Construction of Cryptosystem on the Basis of Triangular Codes

Tkachenco V.G.₁*, Sinyavsky O.V.₂

₁Odessa National Academy of Telecommunications named after O.S.Popov, 65029, Odessa, str. Kovalska 1, Ukraine
₂Military Academy (Odessa), 65009, Odessa, str. Fontansky road, 10, Ukraine
*Corresponding Author: vgtkach@mail.ru

Abstract In this article the triangular codes found dependence of the power of these codes on the length of codewords in them. The methods of construction codes and some triangular propose an effective general method for constructing such codes based on monotone Boolean functions. Designed with correcting codes cryptosystem on the basis of such a code, which allows one to correct the error. The advantage of this cryptosystem is the speed of coding and decoding, and the ability to quickly change the code without changing tables, coding and decoding. Change the code is implemented using the substitution, and the choice of codes is very large. The number of possible codes is 20! (approximately equal to 2.4*10¹⁸) has at length codeword of 20.

Keywords Correcting Codes, Nonlinear Triangular Codes, Cryptosystem, Steiner System, Affine Plane, Projective Plane

1. Introduction

In the process of transmitting information in cryptosystems over telecommunications networks raises the problem of error correction. Control of data integrity and error correction - important tasks at many levels of work with information. One means of solving these problems is the use of the noiseproof codes that underlie the encoding-decoding systems.

Different noiseproof codes for cryptosystems, differing from each other by the basis, distance, redundancy, structure, a functional purpose, correlation properties, algorithms of coding and decoding, a form of a frequency range ([1] - [4]) are so far developed many. On the basis of the maximum types of monotonous Boolean functions (MBF) [5] it is constructed cryptosystems [6], allowing correction of mistakes.

However algorithm of decoding that is used in [6] it is rather difficult, and change of a code demands creation of four new arrays with use of a set of additional operations.

The aim of this work is to develop a code that corrects single errors in the transmission of information in cryptosystems at the expense of no more than 5 readings from the decoding table. To change this code requires only one substitution.

2. Results

In this article as codewords we will consider vectors lengths \( n \) \( \tilde{a} = \left( a_{n-1}, \ldots, a_i, \ldots, a_0 \right) \), which components accept values from a set \( \{0,1\} \), and the number of identity components in a vector is equal to 3. Such codewords have Hamming weight equal to 3. Hamming distance between two codewords \( \tilde{a} \) and \( \tilde{b} \) is called \( \rho(\tilde{a},\tilde{b}) \) the number equal to quantity a component in which they differ. In total such codewords with weight 3 can be \( 2^n \). Code distances between different words in this case can be 2, 4 or 6. For correcting codes only codewords with distance 4 or 6 are applicable. The number of codewords is called as code power. Such codes with code distance 6 are uninviting, as their power is small and is always equal \( \left[ \frac{n}{3} \right] \). Let's consider further the maximum codes with \( \rho(\tilde{a},\tilde{b}) \geq 4 \). From determination of Hamming distance follows that in such codes for each pair of codewords of the general there can be only one unit. It is easy to present such codes in the form of monotonous Boolean functions of a rank \( n \), weight 1 and power \( m \), where \( m \) equally to code power. Let's call such codes triangular.

For research of such codes it is possible to use the theory of graphs. In this case bits of codewords correspond to tops of the graph, and codewords correspond to triangles in this graph(edges in a triangle connect tops which correspond to unit bits in codewords). Thus, since \( \rho(\tilde{a},\tilde{b}) \geq 4 \), that no 2 triangles in the constructed graph have the general edges, i.e. they or have one general top or are not crossed. The number of such triangles being crossed in top \( i \) let's denote through
Lemma 1. For all triangular codes exist top boundary number of codewords equal \( \frac{n(n-1)}{6} \).

**Proof.** Granting that these triangles cannot have general edges, the sum \( \sum_{i=1}^{n} t_i \) of cannot be greater than the number of edges. Therefore, the ratio is fair \( \frac{1}{2} \)

It is obvious that the number of triangles will be in 3 times less number of edges, i.e. \( \frac{n(n-1)}{6} \). The proof of a lemma is ended.

Let's call uninvolved edges in the constructed graph all edges, supplementing this graph to the stout graph.

Lemma 2. If \( n \) even, number of uninvolved edges, incidental to any top of the graph, is odd. If \( n \) odd, number of uninvolved edges, incidental to any top of the graph, is the even.

**Proof.** From each top of the constructed graph come \( 2t_i \) even numbers of edges. To in total top of the stout graph with \( n \) tops incidental to \( n - 1 \) edges. Therefore, for the odd there is an even number of uninvolved edges and on the contrary, for even \( n \) there is an odd number of uninvolved edges. The proof of a lemma is ended.

Concerning power of considered codes it is possible to prove the following statements.

**Theorem 1.** Let \( n \) – even, such that \( n \not\equiv 4 \pmod{6} \). Then the code power does not exceed \( \frac{n(n-2)}{6} \).

**Proof.** We have \( n = 2k \), where \( k \not\equiv 2 \pmod{3} \). Considering a lemma 2, each top should leave, at least, one uninvolved edge. The smallest number of such edges can be carried out, if they in pairs are not adjacent, i.e. form a matching. In this case from each top come \( n-2 \) edges which are involved in triangles, i.e. for all tops \( t_i \) equally, i.e. \( t_i = t \) and \( \sum_{i=1}^{n} t_i = t \sum_{i=1}^{n} 1 = n(n-1) \). Therefore, \( t \leq \frac{n-1}{2} \). Then, \( t = \frac{n}{2} - 1 = \frac{2k}{2} - 1 = k - 1 \).

Considering that \( t \cdot n = 2k(k-1) \) and \( k \not\equiv 2 \pmod{3} \), that \( t \cdot n \) will share totally on 3. Therefore in this case maximum number of triangles \( \frac{t \cdot n}{3} = \frac{2k(k-1)}{3} = \frac{n(n-1)}{6} \).

The number of uninvolved edges on construction is equal \( \frac{n}{2} \). The theorem is proved.

**EXAMPLE 1.** For \( n = 6 \). Maximum number of triangles

\[
\frac{6(6-2)}{6} = 4.
\]

Uninvolved edges (numbering of tops starts from zero): (0,3), (1,4), (2,5). They form a matching, see fig. 1.

![Figure 1](image1.png)

**Figure 1.** The scheme of uninvolved edges for \( n = 6 \)

Adjacency matrix of the graph corresponding to a code with \( n = 6 \), it is shown in table 1.

| tops | 0   | 1   | 2   | 3   | 4   | 5   |
|------|-----|-----|-----|-----|-----|-----|
| 0    | 0   | 1   | 1   | 0   | 1   | 1   |
| 1    | 1   | 0   | 1   | 1   | 0   | 1   |
| 2    | 1   | 1   | 0   | 1   | 1   | 0   |
| 3    | 0   | 1   | 1   | 0   | 1   | 1   |
| 4    | 1   | 0   | 1   | 1   | 0   | 1   |
| 5    | 1   | 1   | 0   | 1   | 1   | 0   |

Numbers of unit tops in each triangle:

(0,1,2), (2,3,4), (1,3,5), (0,4,5).

In this case we have the block design from 4 elements placed on 4 blocks, in each block on 3 elements. This code it is possible to present in the form of monotonous Boolean function, where number of top of a triangle on 1 less numbers of a variable in function:

\[
x_1 x_2 x_3 \lor x_3 x_4 x_5 \lor x_2 x_4 x_6 \lor x_1 x_5 x_6
\]

**EXAMPLE 2.** For \( n = 8 \). Maximum number of triangles

\[
\frac{8(8-2)}{6} = 8.
\]

Uninvolved edges (numbering of tops starts from zero): (0,4), (1,5), (2,6), (3,7). They form a matching (fig. 2).

![Figure 2](image2.png)

**Figure 2.** The scheme of uninvolved edges for \( n = 8 \)

Numbers of unit tops in each triangle:

(0,5,6), (0,1,3), (0,2,7), (1,2,4), (1,6,7), (2,3,5), (3,4,6), (4,5,7).

In this case we have the block design from 8 elements placed on 8 blocks, in each block on 3 elements.

**Theorem 2.** Let \( n \) – even, such that \( n \equiv 4 \pmod{6} \).

Then the power of a code does not exceed \( \frac{n(n-2)-2}{6} \).
Proof. In this case \( n = 2k \), where \( k \equiv 2 \pmod{3} \). If to construct the same matching as in the previous theorem, then number of other edges \( C_n^2 - \frac{n(n-2)}{2} = \frac{n(n-2)}{2} \). As \( n = 4 \pmod{6} \), and \( n-2 \equiv 2 \pmod{6} \), that this number \( \frac{n(n-2)}{2} \) not divided into 3 and all other edges cannot be used for creation of triangles. From a lemma 2 follows that the odd number of uninvolved edges should proceed from each top of our graph. The minimum number of uninvolved edges turns out when for \( n-4 \) tops of the graph the matching, containing is under construction \( \frac{n-4}{2} \) uninvolved edges, and uninvolved edges from other 3 tops meet in the fourth top and form a three-beam star. In total is available \( \frac{n-4}{2} + 3 \) uninvolved edges.

From creation of uninvolved edges follows that in each top, except the star center, it is crossed \( t = \frac{n-2}{2} \) triangles. In top of a star corresponding to the center less triangles are crossed on unit \( \frac{n-4}{2} \).

We have

\[
t \cdot (n-1) + t - 1 = t \cdot n - 1 \leq C_n^2 = \frac{n(n-1)}{2}.
\]

Then

\[
t \leq \frac{n-1}{2} + \frac{1}{n}.
\]

From here \( t = k-1 \), where \( n = 2k \).

Number of triangles in this case

\[
t \cdot n - 1 = \frac{2k(k-1)}{3} = \frac{n(n-1)}{3} - 1 = \frac{n(n-2) - 2}{6}
\]

The theorem is proved.

Any other arrangement, considering a lemma 2, will give smaller number of the involved edges.

EXAMPLE 3. For \( n = 10 \). Number of triangles

\[
\frac{10(10-2)-2}{6} = 13.
\]

Uninvolved edges: \((0,3)\), \((1,4)\), \((2,5)\), \((6,9)\), \((7,9)\), \((8,9)\).

The adjacency matrix of the graph corresponding to a code with 10, is shown in table 2.

| tops | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|------|---|---|---|---|---|---|---|---|---|----|
| 1    | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1  |
| 2    | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1  |
| 3    | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1  |
| 4    | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1  |
| 5    | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1  |
| 6    | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1  |
| 7    | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0  |
| 8    | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0  |
| 9    | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0  |
| 10   | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0  |

Theorem 3. Let \( n \) – odd, such that \( n \not\equiv 5 \pmod{6} \). Let as there is a triangular code with codewords of length \( k = n-1 \). Then there is a code with codewords of length \( n \) and its power is equal to the top border for triangular codes \( \frac{n(n-1)}{6} \).

Proof. When number of tops \( n \) odd such that \( n \not\equiv 5 \pmod{6} \), that \( n-1 \) even and \( n-1 \not\equiv 4 \pmod{6} \). On proved above number of triangles for \( n-1 \) equally \( \frac{(n-1)(n-3)}{6} \). Number of uninvolved edges equally \( \frac{n-1}{2} \) and they are not crossed, forming a matching. In this case for the last \( n-1 \) tops can be constructed with \( \frac{n-1}{2} \) uninvolved edges \( \frac{n-1}{2} \) new triangles.

Therefore number of triangles for this case:

\[
\frac{(n-1)(n-3)}{6} + \frac{n-1}{2} = \frac{n(n-1)}{6}.
\]

It is easy to see that in this case there are no uninvolved edges. All edges are involved. The theorem is proved.

As 2-scheme or simply the block design is called \([7,8]\) set of subsets (called by blocks) sets \( S \), consisting from \( v \) points, such that each block contains \( k \) points, and any set from two points contains exactly in \( \lambda \) blocks. In a case \( \lambda = 1 \) the block design is called as Steiner system \([7,8]\).

Codes from the theorem 3 are block designs with parameters \( v = n \), \( k = 3 \), \( \lambda = 1 \). Thus, the specified codes are Steiner systems.
EXAMPLE 4. For $n = 7$. Number of triangles \( \frac{7(7-1)}{6} = 7 \).

Numbers of unit tops in each triangle:

\( (0,3,6), (0,4,5), (0,1,2), (1,3,5), (1,4,6), (2,5,6), (2,3,4) \).

If instead of tops of triangles to consider points on a straight line, in this case we have \( 2^2 + 2 + 1 = 7 \) points and 7 straight lines which contain on 3 points and this set satisfies to axioms of the projective plane \([7,9]\).

Through two different points of \( P \) and \( Q \) of the plane there passes a straight line, and only one. Any two straight lines have the general point. There are three points which are not lying on one straight line. Each straight line contains not less than three points. Therefore we have the projective plane of the 2nd order or Fano’s plane.

EXAMPLE 5. For $n = 9$. Number of triangles \( \frac{9(9-1)}{6} = 12 \).

Numbers of unit tops in each triangle:

\( (4,3,5), (6,4,8), (0,5,6), (0,4,7), (1,3,0), (3,8,7), (1,5,8), (1,6,7), (2,3,6), (2,4,1), (2,5,7), (2,0,8) \).

In this case we have the affine plane of the 3rd order. \( 3^2 = 9 \) points, \( 3^2 + 3 = 12 \) straight lines which satisfy to axioms \([7,9]\).

1. For any two different points there is only one straight line containing these points.
2. Crossing of two different straight lines contains exactly one point.
3. There is a set from four points, any three of which do not belong to one straight line.

The affine plane of the third order can be received from the projective plane of the third order, deletion of one straight line and the 4th points lying on it.

**Theorem 4.** Let \( n \) – odd, such that \( n \equiv 5 \pmod{6} \). Suppose there is also a triangular code with codewords of length \( k = n-1 \). Then there is a code with codewords of length \( n \) and its power is equal \( \frac{n(n-1)-8}{6} \).

**Proof.** For a case, when \( n \) odd and \( n \equiv 5 \pmod{6} \), for the even \( n-1 \) on proved above (see a theor. 2), we have \( \frac{(n-1)(n-3)-2}{6} \) triangles and \( \frac{n-5}{2} + \frac{n+1}{2} \) uninvolved edges. Then the last \( n \) - th top it is possible to construct with \( \frac{n+1}{2} - 2 \) uninvolved edges (one beam of a three-beam star since otherwise will be crossings of triangles on an edge is used) \( \frac{n-3}{2} \) new triangles.

Therefore number of triangles for this case:

\[ \frac{(n-1)(n-3)-2}{6} + \frac{n-3}{2} = \frac{n(n-1)-8}{6} \]

Number of uninvolved edges:

\[ C_n^2 - \frac{n(n-1)-8}{6} - \frac{n(n-1)-8}{2} = 4 \]

The theorem is proved.

In case codes from the theorem 4 uninvolved edges with new top and two uninvolved beams of a star form a quadrangle since in this case on a lemma 2 top leaves even number of uninvolved edges.

EXAMPLE 6. For $n = 11$. Number of triangles \( \frac{11(11-1)}{6} = 17 \).

Uninvolved edges: \( (6,10) \) \( (6,9) \) \( (8,9) \) \( (8,10) \). A quadrangle from them:

![Figure 4. The scheme of uninvolved edges for $n = 11$](image)

Numbers of unit tops in each triangle:

\( (0,6,8), (0,9,10), (0,4,5), (0,1,3), (1,2,9), (1,4,10), (1,6,7), (1,5,8), (2,4,8), (2,3,10), (2,5,6), (3,5,9), (3,4,6), (3,7,8), (4,7,9), (5,7,10) \).

**Theorem 5.** Let there is a triangular code with codewords of length \( k \) ( \( k \) odd and \( k \not\equiv 5 \pmod{6} \)) power \( \frac{k(k-1)}{6} \). Then there exists a triangle with the codewords of the code length \( 2^{nk} \) power \( \frac{k(k-1)}{6} \).

**Proof.** Let there is a code with words of code length \( k \). Let's put in compliance to everyone \( i \)- th to bit from a codeword of this code the following couple of bits: \( (i+k) \). Let's define that these bits in uninvolved pairs in a code which existence we prove. Let's take from an existing code any codeword of length \( k \). Let unit bits in this codeword have numbers \( i, j, t \). Let's construct of these pairs 4 triangles with tops: 1) \( (i+k), (j+k), (t+k) \). Let's construct of these pairs 4 triangles with tops: 1) \( (i+k) \), \( (j+k) \), \( (t+k) \). Having done such operation for any codeword, we will receive \( 4m \) codewords of length \( n = 2k \). At such construction no 2 triangles have
the general edges. It is obvious that the constructed 4 triangles, from unit bits \(i,j,t\) codeword have no general edges. Let's say that the general edge with a triangle which turns out from unit bits has 4 triangles any of these \(i\), \(j\), \(t\) codeword. From here, considering that in an initial codeword we add length of this codeword to word bits, i.e. we shift the bits corresponding to top of a triangle, on distance equal to length of a codeword, follows that triangles from an initial code with length of a codeword \(k\) also should have the general edges. Really, let 2 triangles have the general edge \((i+s,j+s)\) in the first triangle and \((i_1+s,j_1+s)\) in the second, where \(s\) can accept values or \(k\), or 0. Let \(i<j\) and \(i_1<j_1\). Then, since triangles are crossed on this edge, should be satisfied a condition \(i+s=i_1+s\) here \(s\) at the same time or \(k\), or 0, and \(j+s=j_1+s\) here \(s\) as at the same time or \(k\), or 0, from this it follows that \(i=i_1\) and \(j=j_1\). And it means that triangles from an initial code with length of a codeword \(k\) have the general edges that contradicts code definition. The theorem is proved.

CONSEQUENCE. Serially application of theorems 5 and 3 to a triangular code with codewords of odd length of \(n\) unequal 5 on the module 6 leads to infinite sequence of codes with the infinitely increasing \(n\), in which codes with odd and even alternate \(n\). In this sequence triangular codes with the odd \(n\) have no uninvolved edges.

EXAMPLE 7. A triangular code with \(n=3\) has power \(m=1\). Applying the theorem 5, we will receive a code with \(n=5\) and \(m=4\). Applying the theorem 3, we will receive a code with \(n=7\) and \(m=7\). Repeated applications of these theorems leads to sequence of codes with lengths of codewords equal 3, 6, 7, 14, 15, 30, 31, 62, 63, 126, 127, 254, 255, 510, 511, 1022. Capacities of these codes by theorems 3 and 5 are equal 1, 4, 7, 28, 35, 140, 155, 620, 651, 2604, 2667, 10668, 10795, 43180, 43435, 173740 respectively.

Table 3 shows the dependence of the triangular code of codeword length.

| Length codewords \(n\) | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Code power \(m\)       | 4  | 7  | 8  | 12 | 13 | 17 | 20 | 26 | 28 | 35 | 37 | 43 | 48 | 57 | 60 |

We show that this Steiner system. Since no two triples of the 6 have no common pairs. Since no two of Steiner triple systems \(S_1\) (or \(S_2\)) have no common pairs, the common pairs will not have the triple constructed of pairs of elements of these systems.

On construction number triple in the constructed system \(S\) equally \(v_1 b_1 + v_2 b_2 + 6 b_1 b_2\). For any block designs formulas [8] are carried out: \(bk = vr\), \(r = \lambda(v – 1)(k – 1)\). For Steiner systems with \(k=3\) these formulas look like: \(3b = vr = (v – 1)/2\). From here follows \(b = v(v – 1)/6\). Substituting this expression instead of \(b_1\) and \(b_2\) we receive \(v_1 b_2 + v_2 b_1 + 6 b_1 b_2 = \frac{v_1 v_2 (v_1 v_2 – 1)}{6}\), that is equal to number of triple in Steiner system \(S\). Number of repetitions of each element in this triples equal to \(\frac{v_1 b_2 + v_2 b_1 + 6 b_1 b_2}{v_1 v_2} = \frac{v_1 v_2}{v_1} + \frac{3 b_2}{v_2} + \frac{18 b_1 b_2}{v_1 v_2} = \frac{v_1 v_2 – 1}{2}\).

The theorem is proved.
EXAMPLE 8. Using the previous theorem, from block designs $S_1 (3,1,1,3)$ and $S_2 (3,1,1,3)$ let's receive $S(9,12,4,3,1)$. On the basis of these block designs we can receive infinite sequence of schemes:

$$S(9,12,4,3,1) \Rightarrow S(27,117,13,3,1) \Rightarrow \ldots$$

In some cases and power it is convenient to apply Moore's theorem which proof is provided in [7] to recursive creation of triangular codes of bigger length.

Moore's theorem. Let there are Steiner triple systems of orders $v_1$ and $v_2$: $S_1(v_1, b_1, r_1, 3)$ and $S_2(v_2, b_2, r_2, 3)$. Let also or $v_3=1$, or $v_3$ is order of Steiner triple systems $S(v_3, b_3, r_3, 3)$, which is a subsystem in $S_1$. Then it is possible to construct Steiner triple systems $S(v,b,r,3)$ with $v = v_3 + v_1 (v_2 - v_3)$, the containing $v_1$ order subsystems $v_2$ and at least on one subsystem of orders $v_1$ and $v_3$ (if $v_3$ not equally 1).

Let's show 2 examples of construction on the basis of Moore's theorem.

EXAMPLE 9. Let $v_1=3$, $v_2=3$ and $v_3=1$. Steiner system $S_1(3,1,1,3)$ and $S_2(3,1,1,3)$ are equal and consist of one block $(1,2,3)$. As $v_3=1$, as a row $L_0$ we choose $L_0=(1)$. As $v_1=3$ and $v_2=3$, as rows $L_1-L_3$ we choose $L_1=(2,3)$, $L_2=(4,5)$ and $L_3=(6,7)$, on $v_2-v_3=2$ elements in every row. At the first stage we check a row $L_0$, but it does not contain triple from $S_2$. At the second stage we take on 1 element from $L_0$ and on 2 elements from one of rows $L_1-L_3$ so that they formed the triple in $S_2$. Triple of such triples: 1) $(1,2,3)$, 2) $(1,4,5)$ and 3) $(1,6,7)$. At the 3rd stage we construction triple from rows $L_1-L_3$, choosing on 1 element from every row. For this purpose at first we find what indexes of 3 elements from these rows give in the sum 0 on the module $v_2-v_3=2$. Such triple of indexes four: 1) $(1,2,2)$, 2) $(1,2,1)$, 3) $(2,1,1)$ and 4) $(2,2,2)$. To them correspond triple: 4) $(2,4,7)$, 5) $(2,5,6)$, 6) $(3,4,6)$ and 7) $(3,5,7)$. Steiner system is received $S(7,7,3,3)$.

EXAMPLE 10. Let $v_1=3$, $v_2=7$ and $v_3=1$. Steiner system $S_1(3,1,1,3)$ and $S_2(3,1,1,3)$ are equal and consist of one block $(1,2,3)$. In quality $S_3(7,7,3,3)$ we choose the projective plane: 1) $(1,2,3)$, 2) $(1,4,5)$, 3) $(1,6,7)$, 4) $(2,4,7)$, 5) $(2,5,6)$, 6) $(3,4,6)$ and 7) $(3,5,7)$. As a row $L_0$ we choose $L_0=(1,2,3)$. As $v_1=3$ and $v_2=7$, as rows $L_1-L_6$ we choose $L_1=(4,5,6,7)$, $L_2=(8,9,10,11)$ and $L_3=(12,13,14,15)$, on $v_2-v_3=4$ elements in every row. At the first stage we check a row $L_0$, which contains the triple 1) $(1,2,3)$ of $S_2$. At the second stage we take on 1 element from $L_0$ and on 2 elements from one of rows $L_1-L_6$ so that they formed the triple in $S_2$. Such triple 18: 2) $(1,4,5)$, 3) $(1,6,7)$, 4) $(2,4,7)$, 5) $(2,5,6)$, 6) $(3,4,6)$, 7) $(3,5,7)$, 8) $(1,8,9)$, 9) $(1,10,11)$, 10) $(2,8,11)$, 11) $(2,9,10)$, 12) $(3,8,10)$, 13) $(3,9,11)$, 14) $(1,12,13)$, 15) $(1,14,15)$, 16) $(2,10,15)$, 17) $(2,13,14)$, 18) $(3,10,14)$ and 19) $(3,13,15)$. At the 3rd stage we construction triple from rows $L_1-L_6$, choosing on 1 element from every row. For this purpose at first we find what indexes of 3 elements from these rows give in the sum 0 on the module $v_2-v_3=4$. Such triple of indexes 16: 1) $(1,1,2)$, 2) $(1,2,1)$, 3) $(2,1,1)$, 4) $(1,3,4)$, 5) $(1,4,3)$, 6) $(3,1,4)$, 7) $(3,4,1)$, 8) $(4,1,3)$, 9) $(4,3,1)$, 10) $(2,2,4)$, 11) $(2,4,2)$, 12) $(4,2,2)$, 13) $(2,3,3)$, 14) $(3,2,3)$, 15) $(3,3,2)$ and 16) $(4,4,4)$. To them there correspond triple: 20) $(4,8,13)$, 21) $(4,9,13)$, 22) $(5,8,12)$, 23) $(4,10,15)$, 24) $(4,11,14)$, 25) $(6,8,15)$, 26) $(6,11,12)$, 27) $(7,8,14)$, 28) $(7,10,12)$, 29) $(5,9,15)$, 30) $(5,11,13)$, 31) $(7,9,13)$, 32) $(5,10,14)$, 33) $(6,9,14)$, 34) $(6,10,13)$ and 35) $(7,11,15)$. Steiner system is received $S(15,35,7,3)$.

As the Hamming distance between any codewords not less than 4, such triangular code can correct one symbol of a transferred codeword. Codewords in the table of coding are ordered on increase.

Decoding is carried out by means of the table (the two-dimensional array) where in headings of rows and columns numbers of unit bits, and in the table of number of codewords will be written down. We determine the transferred information message by numbers of two bits of a codeword. Thus numbers of columns correspond to LSB and numbers of rows to the MSB of the transferred message.

EXAMPLE 11. For a triangular code with $n = 12$ on the channel cryptosystem two messages 2 and 1 are transferred. These messages are coded by two codewords (according to table 4): 00000011001 and 000000001111, i.e. all 24 bits are transferred. Let two codewords 00000010001 and 000100000111 have been accepted. At reception numbers of bits of codewords for the 1st codeword are defined these are bits: 0, 4, for the 2nd–0, 1, 2, 7. Let's apply the decoding table (table 5) for definition of the devoted message corresponding to the first codeword. Number of unit LSB of the transferred word is equal 0, and number of the MSB 4. On crossing of the corresponding row and a column costs 2. It means that the message 2 is transferred. The error of transfer for the 1st codeword is corrected.

Let's consider, how there is a decoding in case instead of triple unit bits 4 unit bits, on an example of the second codeword were accepted. It is possible to form 6 pairs of unit bits of the 2nd codeword: 0) (1), (0, 2), (1, 2), (0, 7), (1, 7), (2, 7). To these pairs in the table of decoding there correspond the transferred messages: 1, 1, 1, 6, 0, 17 (0 designates that to this pair there does not correspond any message). Rub from found in the table messages are identical and equal 1. It means that 3 first couples of bits form the second codeword, i.e. the codeword 000000000111 has been transferred. The error of transfer for the 2nd codeword is corrected. It is possible to show that in case of reception of 4 bits instead of triple it is enough to find in tables for the received pairs two conterminuous messages, i.e. in the given example instead of 6 pairs was to check only pairs (0 enough; 1) and (0; 2). In the worst case it is enough to check the 5 pairs that requires 5 readings from table 4.

The power of this code can be increased twice if to codewords of this triangular code to add codewords in which zero and on the contrary are written down instead of units. If to 20 codewords to add 20 more codewords, in which instead of units zero and on the contrary, for $n = 12$ let's receive 40 codewords. Then by means of this code it is possible to code not 20, but 40 messages.
Table 4. Coding table

| Transmitted message | The codewords      |
|---------------------|--------------------|
|                     | decimal form | binary form |
| 1                   | 7           | 0 0 0 0 0 0 0 0 0 0 1 1 1 1 |
| 2                   | 25          | 0 0 0 0 0 0 0 0 1 1 0 0 1 |
| 3                   | 44          | 0 0 0 0 0 0 1 0 1 1 0 0 0 |
| 4                   | 74          | 0 0 0 0 1 0 0 1 0 1 0 1 0 |
| 5                   | 84          | 0 0 0 0 1 0 1 0 1 0 0 0 0 |
| 6                   | 161         | 0 0 0 0 1 0 1 0 0 0 0 1 1 |
| 7                   | 304         | 0 0 0 0 1 0 0 1 1 0 0 0 0 |
| 8                   | 448         | 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 |
| 9                   | 546         | 0 0 1 0 0 0 1 0 0 0 0 1 0 |
| 10                  | 656         | 0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 |
| 11                  | 769         | 0 0 1 1 0 0 0 0 0 0 0 0 1 |
| 12                  | 1120        | 0 1 0 0 0 1 1 0 0 0 0 0 0 0 0 |
| 13                  | 1160        | 0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 |
| 14                  | 1282        | 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 |
| 15                  | 1540        | 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 |
| 16                  | 2066        | 1 0 0 0 0 0 0 0 0 1 0 0 1 0 |
| 17                  | 2180        | 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 |
| 18                  | 2312        | 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 |
| 19                  | 2624        | 1 0 1 0 0 1 0 0 0 0 0 0 0 0 0 |
| 20                  | 3073        | 1 1 0 0 0 0 0 0 0 0 0 0 0 1 |

Table 5. Table decoding

| Bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|------|---|---|---|---|---|---|---|---|---|---|----|----|
| 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 1    | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 2    | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 3    | 2 | 4 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 4    | 2 | 16 | 5 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 5    | 6 | 9 | 3 | 3 | 7 | 0 | 0 | 0 | 0 | 0 | 0 0 |
| 6    | 0 | 4 | 5 | 4 | 5 | 12 | 0 | 0 | 0 | 0 | 0 0 |
| 7    | 6 | 0 | 17 | 13 | 10 | 6 | 8 | 0 | 0 | 0 | 0 0 |
| 8    | 11 | 14 | 0 | 18 | 7 | 7 | 8 | 8 | 0 | 0 | 0 0 |
| 9    | 11 | 9 | 15 | 0 | 10 | 9 | 19 | 10 | 11 | 0 | 0 0 |
| 10   | 20 | 14 | 15 | 13 | 0 | 12 | 12 | 13 | 14 | 15 | 0 0 |
| 11   | 20 | 16 | 17 | 18 | 16 | 0 | 19 | 17 | 18 | 19 | 20 0 |

Let’s consider a triangular code with \( n = 32 \). The power of this code by the theorem 1 is equal 160. If we double power of this code as it is described above, we can code 320 messages. It is enough of it to code all possible binary bytes.

It is possible to show that if in all codewords of a triangular code to rearrange bits by means of the same substitution, the received codewords also form a triangular code. For some codes any such substitution leads to a new code. Such code exists, for example, at \( n = 20 \). In this case by means of substitutions it is possible to form \( 20! = 2 \, 432 \, 902 \, 008 \, 176 \, 640000 \) codes that is approximately equal \( 2.4 \times 10^{18} \).

Applying substitution at a parcel of codewords to the canal cryptosystem and return substitution at their reception, it is easy to change a transferred code. Thus tables of coding and decoding do not change.

3. Conclusions

The main result of article is the universal method of creation of triangular codes on the basis of monotonous Boolean function. In literature triangular codes were not investigated, in the work a number of properties of these
codes is proved. Additional important property of triangular codes is possibility of correction of a single mistake in the accepted codeword. On the basis of triangular codes it is easy to construct cryptosystem with a simple rule of coding, algorithm of decoding and possibility of change of a code one substitution. Owing to possibility of fast change of a code, it can be changed often during transfer. Thus as a key it can be transferred either substitution, or the law of change of substitutions.

REFERENCES

[1] F.J. MacWilliams, N.J.A. Sloane. The theory of error-correcting codes, North-Holland Publishing Company, Amsterdam, 1977, 744.

[2] R.E. Blahut. Theory and practice of error control codes, Addison-Wesley Publishing Company, London, 1983, 576.

[3] E.R. Berlekamp. Algebraic coding theory, McGraw-Hill Book Company 1968, 480.

[4] David J.C. MacKay. Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003.

[5] Ткаченко В.Г. Перечисление типов монотонных булевых функций при синтезе цифровых схем, Наукові праці ОНАЗ ім. О.С. Попова, Одеса, №2, 54 – 69, 2008

[6] Ткаченко В.Г. Синявский О.В., Построение корректирующего кода для криптосистем на основе типов монотонных булевых функций, Наукові праці ОНАЗ ім. О.С. Попова, № 1, 85 – 92, 2010.

[7] Marshall Hall, Jr. Combinatorial theory, Blaisdell Publishing Company, Waltham (Massachusetts), 1967, 424.

[8] P.J. Cameron, J.H. van Lint. Graph Theory and Block Designs, Cambridge University Press, 1975, 144.

[9] F. Karteszi. Introduction to Finite Geometries, Akademiai Kiado, Budapest, 1976, 320.