УДК 519.719.1, 681.322

Ткаченко В. Г., Синявский О. В.
Ткаченко В. Г., Сінявський О. В.
Tkachenco V. G, Sinyavsky O. V.

МЕТОД ПОСТРОЕНИЯ ТРЕУГОЛЬНЫХ КОДОВ ДЛЯ КРИПТОСИСТЕМ

МЕТОД ПОБУДОВИ ТРИКУТНИХ КОДІВ ДЛЯ КРИПТОСИСТЕМ

CONSTRUCTION METHOD OF TRIANGULAR CODES FOR CRYPTOSYSTEMS

Аннотация. В статье определены треугольные коды, найдена зависимость мощности этих кодов от длины кодовых слов в них. Рассмотрены способы построения некоторых треугольных кодов и предложен эффективный универсальный метод построения таких кодов на основе монотонных булевых функций. Разработана криптосистема с корректирующим шифром на основе такого кода, позволяющая исправлять одну ошибку. Достоинствами этой криптосистемы является быстрота шифрации и дешифрации, а также возможность быстрой смены кода без изменения таблиц шифрации и дешифрации. Смена кода реализуется с помощью подстановки, причем выбор кодов очень велик. Число возможных кодов достигает 20! (приближенно равно $2{,}4\cdot10^{18}$) уже при длине кодового слова, равной 20.

Анотація. У статті визначено трикутні коди, знайдена залежність потужності цих кодів від довжини кодових слів в них. Розглянуто способи побудови деяких трикутних кодів і запропонований ефективний універсальний метод побудови таких кодів на основі монотонних булевих функцій. Розроблена криптосистема з коригуючим шифром на основі такого коду, що дозволяє виправляти одну помилку. Перевагами цієї криптосистеми є швидкість шифрування і дешифрування, а також можливість швидкої зміни коду без зміни таблиць шифрації і дешифрації. Зміна коду реалізується за допомогою підстановлення, причому вибір кодів дуже великий. Число можливих кодів досягає 20! (наближено $2{,}4\cdot10^{18}$) вже при довжині кодового слова, що дорівнює 20.

Summary. In this article the triangular codes found dependence of the power of these codes on the length of code words in them. The methods of building 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 advantages of this cryptosystem is the speed of encryption and decryption, and the ability to quickly change the code without changing tables, encryption and decryption. 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 $2.4*10^{18}$) has at length codeword of 20.

В современных криптосистемах широко используются симметричные методы шифрования (с закрытым ключом). Их криптостойкость повышается при использовании малоизвестных кодов и при достаточно частой смене этих кодов [1]. В ряде случаев дополнительно требуется исправлять ошибки, возникающие в процессе передачи. В связи с этим возникает проблема разработки новых корректирующих кодов (кодов с коррекцией ошибок) для криптосистем, с возможностью быстрой смены этих кодов при передаче информации.

К настоящему времени известно много кодов с коррекцией ошибок, отличающихся друг от друга основанием, расстоянием, избыточностью, правилами кодирования и алгоритмами декодирования, спектром расстояний между кодовыми словами ([2] … [4]). На основе максимальных типов [5] монотонных булевых функций (МБФ) построена криптосистема [6], позволяющая коррекцию ошибок.

Однако алгоритм декодирования, используемый в [6], достаточно сложен, а смена кода требует построения четырех новых массивов с использованием множества дополнительных операций.

Целью настоящей статьи является разработка метода построения кода, исправляющего одиночные ошибки при передаче информации в криптосистемах за счет не более 5 считываний из таблицы и требующего для смены кода всего одной подстановки.

В данной статье в качестве кодовых слов будем рассматривать векторы длины n $\tilde{a} = \left(a_{n-1},...,a_i,...,a_0\right)$, компоненты которых принимают значения из множества $\{0,1\}$, и количество единичных компонент в векторе равно 3. Такие кодовые слова имеют вес Хэмминга [4] равный 3. Расстоянием Хэмминга [2] между двумя кодовыми словами $\tilde{a}$ и $\tilde{b}$ называется число $\rho\left(\tilde{a},\tilde{b}\right)$, равное количеству компонент, в которых они различаются. Кодовым расстоянием кода [2] называется

минимальное расстояние Хэмминга среди всех пар кодовых слов кода. Всего кодовых слов длины n с весом 3 может быть C_n^3. Расстояния Хэмминга между различными словами в этом случае могут быть 2, 4 или 6. Для корректирующих кодов применимы только кодовые слова с расстоянием 4 или 6, так как код с кодовым расстоянием ρ может исправлять $(\rho-1)/2$ ошибок ([2] … [4]). Количество кодовых слов в коде называется мощностью кода [3]. Такие коды с кодовым расстоянием 6 малоинтересны, поскольку их мощность мала и всегда равна $[n/3]$. В дальнейшем будем рассматривать максимальные коды с $\rho\left(\tilde{a},\tilde{b}\right)\geq 4$, т.е. те коды, к которым без уменьшения кодового расстояния нельзя добавить ни одного кодового слова. Из определения расстояния Хэмминга следует, что в таких кодах для каждой пары кодовых слов общей может быть только одна единица. Такие коды легко представить в виде монотонных булевых функций ранга *n*, веса 1 и мощности *m*, где *m* равно мощности кода.

Определение 1. Назовём максимальные коды с кодовым расстоянием 4 и кодовыми словами с весом Хэмминга 3 треугольными.

Для исследования таких кодов можно использовать теорию графов. В этом случае номера битов кодовых слов соответствуют вершинам графа, а сами кодовые слова соответствуют треугольникам в этом графе (рёбра в треугольнике соединяют вершины, которые соответствуют номерам единичных битов в кодовых словах). При этом, так как $\rho\left(\tilde{a},\tilde{b}\right)\geq 4$, то никакие два треугольника в построенном графе не имеют общих рёбер, т.е. они либо имеют одну общую вершину либо не пересекаются. В противном случае у двух кодовых слов номера дух единичных битов были бы одинаковы, а значит расстояние Хэмминга между этими кодовыми словами равнялось бы 2. Количество таких треугольников пересекающихся в вершине i обозначим через t_i.

Лемма 1. Для всех треугольных кодов существует верхняя граница числа кодовых слов, равная $\frac{n(n-1)}{6}$.

Доказательство. Учитывая, что такие треугольники не могут иметь общие рёбра, то сумма $\sum_{i=1}^{n} t_i$ не может быть больше количества всех рёбер. Поэтому, справедливо соотношение

$$\sum_{i=1}^{n} t_i \leq C_n^2 = \frac{n(n-1)}{2}.$$

Очевидно, что количество треугольников будет в 3 раза меньше количества рёбер, т.е. $\frac{n(n-1)}{6}$. Доказательство леммы окончено.

Определение 2. Назовём незадействованными рёбрами в построенном графе все рёбра, дополняющие данный граф до полного графа [7].

Лемма 2. Если *n* чётное, то количество незадействованных рёбер, инцидентных произвольной вершине графа, является нечётным. Если же *n* нечётное, то количество незадействованных рёбер, инцидентных произвольной вершине графа, является чётным.

Доказательство. Из каждой вершины построенного графа исходит чётное $2t_i$ количество рёбер. Всего вершине полного графа с *n* вершинами инцидентно *n* – 1 ребер. Следовательно, для нечётного n остаётся чётное количество незадействованных рёбер и наоборот, для чётного n остаётся нечётное количество незадействованных рёбер. Доказательство леммы окончено.

Относительно мощности рассматриваемых кодов можно доказать следующие утверждения.

Теорема 1. Пусть *n* – чётное, такое, что $n\not\equiv 4\left(\mathrm{mod}\,6\right)$(остаток от деления n на 6 не равен 4) тогда, когда мощность не превышает $\frac{n(n-2)}{6}$.

Доказательство. Имеем $n=2k$, где $k\not\equiv 2\left(\mathrm{mod}\,3\right)$. Учитывая лемму 2, из каждой вершины должно выходить, по крайней мере, одно незадействованное ребро. Наименьшее число таких рёбер можно провести, если они попарно не смежны, т.е. образуют паросочетание [7] в полном графе. В этом случае из каждой вершины исходит $n-2$ ребра, которые задействованы в треугольниках, т.е.

для всех вершин t_i одинаково. ($t_i = t$) и $\sum_{i=1}^{n} t_i = t\sum_{i=1}^{n} 1 = tn \le \frac{n(n-1)}{2}$. Следовательно, $t \le \frac{n-1}{2}$.

Тогда, $t = \frac{n}{2} - 1 = \frac{2k}{2} - 1 = k - 1$.

Учитывая, что $t \cdot n = 2k(k-1)$ и $k \not\equiv 2 \pmod 3$, то $t \cdot n$ будет нацело делиться на 3. Поэтому в этом случае максимальное число треугольников

$$\frac{t \cdot n}{3} = \frac{2k(k-1)}{3} = \frac{n(n/2 - 1)}{3} = \frac{n(n-2)}{6}.$$

Количество незадействованных рёбер по построению равно $\frac{n}{2}$. Теорема доказана.

Пример 1. Для $n = 6$. Максимальное количество треугольников $\frac{6(6-2)}{6} = 4$. Пусть кодовые слова равны: 000111, 011100, 101010 и 110001. Незадействованные рёбра(нумерация вершин начинается с нуля): (0,3), (1,4), (2,5). Они образуют паросочетание (рис. 1).

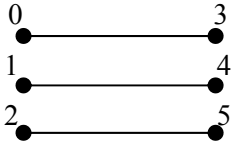

Рисунок 1 – Схема незадействованных ребер для $n = 6$

Матрица смежности [7] графа, соответствующего данному коду, показана в табл. 1. В клетке этой матрицы стоит единица на пересечении двух вершин, если в рассматриваемом графе эти две вершины смежные. Если же две вершины одинаковы или принадлежат незадействованному ребру, то на их пересечении стоит нуль (табл. 1).

Таблица 1 – Матрица смежности графа, соответствующего треугольному коду с $n = 6$

Вершины	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

Номера вершин, соответствующих кодовым словам (номера вершин построенных треугольников): (0,1,2), (2,3,4), (1,3,5), (0,4,5).

Этот код можно представить в виде монотонной булевой функции, где номер вершины треугольника на 1 меньше номера переменной в функции: $x_1x_2x_3 \vee x_3x_4x_5 \vee x_2x_4x_6 \vee x_1x_5x_6$

Пример 2. Для $n = 8$. Максимальное количество треугольников $\frac{8(8-2)}{6} = 8$.

Незадействованные рёбра (нумерация вершин начинается с нуля): (0,4), (1,5), (2,6), (3,7). Они образуют паросочетание (рис. 2).

Для данных незайдествованных ребер можно выбрать следующие кодовые слова: 01100001, 00001011, 10000101, 00010110, 11000010, 00101100, 01011000 и 10110000. По этим словам строятся следующие треугольники: (0,5,6), (0,1,3), (0,2,7), (1,2,4), (1,6,7), (2,3,5), (3,4,6), (4,5,7).

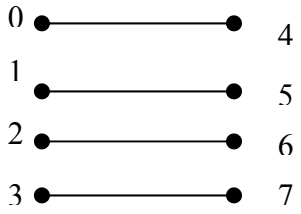

Рисунок 2 – Схема незадействованных ребер для $n=8$

Теорема 2. Пусть n – чётное, такое, что $n \equiv 4 \pmod 6$. Тогда мощность кода не превышает $\frac{n(n-2)-2}{6}$.

Доказательство. В этом случае $n=2k$, где $k \equiv 2 \pmod 3$. Если построить такое же паросочетание как в предыдущей теореме, тогда количество остальных рёбер $C_n^2 - \frac{n}{2} = \frac{n(n-2)}{2}$. Поскольку $n \equiv 4 \pmod 6$, а $n-2 \equiv 2 \pmod 6$, то это число $\frac{n(n-2)}{2}$ не делится на 3 и все остальные рёбра нельзя использовать для построения треугольников. Из леммы 2 следует, что из каждой вершины нашего графа должно исходить нечётное число незадействованных рёбер. Минимальное число незадействованных рёбер получается когда для $n-4$ вершин графа строится паросочетание, содержащие $\frac{n-4}{2}$ незадействованных рёбер, а незадействованные рёбра из остальных 3 вершин сходятся в четвёртой вершине и образуют трёхлучевую звезду. Всего имеется $\frac{n-4}{2}+3$ незадействованных ребра.

Из построения незадействованных рёбер следует, что в каждой вершине, кроме центра звезды, пересекается $t=\frac{n-2}{2}$ треугольников. В вершине, соответствующей центру звезды, пересекается на единицу меньше треугольников $\frac{n-4}{2}$.

Имеем

$$t \cdot (n-1) + t - 1 = t \cdot n - 1 \le C_n^2 = \frac{n(n-1)}{2}.$$

Тогда

$$t \le \frac{n-1}{2} + \frac{1}{n}.$$

Отсюда $t = k-1$, где $n=2k$.

Число треугольников в этом случае

$$\frac{t \cdot n - 1}{3} = \frac{2k(k-1)-1}{3} = \frac{n\left(n/2-1\right)-1}{3} = \frac{n(n-2)-2}{6}.$$

Теорема доказана.

Пример 3. Для $n=10$. Количество треугольников $\frac{10(10-2)-2}{6}=13$.

Незадействованные рёбра: (0,3) (1,4) (2,5) (6,9) (7,9) (8,9).

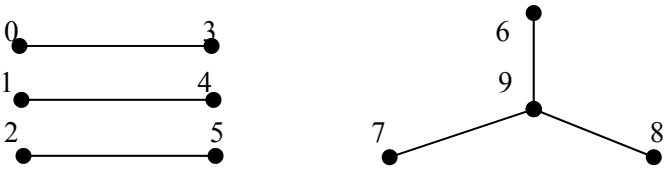

Рисунок 3 – Схема незадействованных ребер для $n=10$

Все ребра полного графа, кроме незайдествованных, принадлежат графу, построенному по треугольному коду. Этот граф имеет матрицу смежности, показанную в табл. 2.

В качестве кодовых слов треугольного кода можно выбрать следующие треугольники:

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

Таблица 2 – Матрица смежности графа, соответствующего треугольному коду с n=10

Вершины	0	1	2	3	4	5	6	7	8	9
0	0	1	1	0	1	1	1	1	1	1
1	1	0	1	1	0	1	1	1	1	1
2	1	1	0	1	1	0	1	1	1	1
3	0	1	1	0	1	1	1	1	1	1
4	1	0	1	1	0	1	1	1	1	1
5	1	1	0	1	1	0	1	1	1	1
6	1	1	1	1	1	1	0	1	1	0
7	1	1	1	1	1	1	1	0	1	0
8	1	1	1	1	1	1	1	1	0	0
9	1	1	1	1	1	1	0	0	0	0

Теорема 3. Пусть n – нечётное, такое, что $n \not\equiv 5 \pmod 6$. Пусть так же существует треугольный код с кодовыми словами длины $k = n-1$. Тогда существует код с кодовыми словами длины n и его мощность равна верхней границе для треугольных кодов $\frac{n(n-1)}{6}$.

Доказательство. Когда число вершин n нечётное такое, что $n \not\equiv 5 \pmod 6$, то $n-1$ чётное и $n-1 \not\equiv 4 \pmod 6$. По доказанному выше число треугольников для $n-1$ равно $\frac{(n-1)(n-3)}{6}$. Число незадействованных рёбер равно $\frac{n-1}{2}$ и они не пересекаются, образуя паросочетание. В этом случае для последней n-й вершины можно построить с $\frac{n-1}{2}$ незадействованными рёбрами $\frac{n-1}{2}$ новых треугольников.

Поэтому число треугольников для этого случая:

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

Легко видеть, что в этом случае нет незадействованных рёбер. Все рёбра задействованы. Теорема доказана.

Второй схемой или просто блок-схемой называется [8,9]: совокупность подмножеств (называемых блоками) множества S, состоящих из v точек, каждый блок содержит k точек, а всякое множество из двух точек содержится ровно в λ блоках. В случае λ = 1 блок-схема называется штейнеровой системой [8,9] порядка v.

Коды из теоремы 3 являются блок-схемами с параметрами $v = n$, $k = 3$, λ = 1. Таким образом, указанные коды являются штейнеровыми системами.

Пример 4. Для $n=7$. Количество кодовых слов $\frac{7(7-1)}{6}=7$. Номера вершин треугольников, соответствующих кодовым словам: (0,3,6), (0,4,5), (0,1,2), (1,3,5), (1,4,6), (2,5,6), (2,3,4).

Если вместо вершин треугольников рассмотреть точки на прямой, то в этом случае мы имеем $2^2+2+1=7$ точек и 7 прямых, которые содержат по три точки и это множество удовлетворяет аксиомам проективной плоскости [6, 10]:

1. Через две различные точки P и Q плоскости проходит прямая, причём только одна.
2. Любые две прямые имеют общую точку.
3. Существуют три точки, не лежащие на одной прямой.
4. Каждая прямая содержит не менее трёх точек.

Поэтому имеем проективную плоскость 2-го порядка или плоскость Фано.

Пример 5. Для $n=9$. Количество кодовых слов $\frac{9(9-1)}{6}=12$. Номера вершин треугольников, соответствующих кодовым словам: (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).

В этом случае имеем аффинную плоскость 3-го порядка. $3^2=9$ точек, $3^2+3=12$ прямых, которые удовлетворяют аксиомам [8, 9]:

1. Для любых двух различных точек существует только одна прямая, содержащая эти точки.
2. Пересечение двух различных прямых содержит ровно одну точку.
3. Существует множество из четырёх точек, никакие три из которых не принадлежат одной прямой.

Аффинная плоскость третьего порядка может быть получена из проективной плоскости третьего порядка, вычёркиванием одной прямой и лежащих на ней четырех точек.

Теорема 4. Пусть n – нечётное, такое, что $n\equiv 5(\bmod 6)$. Пусть также существует треугольный код с кодовыми словами длины $k=n-1$. Тогда существует код с кодовыми словами длины n и его мощность равна $\frac{n(n-1)-8}{6}$.

Доказательство. Для случая, когда n нечётное и $n\equiv 5(\bmod 6)$, для чётного $n-1$ по доказанному выше (см. теорему 2), имеем $\frac{(n-1)(n-3)-2}{6}$ треугольников и $\frac{n-5}{2}+3=\frac{n+1}{2}$ незадействованных рёбер. Тогда последнюю n-ю вершину можно построить с $\frac{n+1}{2}-2$ незадействованными рёбрами (используется один луч трёхлучевой звезды, так как в противном случае будет пересечения треугольников по ребру) $\frac{n-3}{2}$ новых треугольников.

Поэтому число треугольников для этого случая:

$$\frac{(n-1)(n-3)-2}{6}+\frac{n-3}{2}=\frac{n(n-1)-8}{6}.$$

Число незадействованных рёбер:

$$C_n^2-3\frac{n(n-1)-8}{6}=\frac{n(n-1)}{2}-\frac{n(n-1)-8}{2}=4.$$

Теорема доказана.

В случае кодов из теоремы 4 незадействованные рёбра с новой вершиной и двумя незадействованными лучами звезды образуют четырёхугольник, так как в этом случае по лемме 2 из вершины выходит чётное количество незадействованных рёбер.

Пример 6. Для $n=11$. Количество кодовых слов $\frac{11(11-1)-8}{6}=17$.

Незадействованные рёбра: (6,10) (6,9) (8,9) (8,10). Четырёхугольник из них:

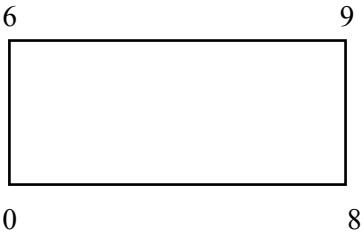

Рисунок 4 – Схема незадействованных ребер для $n=11$

Номера вершин треугольников, соответствующих кодовым словам: (0,6,8), (0,9,10), (0,4,5), (0,1,3), (0,2,7), (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).

Теорема 5. Пусть существует треугольный код со словами кодовой длины k (k нечётно и $k \not\equiv 5(\mathrm{mod}\,6)$) мощности $m=\dfrac{k(k-1)}{6}$. Тогда существует треугольный код со словами кодовой длины $n=2k$ мощности $4m=\dfrac{n(n-2)}{6}$.

Доказательство. Пусть имеется код со словами кодовой длины k. Поставим в соответствие каждому *i*-му биту из кодового слова этого кода следующую пару битов: $(i,i+k)$. Определим, что эти биты незадействованные парами в коде, существование которого мы доказываем. Возьмём из существующего кода произвольное кодовое слово длины k. Пусть единичные биты в этом кодовом слове имеют номера i,j,t. Сопоставим каждому из этих битов пары: $(i,i+k)$, $(j,j+k)$, $(t,t+k)$. Построим из этих пар четыре треугольника с вершинами: 1) (i,j,t), 2) $(i+k,j,t+k)$, 3)$(i+k,j+k,t)$, 4) $(i,j+k,t+k)$. Проделав такую операцию для любого кодового слова, мы получим $4m$ кодовых слов длины $n=2k$. При таком построении никакие два треугольника не имеют общих рёбер. Очевидно, что построенные четыре треугольника, из единичных битов i,j,t кодового слова не имеют общих рёбер. Допустим, что какой-то из этих четырех треугольников имеет общее ребро с треугольником, который получается из единичных битов i_1,j_1,t_1 кодового слова. Отсюда, учитывая, что в исходном кодовом слове мы добавляем к битам слова длину этого кодового слова, т.е. сдвигаем биты, соответствующие вершине треугольника, на расстояние равное длине кодового слова, следует, что треугольники из исходного кода с длиной кодового слова k также должны иметь общие рёбра. Действительно, пусть два треугольника имеют общее ребро $(i+s,\ j+s)$ в первом треугольнике и $(i_1+s,\ j_1+s)$ во втором, где s может принимать значения либо k, либо 0. Пусть $i<j$ и $i_1<j_1$. Тогда, так как треугольники пересекаются по этому ребру, то должны выполняться условия $i+s=i_1+s$, здесь s одновременно либо k, либо 0, и $j+s=j_1+s$, здесь s так же одновременно либо k, либо 0, отсюда следует, что $i=i_1$ и $j=j_1$. А это означает, что треугольники из исходного кода с длиной кодового слова k имеют общие рёбра, что противоречит определению кода. Теорема доказана.

Следствие 1. Зависимость мощности треугольного кода от длины кодового слова близка к квадратичной.

Следствие 2. Поочередно применение теорем 5 и 3 к треугольному коду с кодовыми словами нечетной длины *n* неравной 5 по модулю 6 приводит к бесконечной последовательности кодов с бесконечно увеличивающимся n, в которой чередуются коды с нечетным и четным n. В этой последовательности треугольные коды с нечетным n не имеют незадействованных ребер.

В [8] для штейнеровых систем с длиной блока 3 доказано, что такие системы существуют тогда и только тогда, когда их порядок равен 1 или 3 по модулю 6. Для треугольных кодов отсюда следует, что для длин кодовых слов *n*, равных 1 или 3 по модулю 6 существуют треугольные коды мощности $\dfrac{n(n-1)}{6}$.

Пример 7. Треугольный код с $n=3$ имеет мощность $m=1$. Применяя теорему 5, получим код с $n=5$ и $m=4$. Применяя теорему 3, получим код с $n=7$ и $m=7$. Повторные применения этих теорем приводит к последовательности кодов с длинами кодовых слов равных 3, 6, 7, 14, 15, 30, 31, 62, 63, 126, 127, 254, 255, 510, 511, 1022 мощности этих кодов по теоремам 3 и 5 равны 1, 4, 7, 28, 35, 140, 155, 620, 651, 2604, 2667, 10668, 10795, 43180, 43435, 173740 соответственно.

В табл. 3 приведена зависимость мощности треугольного кода m от длины кодового слова n при $6 \le n \le 20$.

Таблица 3 – Зависимость мощности треугольного кода m от длины кодового слова n

Длина код. слова, n	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Мощность кода, m	4	7	8	12	13	17	20	26	28	35	37	43	48	57	60

В теоремах 3, 4 и 5 показаны простые и эффективные способы построения треугольных кодов из известных треугольных кодов с меньшей длиной кодового слова. Однако для многих длин кодового слова построить треугольный код, используя эти способы невозможно. Поэтому был разработан универсальный метод построения треугольных кодов на основе монотонных булевых функций, не использующий треугольный код с меньшей длиной кодового слова. Метод, разработанный для построения таких кодов, реализован на ЭВМ в виде программы на языке Delphi. В случае полного перебора троек вершин количество комбинаций, которые нужно перебрать, оценивается числом $C^{m}_{C^{3}_{n}}$, где m – мощность кода. Например, для $n=12$ это число порядка 10^{28} (10 октиллионов). Перебор такого числа комбинаций даже для самых быстродействующих ЭВМ невозможен за разумное время. Рассмотрим представление этого кода в виде монотонной булевой функции. Здесь переменные соответствуют вершинам треугольников. Вынесем одну из переменных, например, x_1, за скобки. Тогда в скобках остаются пары вершин, никакие две из которых не имеют общей переменной. Такой подбор пар вершин для общей переменной значительно сокращает перебор. Основным этапом метода является выбор для заданной вершины подходящих пар. При этом всегда проверяется, не была ли задействована эта пара в уже найденных треугольниках. Как только для вершины найдено $n-2$ пар, то переходим к следующей вершине. При работе данного метода возможны тупиковые ситуации. В этом случае убираем одну из вершин, для которой найдены все пары и ставим на её место одну из свободных вершин. При замене вершины рёбра, связанные с освобождаемой вершиной тоже освобождаются. Это значительно повышает быстродействие. Так, например, для $n=50$ на ПЭВМ программа выполняется около 3-х минут (тактовая частота процессора 2 ГГц, кэш второго уровня 512 кБ). При этом находится код мощности равной 400, что совпадает с верхней границей в теореме 1.

Этот метод применялся для всех длин кодовых слов $n \le 80$. Во всех случаях мощность кода совпадала с мощностью полученных в доказанных теоремах.

Так как расстояние Хэмминга между любыми кодовыми словами не меньше 4, то такой треугольный код может исправлять один символ передаваемого кодового слова. Кодовые слова в таблице кодирования упорядочены по возрастанию.

Декодирование проводится с помощью таблицы (двумерного массива), где в заголовках строк и столбцов будут записаны номера единичных битов, а в самой таблице номера кодовых слов. По номерам двух битов кодового слова мы определяем переданное информационное сообщение. При этом номера столбцов соответствуют младшему биту, а номера строк старшему биту передаваемого сообщения.

Пример 8. Для треугольного кода с $n=12$ по каналу криптосистемы передаётся два сообщения 2 и 1. Эти сообщения кодируются двумя кодовыми словами (по табл. 4): 000000011001 и 000000000111, т.е. всего передаётся 24 бита. Пусть были приняты два кодовых слова 000000010001 и 000010000111. При приёме определяются номера битов кодовых слов для 1-го кодового слова это биты: 0, 4, для 2-го – 0, 1, 2, 7. Применим таблицу декодирования (табл. 5) для определения переданного сообщения соответствующего первому кодовому слову. Номер младшего единичного бита переданного слова равен 0, а номер старшего 4. На пересечении соответствующей строки и столбца стоит 2. Это значит, что передано сообщение 2. Ошибка передачи для 1-го кодового слова исправлена.

Рассмотрим, как происходит декодирование в случае, если вместо трёх единичных битов было принято 4 единичных бита, на примере второго кодового слова. Из единичных битов 2-го ко-

дового слова можно образовать шесть пар: (0;1), (0;2), (1;2), (0;7), (1;7), (2;7). Этим парам в таблице декодирования соответствуют переданные сообщения: 1, 1, 1, 6, 0, 17 (0 обозначает, что данной паре не соответствует никакое сообщение). Три из найденных в таблице сообщений одинаковы и равны 1. Это означает, что три первых пары битов образуют второе кодовое слово, т.е. было передано кодовое слово 000000000111. Ошибка передачи для 2-го кодового слова исправлена. Можно показать, что в случае приёма 4 битов вместо трёх достаточно найти в таблице для полученных пар два совпадающих сообщения, т.е. в приведенном примере вместо шести пар достаточно было проверить только пары (0;1) и (0;2). В худшем случае достаточно проверить пять пар, что требует 5 считываний из табл. 5.

Таблица 4 – Одномерный массив кодирования

Передаваемое сообщение	Кодовое слово												
	Десятичный	Двоичный вид											
1	7	0	0	0	0	0	0	0	0	0	1	1	1
2	25	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
4	74	0	0	0	0	0	1	0	0	1	0	1	0
5	84	0	0	0	0	0	1	0	1	0	1	0	0
6	161	0	0	0	0	1	0	1	0	0	0	0	1
7	304	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
9	546	0	0	1	0	0	0	1	0	0	0	1	0
10	656	0	0	1	0	1	0	0	1	0	0	0	0
11	769	0	0	1	1	0	0	0	0	0	0	0	1
12	1120	0	1	0	0	0	1	1	0	0	0	0	0
13	1160	0	1	0	0	1	0	0	0	1	0	0	0
14	1282	0	1	0	1	0	0	0	0	0	0	1	0
15	1540	0	1	1	0	0	0	0	0	0	1	0	0
16	2066	1	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
18	2312	1	0	0	1	0	0	0	0	1	0	0	0
19	2624	1	0	1	0	0	1	0	0	0	0	0	0
20	3073	1	1	0	0	0	0	0	0	0	0	0	1

Таблица 5 – Двумерный массив декодирования

Биты	**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

Мощность этого кода можно увеличить в два раза, если к кодовым словам данного треугольного кода добавить кодовые слова, в которых записаны вместо единиц нули и наоборот. Если к 20 кодовым словам добавить ещё 20 кодовых слов, в которых вместо единиц нули и наоборот, то для $n = 12$ получим 40 кодовых слов. Тогда с помощью этого кода можно кодировать не 20, а 40 сообщений.

Рассмотрим треугольный код с $n = 32$. Мощность этого кода по теореме 1 равна 160. Если мы удвоим мощность этого кода, как описано выше, то сможем кодировать 320 сообщений. Этого достаточно, чтобы кодировать все возможные двоичные байты.

Можно показать, что если во всех кодовых словах треугольного кода переставить биты с помощью одной и той же подстановки, то полученные кодовые слова также образуют треугольный код. Для некоторых кодов любая такая подстановка приводит к новому коду. Такой код существует, например, при $n = 20$. В этом случае с помощью подстановок можно образовать 20! = 2 432 902 008 176 640 000 кодов, что приблизительно равно $2{,}4 \cdot 10^{18}$. Применяя подстановку при посылке кодовых слов в канал криптосистемы и обратную подстановку при их приеме, легко изменять передаваемый код. При этом таблицы кодирования и декодирования не меняются.

В заключение отметим следующее. Основным результатом статьи является универсальный метод построения треугольных кодов на основе монотонных булевых функций. Так как в литературе треугольные коды не исследовались, то в статье введено два определения и доказан ряд свойств этих кодов. Для них применяется простое правило кодирования (одно считывание из одномерного массива), простой алгоритм декодирования (не более 5 считываний из двумерного массива) и простая смена кода (меняется только одна подстановка), причем выбор кода при его смене происходит из очень большого числа кодов. Дополнительным важным свойством треугольных кодов является возможность исправления одиночной ошибки в принятом кодовом слове. На основе треугольных кодов легко построить криптосистему с простым правилом кодирования, алгоритмом декодирования и возможностью смены кода одной подстановкой. Вследствие возможности быстрой смены кода, его можно часто менять во время передачи. При этом в качестве ключа может передаваться либо подстановка, либо закон изменения подстановок. Из-за недостатка места не рассмотрен метод перебора кодов, изоморфных данному коду. Его предполагается рассмотреть в отдельной статье.

Литература

1. *Мао В.* Современная криптография: теория и практика / Мао Венбо. – М.: Вильямс, 2005. – 768 с.
2. *Мак-Вильямс Ф.Дж.* Теория кодов, исправляющих ошибки / Ф.Дж.. Мак-Вильямс, Н.Дж.А. Слоэн – М.: Связь, 1979. – 744 с.
3. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Мир, 1986. – 576 с.
4. *Банкет В.Л.* Помехоустойчивое кодирование в телекоммуникационных системах: учеб. пособ. / Банкет В.Л., Иващенко П.В., Ищенко Н.А. − Одесса, 2011. – 104 с.
5. *Ткаченко В.Г.* Перечисление типов монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 2. – С. 54 – 69.
6. *Ткаченко В.Г.* Построение корректирующего кода для криптосистем на основе типов монотонных булевых функций / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – 2010. – № 1. – С. 85 – 92.
7. Лекции по теории графов/ [Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И.].– М.: Наука, 1990. – 384 с.
8. *Холл М.* Комбинаторика / Холл М. – М.*:* Мир, 1970. – 424 с.
9. *Камерон П.* Теория графов, теория кодирования и блок-схемы / П. Камерон, Дж. ван Линт – М.: Наука, 1980. – 144 с.
10. *Картеси Ф.* Введение в конечные геометрии / Картеси Ф. – М.*:* Наука, 1980. – 320 с.