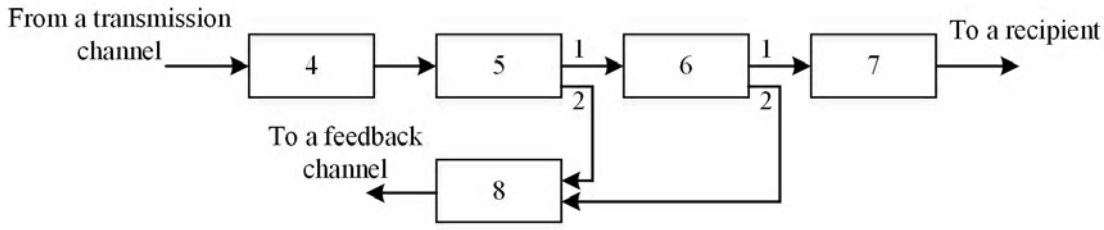

Figure 2 – The structural scheme of the FCGNI decoder

The demodulator 4 allocates data block (which can be affected by interference) from a received sequence (signal and noise mixture). Then the received data block comes to the block of permutation estimation 5. In block 5, the permutation correctness is evaluated – it is verified that each of the symbols $\{0,1,2,...,M-1\}$ is contained only once and that the permutation belongs to the allowed part of permutation set.

If the correctness condition is not satisfied, the permutation estimation block 5 erases the received data block and, by the bus 2, generates a command of retransmission of data in error for the request generation block 8. The request generation block 8 transmits this command to the transmitting station via a feedback channel.

If the correctness condition is satisfied, the permutation estimation block 5, by the bus 1, delivers the received permutation to the block 6 of estimation a number of permutation inversions. If the number of inversions in the received permutation does not belong to a given class of residues, then the block 6 of estimation a number of permutation inversions, by the bus 2, generates a command of retransmission of data in error for the request generation block 8.

If the received permutation has retained the number of inversions belonging to a given class of residues, then, by bus 1 of the block 6 of estimation a number of permutation inversions, the received permutation is transmitted to the permutation decoding block 7. This block performs the inverse transformation of the permutation into an information word using the corresponding table. The decoded permutation from the output of the block 7 is given to a recipient.

Thus, FCGNI detects:

– all errors that transform the transmitted permutation into non-permutation;

– all errors that transform the transmitted permutation into a permutation with a number of inversions that does not belong to a given class of residues.

4 EXPERIMENTS

In Table 1, for $M=8$ $(n=24)$ there are shown the results of experimental estimates of the maximum cardinality $W_{\max}$ of the permutation class $B_M(q,R)$; the value of R at which it is achieved; the value of $k_{\max}=\lfloor i_M(q,R)\rfloor$; the code rate $\nu_{1\max}$ corresponding to $k_{\max}$.

Remark. The EC symbols mean that all the classes $B_M(q,R)$ for a given q have an equal cardinality that is defined by (9).

We estimate the probability of undetected error (12), the code rate and the relative transmission rate (13). To do this, we randomly select from each class $B_8(q,R)$ the 2^K permutations that form the signal-code construction (SCC).

5 RESULTS

Fig. 3 shows the graph of dependence of the estimated probability of FCGNI undetected error on the modulus q for $p_0=10^{-3}$.

The dotted line in the graph indicates the estimated probability of FCDR undetected error for $M=8$, $P_{ud}(FCDR,10^{-3})=1{,}18\cdot10^{-5}$. In addition, it is presented the graph for the values of R from Table 1 providing the maximum cardinality of the class $B_8(q,R)$.

Table 1 – Classes $B_8(q,R)$ of maximum cardinality for $q\in[2,28]$

q	2	3	4	5	6	7	8	9	10
$W_{\max}$	20160	13440	10080	8064	6720	5760	5040	4522	4184
R	EC	EC	EC	EC	EC	EC	EC	5	4
$k_{\max}$	14	13	13	12	12	12	12	12	12
$\nu_{1\max}$	0,583	0,540	0,540	0,500	0,500	0,500	0,500	0,500	0,500
q	11	12	13	14	15	16	17	18	19
$W_{\max}$	3988	3890	3850	3838	3836	3836	3836	3836	3836
R	3	2	1	0	14	14	14	14	14
$k_{\max}$	11	11	11	11	11	11	11	11	11
$\nu_{1\max}$	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458
q	20	21	22	23	24	25	26	27	28
$W_{\max}$	3836	3836	3836	3836	3836	3836	3836	3836	3836
R	14	14	14	14	14	14	14	14	14
$k_{\max}$	11	11	11	11	11	11	11	11	11
$\nu_{1\max}$	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458

If values of R are chosen to ensure the maximum transmission reliability, the graph of dependence of the estimated probability of FCGNI undetected error on the modulus q for $p_0 = 10^{-3}$ will take the form shown in Figure 4. In addition, it is presented the graph for R providing the maximum transmission reliability of the class $B_8(q, R)$.

Note that in the general case, the classes with the maximum transmission reliability and the classes with the minimum cardinality are not the same for a given $q \in [2, 28]$.

A comparison of code rates providing the maximum SCC cardinality and the maximum reliability on $q \in [2, 28]$ are shown in Fig. 5.

The graph of dependence of the estimated relative transmission rate for FCGNI on the value of q for $M = 8$ and $p_0 = 10^{-3}$ is shown in Fig. 6. For each $q \in [2, 28]$ it is shown the estimated maximum relative transmission rate. The values of R in this case are given in Table 2.

The dashed-dot line on the graph indicates the estimated FCDR relative transmission rate for $M = 8$, $\nu_0\left(FCDR, 10^{-3}\right) = 0,610$.

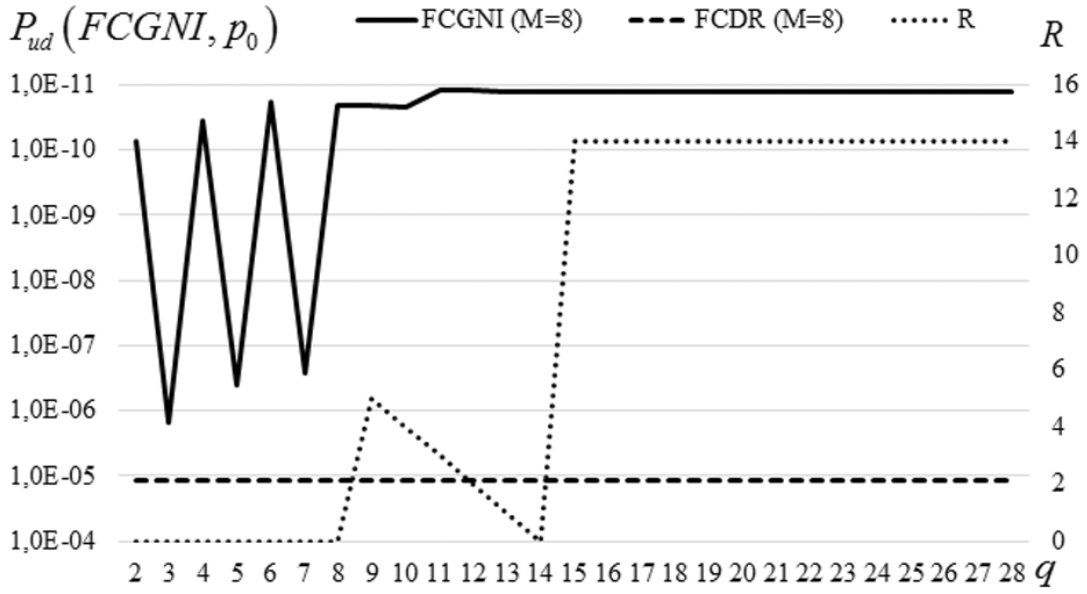

Figure 3 – Graph of dependence of the estimated probability of FCGNI undetected error on the modulus q for $p_0 = 10^{-3}$ (maximum code rate in the class $B_8(q, R)$)

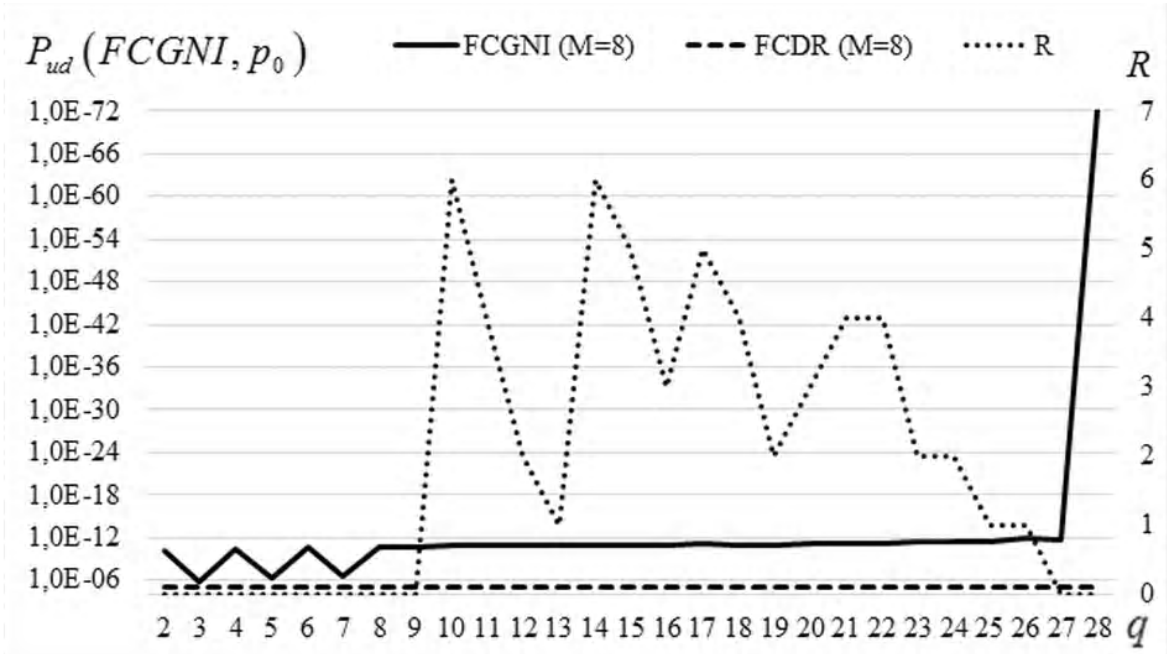

Figure 4 – Graph of dependence of the estimated probability of FCGNI undetected error on the modulus q for $M = 8$ and $p_0 = 10^{-3}$ (maximum transmission reliability in the class $B_8(q, R)$)

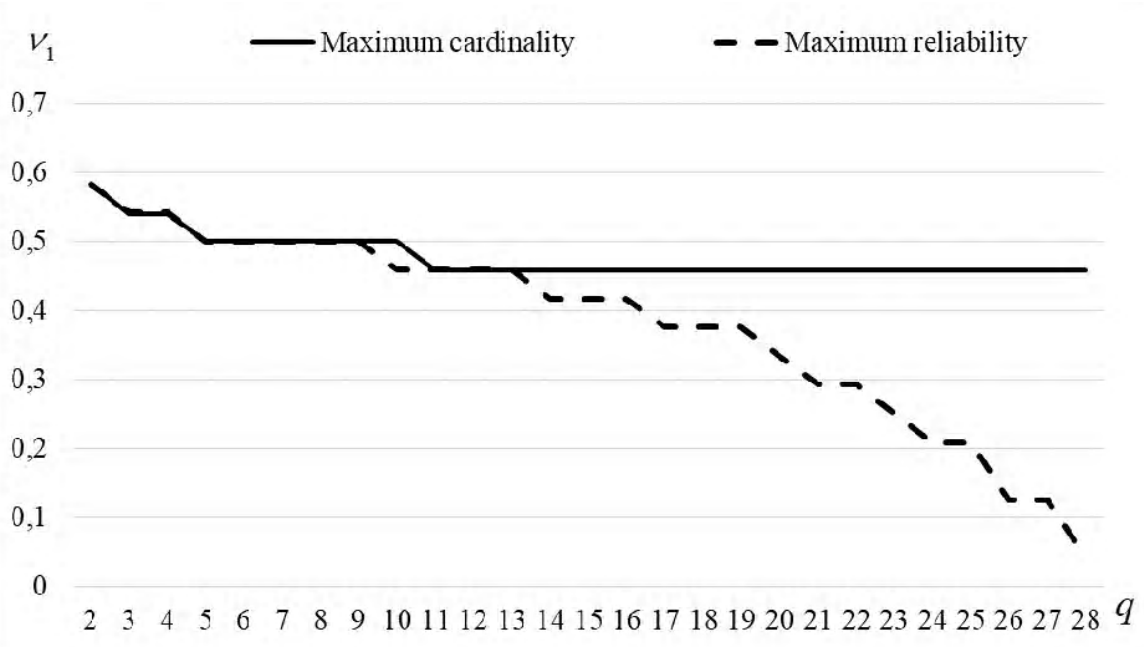

Figure 5 – Graphs of code rates providing the maximum SCC cardinality and the maximum reliability on $q \in [2,28]$ for $M = 8$ and $p_0 = 10^{-3}$

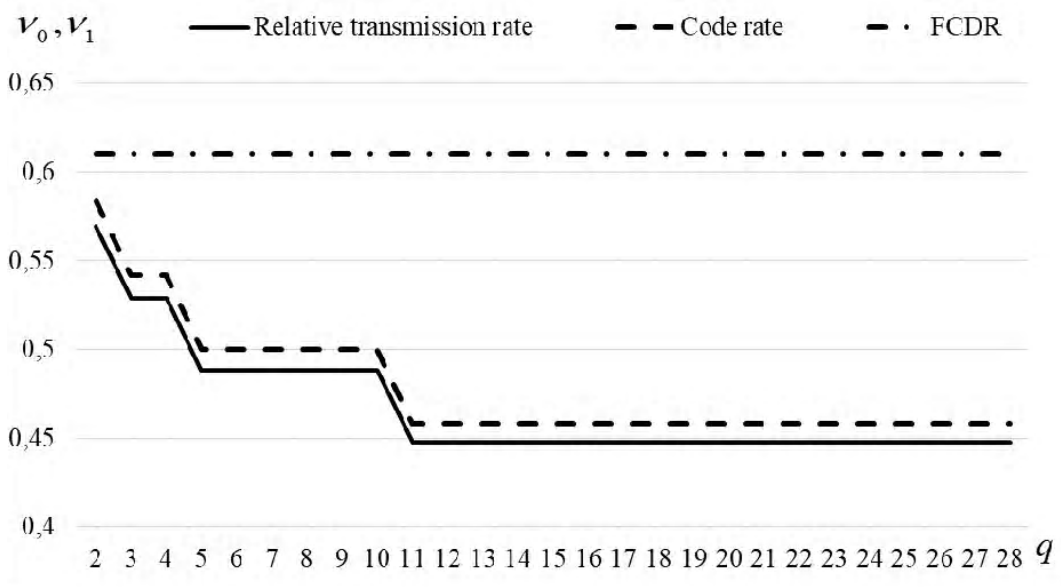

Figure 6 – Graph of dependence of the estimated FCGNI relative transmission rate on $q \in [2,28]$ for $M = 8$ and $p_0 = 10^{-3}$ (maximum relative transmission rate in the class $B_M(q,R)$)

Table 2 – Values of R for the maximum relative transmission rate for $q \in [2,28]$

q	2	3	4	5	6	7	8	9	10
R	ER	ER	ER	ER	ER	ER	ER	ER	3–5
q	11	12	13	14	15	16	17	18	19
R	ER	ER	ER	0–5,9–13	0–4,9–14	0–2,10–15	0,1,10–16	0,10–17	10–18
q	20	21	22	23	24	25	26	27	28
R	10–18	10–18	10–18	10–18	10–18	10–18	10–18	10–18	10–18

Remark. The ER symbols mean that all the classes $B_M(q,R)$ for a given q have an equal relative transmission rate.

6 DISCUSSION

The graph of Fig. 6 indicates that for $M = 8$ and $p_0 = 10^{-3}$ the relative transmission rate reaches the maximum values at the maximum values of the code rate. This is explained by the fact that $Q \gg P_{ud}\left(FCGNI, p_0\right)$ and, according to (14), $\nu_2 \approx Q$. Therefore, it is advisable to use $B_8\left(2, R\right)$, $R \in \{0;1\}$ to maximize the relative transmission rate for $M = 8$ and $p_0 = 10^{-3}$. For others M and $p_0 = 10^{-3}$, the values of q and R can vary.

It also follows from Figure 6 that FCDR exceeds FCGNI in the relative transmission rate for $M = 8$ and $p_0 = 10^{-3}$. Additional studies show that for $M = 8$ FCGNI has a gain in this indicator at $p_0 > 0.1$. At the same time, Figures 3 and 4 indicate that FCGNI is aimed at reducing the probability of undetected error (for example, for $q = 2$ – by more than five orders in comparison with FCDR). This can be useful in systems with high requirements for the probability of "false alarm".

Note that the presented coding method has a disadvantage inherent in all block ciphers. Identical plaintext blocks are converted into identical ciphertext blocks. Therefore, in order to eliminate the statistical redundancy and reduce the probability of identical blocks appearance, it is advisable to compress the plaintext before transformation.

CONCLUSIONS

The problem of increasing the reliability of information transmission using FCDR is solved.

The scientific novelty of the work is as follows. The method of factorial coding with data recovery by permutation has been further developed by using in SCC permutations with a number of inversions from a given class of residues. This makes it possible to reduce the number of undetected errors and, accordingly, to increase the transmission reliability.

The practical significance of the obtained results lies in the experimental estimates of FCGNI parameters, as well as in the developed structural schemes of encoding and decoding devices, which make it possible to carry out their practical implementation.

It is shown that by choosing the appropriate class of residues for the number of inversions ω in a permutation π, one can select a desired value of energy gain in exchange for the loss of the relative transmission rate. For example, the choice of the class $B_8\left(2,1\right)$ provides for $M = 8$ and $p_0 = 10^{-3}$ the probability of undetected error $P_{ud}\left(FCGNI, p_0\right) = 7.24 \cdot 10^{-11}$ and the code rate $\nu_1 = 0.583$. For comparison, the same indicators for FCDR – $P_{ud}\left(FCDR, p_0\right) = 1.18 \cdot 10^{-5}$, $\nu_1 = 0.625$. At the same time, the task of developing the principles for choosing a permutations set of a given class that forms an optimal structure of SCC is the subject of further research.

ACKNOWLEDGMENTS

The work was carried out as a result of joint research of the Department of Information Security and Computer Engineering and the Department of Applied Mathematics of Cherkasy State Technological University on the topic "Models, methods and means of complex information protection based on factorial coding" within the framework of the research work "Synthesis of cryptographic transformation operations with given characteristics" (state registration number 0116U008714) of the Department of Information Security and Computer Engineering of Cherkasy State Technological University.

The authors are grateful to the Associate Professor of the Department of Information Security and Computer Engineering of Cherkasy State Technological University Ph.D., Associate Professor Shvydkyi Valerii Vasylovych for comprehensive support in writing the work and useful discussions of the results.

REFERENCES

1. Фауре Э. В. Контроль целостности информации на основе факториальной системы счисления/ Э. В. Фауре, В. В. Швыдкий, А. И. Щерба // Journal of Baku Engineering University – Mathematics and Computer Science. – 2017. – Vol. 1, № 1. – P. 3–13.
2. Фауре Э. В. Комбинированное факториальное кодирование и его свойства / Э. В. Фауре, В. В. Швыдкий, В. А. Щерба // Радіоелектроніка, інформатика, управління. – 2016. – № 3. – С. 80–86. DOI: 10.15588/1607-3274-2016-3-10.
3. Пат. 107655 Україна, МПК G06F21/64 (2013.01), H04L1/16 (2006.01). Спосіб контролю цілісності інформації / Рудницький В. М., Фауре Е. В., Швидкий В. В., Щерба А. І. ; заявник та патентовласник Черкаський державний технологічний університет. – № a201505937 ; заявл. 16.06.2015; опубл. 24.06.2016, Бюл. № 12.
4. Пат. 107657 Україна, МПК H03M13/09 (2006.01), H04K1/06 (2006.01), G09C1/06 (2006.01). Спосіб комбінованого кодування інформації / Рудницький В. М., Фауре Е. В., Швидкий В. В., Щерба А. І. ; заявник та патентовласник Черкаський державний технологічний університет. – № a201508148 ; заявл. 17.08.2015; опубл. 24.06.2016, Бюл. № 12.
5. Фауре Э. В. Факториальное кодирование с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – № 2. – С. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932.
6. Фауре Э. В. Метод повышения эффективности факториального кодирования с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – №4. – С. 57–61.
7. Фауре Э. В. Факториальное кодирование с несколькими контрольными суммами / Э. В. Фауре // Вісник Житомирського державного технологічного університету. – 2016. – №3. – С. 104–113. DOI: 10.26642/tn-2016-3(78)-104-113.
8. Пат. 117004 Україна, МПК H03M13/09 (2006.01), H04L1/16 (2006.01), G04C1/06 (2006.01). Спосіб факторіального кодування з відновленням даних / Фауре Е. В., Харін О. О., Швидкий В. В., Щерба А. І. ; заявник та патентовласник Черкаський державний технологічний університет. – №u201613641; заявл.30.12.2016; опубл.12.06.2017, Бюл.№11.
9. Фауре Э. В. Факториальное кодирование с исправлением ошибок / Э. В. Фауре // Радіоелектроніка, інформатика, управління. – 2017. – № 3. – С. 130–138. DOI: 10.15588/1607-3274-2017-3-15.

10. Graham R. L. Concrete mathematics: a foundation for computer science / Ronald L. Graham, Donald E. Knuth, Oren Patashnik. – 2nd ed. – Reading: Addison-Wesley, 1994. – 657 p. ISBN13: 978-0201558029, ISBN10: 0201558025.
11. MacMahon P. A. The indices of permutations and the derivation therefrom of functions of a single variable associated with the permutations of any assemblage of objects / P. A. MacMahon // American Journal of Mathematics. – 1913. – № 35 (3). – P. 281–322. DOI: 10.2307/2370312.
12. Comtet L. Advanced Combinatorics / Louis Comtet. – Dordrecht: D. Reidel Publishing Company, 1974. – 343 p. DOI: 10.1007/978-94-010-2196-8.
13. Moritz R. H. A Coin-Tossing Problem and Some Related Combinatorics / Roger H. Moritz, Robert C. Williams // Mathematics Magazine. – 1988. – №1. – Vol. 61. – P. 24–29. DOI: 10.2307/2690326.
14. Mendes A. A Note on Alternating Permutations / Anthony Mendes // The American Mathematical Monthly. – 2007. – Vol. 114, № 5. – P. 437–440.
15. Stanley R. P. Enumerative Combinatorics / Richard P. Stanley. – V.1. – 2nd ed. – New York : Cambridge University Press, 2011. – 725 p. ISBN13: 978-1107602625, ISBN10: 1107602629.
16. The on-line encyclopedia of integer sequences. A008302. – Режим доступа : http://oeis.org/A008302.
17. Кнут Дональд Э. Искусство программирования. В 7 т. Т.3. Сортировка и поиск, 2-е изд. / Дональд Эрвин Кнут ; пер. с англ. под ред. В. Т. Тертышного и И. В. Красикова. – М. : ООО «И. Д. Вильямс», 2007. – 832 с. ISBN: 978-5-8459-0082-1.
18. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк Изд. 2-е. – М. : Советское радио, 1970. – 728 с.

Article was submitted 31.12.2017.
After revision 22.01.2018.

Фауре Э. В.[1], Щерба А. И.[2], Харин А. А.[3]

ФАКТОРІАЛЬНІ КОДИ З ЗАДАНИМ ЧИСЛОМ ІНВЕРСІЙ

[1]Канд. техн. наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна

[2]Канд. фіз.-мат. наук, доцент, зав. кафедри прикладної математики Черкаського державного технологічного університету, Черкаси, Україна

[3]Аспірант кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна

Актуальність. Факторіальне кодування з відновленням даних за перестановкою забезпечує комплексний захист інформації від несанкціонованого читання і помилок в каналі зв'язку і має властивість самосинхронізації. У той же час, таке кодування не дозволяє виявити всі помилки малої кратності, що призводить до порівняно невеликого показника підвищення достовірності.

Метою цієї роботи є розробка та дослідження методу факторіального кодування з заданим числом інверсій, спрямованого на підвищення достовірності передавання інформації за рахунок введення додаткової надлишковості шляхом вибору класу перестановок, які відповідають заданому критерію.

Метод. Основна ідея пропонованого методу полягає в штучному внесенні надлишковості за рахунок зменшення потужності використовуваних перестановок. Такий підхід дозволяє з усієї множини перестановок виділити клас, який володіє необхідними, наперед заданими, властивостями. У якості ознаки приналежності до використовуваного класу перестановок у роботі запропоновано використовувати відповідність числа їх інверсій заданому класу лишків. Виконано теоретичну оцінку параметрів коду.

Результати. Побудовано сигнально-кодові конструкції для факторіального коду з заданим числом інверсій для порядку перестановок $M = 8$. Для кожного з можливих класів досліджено потужність, швидкість коду, оцінку ймовірності невиявленої помилки і відносної швидкості передавання для систем з вирішальним зворотним зв'язком і незалежними бітовими помилками. Показано, що параметри коду не є інваріантними по відношенню до вибраного класу лишків для заданого модуля. Розроблено структурні схеми пристроїв кодування та декодування.

Висновки. Отримав подальший розвиток метод факторіального кодування з відновленням даних за перестановкою, який за рахунок використання перестановок, число інверсій у яких належить обраному класу лишків, дозволив підвищити достовірність передавання в обмін на втрату швидкості коду.

Ключові слова: факторіальне кодування, перестановка, інверсія, надлишковість, клас лишків, достовірність передавання, відносна швидкість передавання.

Фауре Э. В.[1], Щерба А. И.[2], Харин А. А.[3]

[1]Канд. техн. наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина

[2]Канд. физ.-мат. наук, доцент, зав. кафедры прикладной математики Черкасского государственного технологического университета, Черкассы, Украина

[3]Аспирант кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина

ФАКТОРИАЛЬНЫЕ КОДЫ С ЗАДАННЫМ ЧИСЛОМ ИНВЕРСИЙ

Актуальность. Факториальное кодирование с восстановлением данных по перестановке обеспечивает комплексную защиту информации от несанкционированного чтения и ошибок в канале связи и обладает свойством самосинхронизации. В то же время, такое кодирование не позволяет обнаружить все ошибки малой кратности, что приводит к сравнительно небольшому показателю повышения достоверности.

Целью данной работы является разработка и исследование метода факториального кодирования с заданным числом инверсий, направленного на повышение достоверности передачи информации за счет введения дополнительной избыточности путем выбора класса перестановок, удовлетворяющих заданному критерию.

Метод. Основная идея предлагаемого метода состоит в искусственном внесении избыточности за счет уменьшения мощности используемых перестановок. Такой подход позволяет из всего множества перестановок выделить класс, обладающий необходимыми, наперед заданными, свойствами. В качестве признака принадлежности к используемому классу перестановок в работе предложено использовать соответствие числа их инверсий заданному классу вычетов. Выполнена теоретическая оценка параметров кода.

Результаты. Построены сигнально-кодовые конструкции для факториального кода с заданным числом инверсий при порядке перестановок $M = 8$. Для каждого из возможных классов исследованы мощность, скорость кода, оценки вероятности необнаруженной

ошибки и относительной скорости передачи для систем с решающей обратной связью и независимыми битовыми ошибками. Показано, что параметры кода не являются инвариантными по отношению к выбранному классу вычетов при заданном модуле. Разработаны структурные схемы устройств кодирования и декодирования.

Выводы. Получил дальнейшее развитие метод факториального кодирования с восстановлением данных по перестановке, который за счет использования перестановок, число инверсий в которых принадлежит выбранному классу вычетов, позволил повысить достоверность передачи в обмен на потерю скорости кода.

Ключевые слова: факториальное кодирование, перестановка, инверсия, избыточность, класс вычетов, достоверность передачи, относительная скорость передачи.

REFERENCES

1. Faure E'. V., Shvydkii V. V., and Shcherba A. I. Kontrol' celostnosti informacii na osnove faktorial'noj sistemy schisleniya, *Journal of Baku Engineering University, Mathematics and Computer Science,* 2017, Vol. 1, No. 1, pp. 3–13.
2. Faure E'. V., Shvydkii V. V., and Shcherba V. A. Kombinirovannoe faktorial'noe kodirovanie i ego svoistva, Radioelektronika, informatika, upravlinnya, 2016, No. 3, pp. 80–86. DOI: 10.15588/1607-3274-2016-3-10.
3. Rudnyc'kyj V. M., Faure E'. V., Shvydkyj V. V., and Shherba A. I. Pat. 107655 Ukrai'na, MPK G06F 21/64 (2013.01), H04L 1/16 (2006.01). Sposib kontrolju cilisnosti informacii'; zajavnyk ta patentovlasnyk Cherkas'kyj derzhavnyj tehnologichnyj universytet. – № a201505937; zajavl. 16.06.2015; opubl. 24.06.2016, Bjul. № 12.
4. Rudnyc'kyj V. M., Faure E'. V., Shvydkyj V. V., and Shherba A. I. Pat. 107657 Ukrai'na, MPK H03M 13/09 (2006.01), H04K 1/06 (2006.01), G09C 1/06 (2006.01). Sposib kombinovanogo koduvannja informacii'; zajavnyk ta patentovlasnyk Cherkas'kyj derzhavnyj tehnologichnyj universytet. № a201508148 ; zajavl. 17.08.2015; opubl. 24.06.2016, Bjul. № 12.
5. Faure E'. V. Faktorial'noe kodirovanie s vosstanovleniem dannykh, Visnik Cherkas'kogo derzhavnogo tekhnologichnogo universitetu, 2016, No. 2, pp. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932.
6. Faure E'. V. Metod povysheniya effektivnosti faktorial'nogo kodirovaniya s vosstanovleniem dannykh, Visnik Cherkas'kogo derzhavnogo tekhnologichnogo universitetu, 2016, No. 4, pp. 57–61.
7. Faure E'. V. Faktorial'noe kodirovanie s neskol'kimi kontrol'nymi summami, Visnik Zhitomirs'kogo derzhavnogo tekhnologichnogo universitetu, 2016, No. 3, pp. 104–113. DOI: 10.26642/tn-2016-3(78)-104-113.
8. Faure E'. V., Harin O. O., Shvydkyj V. V., and Shherba A. I. Pat. 117004 Ukrai'na, MPK H03M 13/09 (2006.01), H04L 1/16 (2006.01), G04C 1/06 (2006.01). Sposib faktorial'nogo koduvannja z vidnovlennjam danyh; zajavnyk ta patentovlasnyk Cherkas'kyj derzhavnyj tehnologichnyj universytet. № u201613641 ; zajavl. 30.12.2016; opubl. 12.06.2017, Bjul. № 11.
9. Faure E'. V. Faktorial'noe kodirovanie s ispravleniem oshibok, *Radio Electronics, Computer Science, Control,* 2017, No. 3, pp. 130–138. DOI: 10.15588/1607-3274-2017-3-15.
10. Graham R. L., Knuth D. E., and Patashnik O. Concrete mathematics: a foundation for computer science. 2nd ed. Reading, Massachusetts, Addison-Wesley, 1994, 657 p. ISBN13: 978-0201558029, ISBN10: 0201558025.
11. MacMahon P. A. The indices of permutations and the derivation therefrom of functions of a single variable associated with the permutations of any assemblage of objects, American Journal of Mathematics, 1913, No. 35, Vol. 3, pp. 281–322. DOI: 10.2307/2370312.
12. Comtet L. Advanced Combinatorics, Dordrecht, D. Reidel Publishing Company, 1974, 343 p. DOI: 10.1007/978-94-010-2196-8.
13. Moritz R. H. and Williams R. C. A Coin-Tossing Problem and Some Related Combinatorics, Mathematics Magazine, 1988, No. 1, Vol. 61, pp. 24-29. DOI: 10.2307/2690326.
14. Mendes A. A Note on Alternating Permutations, The American Mathematical Monthly, 2007, No. 5, Vol. 114, pp. 437-440.
15. Stanley R. P. Enumerative Combinatorics, V.1., 2nd ed., New York, Cambridge University Press, 2011, 725 p. ISBN13: 978-1107602625, ISBN10: 1107602629.
16. The on-line encyclopedia of integer sequences. A008302, Rezhim dostupa: http://oeis.org/A008302.
17. Knuth Donald E. [Per. s angl. pod red. Tertyshnogo V. T. i Krasikova I.V.]. Iskusstvo programmirovaniya. V 7 t. Vol. 3. Sortirovka i poisk, 2-e izd., M, OOO «I.D. Vil'yams», 2007, 832 p. ISBN: 978-5-8459-0082-1.
18. Fink L. M. Teoriya peredachi diskretnykh soobshchenii. [Izd. 2-e.]. M., Sovetskoe radio, 1970, 728 p.