УДК 519.719.1, 681.322

В. Г. Ткаченко*, О. В. Синявский**
*Одесская национальная академия связи им. А.С.Попова, ул. Кузнечная 1, 65029, Одесса
**Военная академия, ул. Фонтанская дорога, 10, 65009, Одесса

ПОСТРОЕНИЕ КРИПТОСИСТЕМЫ НА ОСНОВЕ МНОГОУГОЛЬНЫХ КОДОВ

В статье определены блоковые нелинейные многоугольные коды. Рассмотрены способы построения некоторых многоугольных кодов и предложен эффективный универсальный рекурсивного метода построения кодов большой длины на основе штейнеровых систем для криптосистем с коррекцией ошибок. Разработана криптосистема с корректирующим шифром на основе такого кода. Достоинствами этой криптосистемы является быстрота шифрации и дешифрации, а также возможность быстрой смены кода без изменения таблиц шифрации и дешифрации.
Ключевые слова: *Корректирующие коды – Нелинейные многоугольные коды – Криптосистема – Штейнеровые системы – Аффинная плоскость – Проективная плоскость.*

В. Г. Ткаченко*, О. В. Сінявський**
* Одеська національна академія зв'язку ім. О.С.Попова, вул. Ковальська 1, 65029, Одеса
**Військова академія, вул. Фонтанська дорога, 10, 65009, Одеса

ПОБУДОВА КРИПТОСИСТЕМИ НА ОСНОВІ МНОГОКУТНИХ КОДІВ

У статті визначені блокові нелінійні многокутні коди. Розглянуто способи побудови деяких многокутних кодів та запропоновано ефективний універсальний рекурсивний метод побудови кодів великої довжини на основі штейнерових систем для криптосистем з корекцією помилок. Розроблена криптосистема з коригувальним шифром на основі такого коду. Перевагами цієї криптосистеми є швидкість шифрування та дешифрування, а також можливість швидкої зміни коду без зміни таблиць шифрування та дешифрування .
Ключові слова: *Коригувальні коди – Нелінійні многокутні коди – Криптосистема – Штейнерови системи – Афінна площина – Проективна площина.*

I. ВВЕДЕНИЕ

В процессе передачи информации в криптосистемах по телекоммуникационным сетям связи возникает проблема коррекции ошибок. Контроль целостности данных и коррекции ошибок — важные задачи на многих уровнях работы с информацией. Одним из средств решения этих задач является применение помехоустойчивых кодов, лежащих в основе криптосистем.

К настоящему времени разработано много различных помехоустойчивых кодов для криптосистем, отличающихся друг от друга расстоянием, избыточностью, структурой, функциональным назначением, корреляционными свойствами, алгоритмами кодирования и декодирования, формой частотного спектра ([1] … [4]). На основе монотонных булевых функций построен ряд криптосистем [5 – 8], с коррекцией ошибок. В частности, в системе на основе треугольных кодов для построения кодов большой длины использовался рекурсивный метод [6].

Однако рекурсивный метод, используемый в [6] не позволяет строить коды, если число единиц в код слове больше 3.

Целью настоящей работы является разработка рекурсивного метода для построения кодов большой длины для криптосистем с коррекцией ошибок.

II. ПОСТАНОВКА ЗАДАЧИ

В данной статье в качестве кодовых слов будем рассматривать векторы длины n $\tilde{p} = (p_1, ..., p_i, ..., p_n)$, компоненты которых принимают значения из множества $\{0,1\}$, и количество единичных компонент в векторе равно k. Такие кодовые слова имеют вес Хэмминга(количество единиц в кодовом слове) равный k. Расстоянием Хэмминга (кодовым расстоянием) между двумя кодовыми словами $\tilde{p}$ и $\tilde{s}$ называется число $\rho(\tilde{p},\tilde{s})$ равное количеству компонент, в которых они различаются [1]. Длиной кода назовём длину кодового слова. Всего таких кодовых слов с весом k могут быть C_n^k. Кодовые расстояния между различными словами в этом случае могут быть 2, 4, 6, …, 2k. Для корректирующих кодов применимы только кодовые слова с расстоянием 4, 6, …, 2k. Количество кодовых слов называется мощностью кода. Такие коды с кодовым расстоянием 2k малоинтересны, поскольку их мощность мала и всегда равна $\left[\frac{n}{k}\right]$. В любой такой паре кодовых слов нет совпадающих единичных бит. В дальнейшем будем рассматривать максимальные коды с $\rho(\tilde{p},\tilde{s}) \geq 2k-2$, поскольку они исправляют максимальное количество ошибок. 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. [6-8]

Для исследования таких кодов можно использовать блок-схемы.

В [9-11] приведены следующие определения блок-схемы, BIB блок-схемы, аффинной и проективной плоскостей.

Определение. Уравновешенной неполной блок-схемой (или просто блок-схемой) $B(v,b,r,k,\lambda)$ называется такое размещение *v* различных элементов по *b* блокам, что каждый блок содержит точно *k* различных элементов, каждый элемент появляется точно в *r* различных блоках и каждая пара различных элементов b_i, b_j появляется точно в λ блоках.

ПРИМЕР 1. Для $v=7, b=7, r=3, k=3, \lambda=1$ имеем такие блоки:

*b*0: (0, 1, 3)
*b*1: (1, 2, 4)
*b*2: (2, 3, 5)
*b*3: (3, 4, 6)
*b*4: (4, 5, 0)
*b*5: (5, 6, 1)
*b*6: (6, 0, 2)

Определение. Уравновешенной относительно пар (элементов) блок-схемой $BIB(v,(b_1,...,b_m),(k_1,...,k_m),\lambda)$ называется такое размещение *v* элементов по $b=\sum_1^m b_i$ блокам, что: 1) b_i блоков содержит по $k_i < v$ различных элементов при некотором $i = 1, ..., m$; 2) каждая пара элементов появляется вместе точно в λ блоках.

Любая блок-схема или *BIB* блок-схема является кодом. В этом случае номера единичных битов кодовых слов соответствуют элементам блока, а сами кодовые слова соответствуют блокам в этой блок-схеме. При этом, т.к. $\rho(\tilde{a},\tilde{b}) \geq 2k-2$, то никакие 2 блока в построенном графе не имеют общих пар элементов. Очевидно, что число λ соответствует расстоянию Хэмминга, а именно: $\rho(\tilde{a},\tilde{b}) = 2(k-\lambda)$.

Определение. Корректирующая способность – характеристика кода, которая равна максимальному количеству исправляемых ошибок в кодовых словах.

Определяется как $\left[\frac{d-1}{2}\right]$, где d – минимальное расстояние между кодовыми словами.

Так как число кодовых слов, у которых $\rho(\tilde{a},\tilde{b}) = 2k$ мало, то наибольшая корректирующая способность кода достигается, когда $\lambda = 1$ и равна

$$\left[\frac{2(k-1)-1}{2}\right] = \left[\frac{2k-3}{2}\right]$$

В дальнейшем рассматриваются только блок-схемы с $\lambda = 1$, т.е. штейнеровы системы.

В предложенном методе построение корректирующих кодов будут использованы проективная и аффинная плоскости.

Определение. Система $PG(2,n)$, имеющая конечное количество точек называется проективной плоскостью порядка n, если удовлетворяет следующим аксиомам:

1. Через две различные точки *P* и *Q* плоскости проходит прямая, причем, 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

В общем случае проективная плоскость порядка n имеет n^2+n+1 точек и столько же прямых. Каждая линия содержит $n+1$ точек, и каждая точка принадлежит $n+1$ прямой.

Определение. Система $EG(2,n)$, имеющая конечное количество точек называется аффинной плоскостью порядка n, если удовлетворяет следующим аксиомам:

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.

В общем случае проективная плоскость порядка n имеет n^2 точек и n^2+n прямых. Каждая линия содержит n точек, и каждая точка принадлежит $n+1$ прямой.

Аффинная и проективная плоскости являются блок-схемами, в которых каждый блок состоит из номеров точек находящихся на некоторой прямой.

Дадим определение k-угольного кода.

Определение 1. k-угольным кодом называется штейнерова система, в каждом блоке которой содержится k элементов.

k-угольные коды являются блоковыми и нелинейными, поскольку разность любых кодовых слов не являются кодом.

Перед тем как описать рекурсивный метод построения кодов на основе блок-схем введём следующие определения.

Определение 2. Проективным расширением штейнеровой системы *A*0(*v*, *b*, *r*, *k*) называется штейнерова система *C*0, полученная объединением блоков *b* проективных плоскостей *B*0(*k*(*k* – 1) + 1, *k*(*k* – 1) + 1, *k*, *k*) = *PG*(2, *k* – 1), построенных для каждого блока штейнеровой системы *A*0.

Определение 3. Аффинным расширением штейнеровой системы *A*0(*v*, *b*, *r*, *k*) называется штейнерова система *C*0, полученная объединением блоков *b* аффинных плоскостей *B*0((*k* – 1)(*k* – 1), *k*(*k* – 1), *k*, *k* – 1) = *EG*(2, *k* – 1), построенных для каждого блока штейнеровой системы *A*0.

Определение 4. Проективно-аффинным расширением *BIB* штейнеровой системы *A*0(*v*, (*b*1, *b*2), (*k*,*k*+1)) называется штейнерова система *C*0, полученная объединением блоков *b*1 проективных плоскостей *B*0(*k*(*k* – 1) + 1, *k*(*k* – 1) + 1, *k*, *k*) = *PG*(2, *k* – 1), построенных для каждого блока из *k* элементов, и *b*2 аффинных плоскостей *B*0(*k*·*k*, *k*(*k* + 1), *k* + 1, *k*)

= $EG(2, k)$, построенных для каждого блока из $k + 1$ элемента *BIB* штейнеровой системы $A0$.

III. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Опишем рекурсивный метод построения блок-схем на примере построения кода длиной 64 из кода длиной 21.

ПРИМЕР 2. В качестве блок-схемы $A0$ длины 21 возьмем проективную плоскость 4-го порядка $PG(2,4)$ $v = 21$, $b = 21$, $r = 5$, $k = 5$, $\lambda = 1$

1)(1,2,7,9,19)
2)(2,3,8,10,20)
3)(0,3,4,9,11)
4)(0,1,6,8,18)
5)(1,4,5,10,12)
6)(2,5,6,11,13)
7)(3,6,7,12,14)
8)(4,7,8,13,15)
9)(5,8,9,14,16)
10)(6,9,10,15,17)
11)(7,10,11,16,18)
12)(8,11,12,17,19)
13)(9,12,13,18,20)
14)(0,10,13,14,19)
15)(1,11,14,15,20)
16)(0,2,12,15,16)
17)(1,3,13,16,17)
18)(2,4,14,17,18)
19)(3,5,15,18,19)
20)(4,6,16,19,20)
21)(0,5,7,17,20)

Пусть множество E, состоит из точки 0 и пар (x, y), где $0 \le x \le 20$, $0 \le y \le 2$. Построим блоки, содержащие 0, следующим образом: $\left(0,(x,0),(x,1),(x,2)\right)$. Будем такие блоки называть выделенными блоками. В парах (x,y) в качестве элементов x возьмём элементы блока 1 блок-схемы $A0$: (1,2,7,9). В результате получим 16-элементное множество $E1$. Перенумеруем все пары (x,y) следующим образом $(0,0)=1$, $(1,0)=2$, …, $(0,1)=22$, ... , $(20,2)=63$. В результате получим такое множество $E1$={0,1,2,7,9,19,22,23,28,30,40,43,44,49,51,61}. На этом множестве построим блок-схему $B1$ – аффинную плоскость 4-го порядка $EG(2,4)$ $v = 16$, $b = 20$, $r = 5$, $k = 4$, $\lambda = 1$.

1.1)(0,1,22,43)
1.2)(0,2,23,44)
1.3)(0,7,28,49)
1.4)(0,9,30,51)
1.5)(0,19,40,61)
1.6)(1,2,9,28)
1.7)(2,7,40,43)
1.8)(7,9,23,61)
1.9)(1,23,30,40)
1.10)(2,22,51,61)
1.11)(7,22,30,44)
1.12)(23,43,49,51)
1.13)(9,19,43,44)
1.14)(9,22,40,49)
1.15)(28,30,43,61)
1.16)(28,40,44,51)
1.17)(1,44,49,61)
1.18)(2,19,30,49)
1.19)(1,7,19,51)
1.20)(19,22,23,28)

Выделенными блоками в блок-схеме B1 являются блоки, содержащие 0, т.е. с номерами 1.1-1.5

Аналогично по блоку 2 блок-схемы $A0$ $PG(2,4)$ строим множество $E2$={0,2,3,8,10,20,23, 24,29,31,41,44,45,50,52,62}. На этом множестве построим блок-схему $B2$ – аффинную плоскость 4-го порядка $EG(2,4)$ $v = 16$, $b = 20$, $r = 5$, $k = 4$, $\lambda = 1$ с помощью такой замены элементов блок-схемы $B1$(согласно лемме 3):

1--->2--->3, 7--->8, 9--->10, 19--->20, 22--->23--->24, 28--->29, 30--->31, 40--->41, 43--->44--->45, 49--->50, 51--->52, 61--->62

2.1)(0,2,23,44)
2.2)(0,3,24,45)
2.3)(0,8,29,50)
2.4)(0,10,31,52)
2.5)(0,20,41,62)
2.6)(2,3,10,29)
2.7)(2,8,20,52)
2.8)(2,24,31,41)
2.9)(2,45,50,62)
2.10)(3,8,41,44)
2.11)(3,20,31,50)
2.12)(3,23,52,62)
2.13)(8,10,24,62)
2.14)(8,23,31,45)
2.15)(10,20,44,45)
2.16)(10,23,41,50)
2.17)(20,23,24,29)
2.18)(24,44,50,52)
2.19)(29,31,44,62)
2.20)(29,41,45,52)

Выделенными блоками в блок-схеме B2 являются блоки 2.1-2.5

Использовав таким образом все 21 блок блок-схемы $A0$, мы получим 21 аффинную плоскость, в которые будут входить 420 блоков. При этом невыделенные блоки не будут иметь повторяющихся пар таких блоков будет $15 \cdot 21 = 315$. Теперь, мы добавим блоки, по которым происходят пересечения блок-схем Bi и Bj, $1 \le i, j \le 21; i \ne j$. Такие пересечения будут происходить только по выделенным блокам (лемма 1). таких блоков во всех Bj будет $21 \cdot 5 = 105$. Но по лемме таких блоков будет 21. Поэтому будем иметь в сумме 315 + 21 = 336 непересекающихся блоков. Таким образом, мы получили все блоки штейнеровой системы $C0$ с параметрами v = 64, b = 336, r = 21, k = 4.

Для распространения построения из примера 1 на произвольные штейнеровы системы предварительно докажем 3 леммы.

ЛЕММА 1. Любой невыделенный блок может входить только в одну из штейнеровых систем Bi.

Доказательство. Так как в качестве $A0$ рассматривается штейнерова система, то любые 2 блока a_i и a_j из $A0$ либо не пересекаются, либо имеют один общий элемент. В первом случае множества Ei и Ej имеют один общий элемент, равный 0, а значит штейнеровы системы Bi и Bj, построенные из элементов этих множеств, не имеют общих блоков. Во

втором случае блоки a_i и a_j имеют общий элемент x, а множества Ei и Ej имеют в качестве общих элементов 0 и пары (x, y), где x постоянно, а y может принимать все допустимые значения. Всего общих элементов в Ei и Ej столько, сколько их содержится в одном блоке штейнеровых систем Bi и Bj. Все эти общие элементы входят в один выделенный блок, общий для штейнеровых систем Bi и Bj. Это доказывает, что Bi и Bj не имеют общих невыделенных блоков.

ЛЕММА 2. Любые 2 несовпадающих блока штейнеровых систем Bi и Bj не содержат общую пару элементов.

Доказательство. По построению выделенные блоки не имеют общей пары и никакая пара из выделенного блока не может входить в невыделенный блок. Допустим 2 невыделенных блока из Bi и Bj содержат общую пару элементов. Тогда эта пара является общей для множеств Ei и Ej, а значит согласно лемме 1 входит в выделенный блок, общий для Bi и Bj. Тогда Bi содержит выделенный и невыделенный блоки с общей парой элементов. Это противоречит тому, что Bi является штейнеровой системой. Лемма доказана.

ЛЕММА 3. Любая штейнерова система Bi получается перенумерацией элементов штейнеровой системы $B1$.

Доказательство. Штейнеровы системы $B1$ и Bi строятся из блоков a_1 и a_i штейнеровой системы $A0$. Однозначно отобразим элементы блока a_1 на элементы блока a_i. При этом общий элемент 2 блоков (если он есть) отображается на себя. Элементам блоков a_1 и a_i соотвествуют компоненты x в парах (x, y), принадлежащих множествам $E1$ и Ei. При таком отображеннии получается однозначная перенумерация элементов множества $E1$ в элементы множества Ei. При этом из штейнеровой системы $B1$ получается штейнерова система Bi.

В доказательстве лемм 1-3 не используется то, что в примере 1 в качестве Bi и Bj берутся аффинные плоскости. Поэтому леммы 1-3 справедливы, когда Bi и Bj является штейнеровыми системами

Распространим построение из примера 2 на случай произвольных v и k.

Теорема 1. Если существует штейнерова система $A0(v, b, r, k)$ и существует аффинная плоскость k–1-го порядка $B0((k-1)^2, k(k-1), k, k-1) = EG(2,k-1)$, то существует аффинное расширение $C0(v(k-2)+1, b\cdot k(k-2)+v, v, k-1)$ штейнеровой системы $A0$. Аффинные плоскости Bi существуют для $k-1$ вида p^i, где p – простое число.

Доказательство. Согласно лемме 1 в b аффинных плоскостях Bi присутствуют $b\cdot k(k-1) - b\cdot k$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в аффинном расширении $C0$ штейнеровой системы $A0$ содержится $b\cdot k(k-2)+v$ блоков. Во все эти блоки по построению входят $v(k-2)+1$ элементов, так как x в парах (x, y) меняется в общем случае от 0 до $v-1$, а y от 0 до $k-3$. Каждая пара (x, y) входит в $r\cdot(k-1)$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r\cdot(k-1)+1=v$, то каждый элемент аффинного расширения $C0$ входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b\cdot k(k-2)+v$ блоках содержится $b\cdot k(k-2)\cdot(k-1)\cdot(k-2)/2 + v\cdot(k-1)\cdot(k-2)/2$ пар. Поскольку для блок-схем $b\cdot k = v\cdot r$, то количество пар равно $v\cdot(v-1)\cdot(k-2)^2/2 + v\cdot(k-1)\cdot(k-2)/2 = v^2\cdot(k-2)^2/2 + v\cdot(k-2)/2$, т.е. количеству пар, которые образуют $v(k-2)+1$ элементов. Это доказывает, что $C0$ штейнерова система.

В случае когда $v=40$, то эту теорему применить нельзя. Из блок-схемы с $v=13$ построить блок-схему $v=40$ можно с помощью проективной плоскости.

Теорема 2. Если существует штейнерова система $A0(v, b, r, k)$ и существует проективная плоскость k–1-го порядка $B0(k(k-1)+1, k(k-1)+1, k, k) = PG(2,k-1)$, то существует проективное расширение $C0(v(k-1)+1, b(k-1)\cdot(k-1)+v, v, k)$ штейнеровой системы $A0$. Проективная плоскость $B0$ существует для $k-1$ вида p^i, где p – простое число. Штейнерова система $B0$ симметрична.

Доказательство. Согласно лемме 1 в b проективных плоскостях Bi присутствуют $b\cdot(k(k-1)+1) - b\cdot k$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в проективном расширении $C0$ блок-схемы $A0$ содержится $b(k-1)^2 + v$ блоков. Во все эти блоки по построению входят $v(k-1)+1$ элементов, так как x в парах (x, y) меняется в общем случае от 0 до v-1, а y от 0 до $k-3$. Каждая пара (x, y) входит в $r\cdot(k-1)$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r\cdot(k-1)+1=v$, то каждый элемент проективного расширения $C0$ входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b(k-1)^2 + v$ блоках содержится $b(k-1)^2\cdot k\cdot(k-1)/2 + v\cdot k\cdot(k-1)/2$ пар. Поскольку для блок-схем $b\cdot k = v\cdot r$, то количество пар равно $v\cdot(v-1)\cdot(k-1)^2/2 + v\cdot k\cdot(k-1)/2 = v\cdot(k-1)(v\cdot(k-1)+1)/2$, т.е. количеству пар, которые образуют $v(k-1)+1$ элементов. Это доказывает, что $C0$ штейнерова система.

ПРИМЕР 3. Из блок-схемы $A0(13, 13, 4, 4)$ и такой же блок-схемы $B0(13, 13, 4, 4)$ получим блок-схему $C0(40, 130, 13, 4)$. Пусть блок-схемы $A0$ и $B0$ такие:

1)	(1,	2,	3,	4)
2)	(1,	5,	6,	7)
3)	(1,	8,	9,	10)
4)	(1,	11,	12,	13)
5)	(2,	5,	8,	11)
6)	(2,	6,	9,	12)
7)	(2,	7,	10,	13)
8)	(3,	6,	10,	11)
9)	(3,	5,	9,	13)
10)	(3,	7,	8,	12)
11)	(4,	5,	1,0,	12)
12)	(4,	6,	8,	13)
13)	(4,	7,	9,	11)

Из блока 1 получим так же как в примере 2 блок-схему $B1(13, 13, 4, 4)$. Из неё перенумерацией элементов получим блок-схемы $B2 - B13$. В результате получим 117 невыделенных и 13 выделенных блоков блок-схемы $C0$.

Повторно применяя теорему 2 к $C0(40,130,13,4) = A1$ получим бесконечную последовательность штейнеровых систем:

$$A0(13,13,4,4) \Rightarrow A1(40,130,13,4) \Rightarrow ...$$

$$A3(364,11011,121,4)...A6(9841,8069620,3280,4) \Rightarrow ..$$

В случае, когда $v = 52$ теорему 1 и 2 применить нельзя. Зато можно построить штейнерову систему с $v = 52$, используя штейнерову систему $A0$

Теорема 3. Если существует *BIB* штейнерова система $A0(v, (b1, b2), (k,k + 1))$, существует проективная плоскость k–1-го порядка $B0(k(k – 1) + 1, k(k – 1) + 1, k, k) = PG(2,k – 1)$ и существует аффинная плоскость k-го порядка $D0(k·k, k(k + 1), k + 1, k) = EG(2,k)$, то существует проективно-аффинное расширение $C0(v(k – 1) + 1, b1(k – 1)(k – 1)+b2(k·k – 1) + v, v, k)$ *BIB* штейнеровой системы $A0$. Обе плоскости существуют для $k – 1$ вида $p_1^{i_1} \cdot i1$ и k вида $p_2^{i_2}$, где p_1 и p_2 – простые числа.

Доказательство. Согласно лемме 1 в $b1$ проективных и $b2$ аффинных плоскостях Bi присутствуют $b1·(k(k – 1) + 1) – b1·k + b2·k(k + 1) – b2·(k + 1)$ невыделенных блоков. Добавляя к ним v выделенных блоков получим, что в проективно-аффинном расширении $C0$ блок-схемы $A0$ содержится $b1(k – 1)^2 + b2(k^2 – 1) + v$ блоков. Во все эти блоки по построению входят $v(k – 1) + 1$ элементов, так как x в парах (x, y) меняется в общем случае от 0 до v-1, а y от 0 до $k – 2$. Каждая пара (x, y) входит в $r(k-1)+k$ невыделенных блоков и в один выделенный блок. 0 входит в v выделенных блоков. Так как в любой штейнеровой системе выполняется $r·(k – 1) + 1 = v$, то каждый элемент проективного расширения $C0$ входит в v блоков, а пара элементов $((x_1, y_1), (x_2, y_2))$ согласно лемме 2 входит только в один блок. Во всех $b1(k – 1)^2 + b2(k^2 – 1) + v$ блоках содержится $b1(k – 1)^2·k·(k – 1)/2 + b2(k^2 – 1)·k·(k – 1)/2 + v·k·(k – 1)/2$ пар. Поскольку для блок-схем $(b1 + b2)·k = v· r$, то количество пар равно $v·(v – 1)·(k – 1)^2/2 + v·k·(k – 1)/2 = v·(k – 1)(v·(k – 1)+1)/2$, т.е. количеству пар, которые образуют $v(k – 1) + 1$ элементов. Это доказывает, что $C0$ штейнерова система.

ПРИМЕР 4. Пусть заданы *BIB* блок-схема $A0(v=17, (b1=16, b2=4), (k=4, k+1=5))$:

$a1)$ (0, 1, 2, 3, 4)
$a2)$ (0, 5, 6, 7, 8)
$a3)$ (0, 9, 10, 11, 12)
$a4)$ (0, 13, 14, 15, 16)
$a5)$ (1, 5, 9, 13)
$a6)$ (1, 6, 10, 14)
$a7)$ (1, 7, 11, 15)
$a8)$ (1, 8, 12, 16)
$a9)$ (2, 5, 10, 15)
$a10)$ (2, 6, 9, 16)
$a11)$ (2, 7, 12, 13)
$a12)$ (2, 8, 11, 14)
$a13)$ (3, 5, 11, 16)
$a14)$ (3, 6, 12, 15)
$a15)$ (3, 7, 9, 14)
$a16)$ (3, 8, 10, 13)
$a17)$ (4, 5, 12, 14)
$a18)$ (4, 6, 11, 13)
$a19)$ (4, 7, 10, 16)
$a20)$ (4, 8, 9, 15),

проективная плоскость 3-го порядка $B0(13, 13, 4, 4)$ и аффинная плоскость 4-го порядка $D0(16, 20, 5, 4)$. Из $A0$, $B0$ и $D0$ можно построить проективно-аффинное расширение $C0(52, 221, 17, 4)$. А именно, из блоков $a1 – a4$ блок-схемы $A0$ получим 4 аффинных плоскости $D1 – D4(13, 13, 4, 4)$(как в примере 2), которые дадут 144 невыделенных блока, а из остальных блоков схемы $A0$ получим 16 проективных плоскостей $B5 – B20(16, 20, 5, 4)$(как в примере 3), которые дадут 60 невыделенных и 17 выделенных блоков(по построению) проективно-аффинного расширения $C0(52, 221, 17, 4)$.

Так как расстояние Хэмминга между любыми кодовыми словами не меньше $2(k-1)$, то такой четырёхугольный код может исправлять $\left[\frac{2k-3}{2}\right]$ символов 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 5. Обнаружение одной ошибки. Рассмотрим код с $k = 4$ и длиной n, по каналу криптосистемы передаётся два сообщения 2 и 1. Эти сообщения кодируются двумя кодовыми словами (по таблице 1): 0000…01110001 и 0000…00001111, т.е. всего передаётся $2n$ бита. Пусть были приняты два кодовых слова 0000…0110001 и 000…10001111. При приёме определяются номера битов кодовых слов для 1-го кодового слова это биты: 0, 4, 5, для 2-го – 0, 1, 2, 3, 7. Применим таблицу декодирования (таблица 2) для определения преданного сообщения соответствующего первому кодовому слову. Номер младшего единичного бита переданного слова равен 0, а номер старшего 5. 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 четырёх единичных битов было принято 5 единичных бита, на примере второго кодового слова. Из единичных битов 2-го кодового слова можно образовать 10 пар: (0;1), (0;2), (0;3), (1;2), (1;3), (2;3), (0;7), (1;7), (2;7), (3;7). Этим парам в таблице декодирования соответствуют переданные сообщения: 1, 1, 1, 1, 1, 1, 4, 6, 9, 10. Шесть из найденных в таблице сообщениях одинаковы и равны 1. Это означает, что 6 первых пары битов образуют второе кодовое слово, т.е. было передано кодовое слово 0000…00001111. Ошибка передачи для 2-го кодового слова исправлена. Можно показать, что в случае приёма 5 битов вместо 4 достаточно найти в таблицы для полученных пар два совпадающих сообщения, т.е. в приведенном примере

вместо 6 пар достаточно было проверить только пары (0;1) и (0;2). В худшем случае достаточно проверить 6 пар, что требует 6 считываний из таблицы 1.

Несложно подсчитать, сколько в среднем нужно проверить пар в этом случае. Обозначим через x случайную величину – количество проверяемых пар, p – вероятности значений x. Значения p_i найдём по формуле $p_i = \frac{C_6^1 \cdot C_4^{i-2}}{C_{10}^{i-1}} \cdot \frac{5}{10-i+1}$. Имеем закон распределения этой случайной величины:

x_i	2	3	4	5	6
p_i	0,333333	0,333333	0,214286	0,095238	0,02381

Математическое ожидание mx = 3,14. Следовательно, в этом случае в среднем нужно проверить 3 пары битов.

Таблица 1

Передаваемое сообщение	Кодовое слово												
	Двоичный вид												
1	0	0	0	0	…	0	0	0	0	1	1	1	1
2	0	0	0	0	…	0	1	1	1	0	0	0	1
3	1	0	0	1	…	0	0	0	0	0	0	0	1
4	0	1	1	0	…	1	0	0	0	0	0	0	1
5	0	0	1	1	…	0	0	0	1	0	0	1	0
6	0	0	0	0	…	1	0	1	0	0	0	1	0
7	1	1	0	0	…	0	1	0	0	0	0	1	0
8	0	1	0	1	…	0	0	1	0	1	0	0	0
9	0	0	0	1	…	1	1	0	0	0	1	0	0
10	1	0	0	0	…	1	0	0	1	1	0	0	0
11	0	0	1	0	…	0	1	0	0	1	0	0	0
12	0	1	0	0	…	0	0	0	1	0	1	0	0
13	1	0	1	0	…	0	0	1	0	0	1	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…	…
n	0	0	0	0	…	0	0	0	0	0	0	0	0

Таблица 2

Биты	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**…**	***n***
0	0	0	0	0	0	0	0	0	…	0
1	1	0	0	0	0	0	0	0	…	0
2	1	1	0	0	0	0	0	0	…	0
3	1	1	1	0	0	0	0	0	…	0
4	2	5	12	10	0	0	0	0	…	0
5	2	6	13	8	2	0	0	0	…	0
6	2	7	9	11	2	2	0	0	…	0
7	4	6	9	10	10	6	9	0	…	0
8	3	6	12	11	12	6	11	6	…	0
9	3	5	9	8	5	8	9	9	…	0
10	4	5	13	11	5	13	11	4	…	0
11	4	7	12	8	12	8	7	4	…	0
12	3	7	13	10	10	13	7	10	…	0
…	…	…	…	…	…	…	…	…	…	0
n	0	0	0	0	0	0	0	0	…	0

ПРИМЕР 6. Обнаружение двух ошибок. В рассматриваемом примере возможны случаи когда:

x_i	2	3	4	5	6
p_i	0,142857	0,197802	0,197802	0,167832	0,125874
x_i	7	8	9	10	11
p_i	0,083916	0,048951	0,023976	0,008991	0,001998

1. Приняты две единицы, остальные нули.
2. Приняты четыре единицы, одна из которых находится не на своём месте.
3. Приняты шесть единиц.

В первом случае сразу по двум единицам определяем передаваемое кодовое слово.

Во втором случае имеем 3 верных (соответствуют одному передаваемому сообщению) и 3 неверных пар (соответствуют разным передаваемым сообщениям). Тогда достаточно найти две пары одного передаваемому сообщению. Для нахождения двух пар из одного передаваемого сообщения надо проверить минимум 2 и максимум 5 пар. Подсчитаем, сколько в среднем нужно проверить пар битов. Пусть x случайная величина – количество проверяемых пар, p – вероятности значений x. Значения p_i найдём по формуле $p_i = \frac{C_3^1 \cdot C_3^{i-2}}{C_6^{i-1}} \cdot \frac{2}{6-i+1}$. Имеем закон распределения этой случайной величины:

x_i	2	3	4	5
p_i	0,2	0,3	0,3	0,2

Математическое ожидание mx = 3,5. Следовательно, в этом случае в среднем нужно проверить 3 – 4 пар битов.

В третьем случае имеем 6 верных (соответствуют одному передаваемому сообщению) и 9 неверных пар (соответствуют разным передаваемым сообщениям). Для нахождения двух пар из одного передаваемого сообщения надо проверить минимум 2 и максимум 11 пар.

Подсчитаем, сколько в среднем пар битов в этом случае надо проверить. Аналогично предыдущему, закон распределения для этой случайной величины:

Математическое ожидание mx = 4,57. Следовательно, в третьем случае в среднем нужно проверить 4 – 5 пар битов.

IV. ЗАКЛЮЧЕНИЕ

В заключение отметим следующее. Основным результатом работы является разработка универсального рекурсивного метода построения кодов большой длины на основе штейнеровых систем для криптосистем с коррекцией ошибок. Такие коды обладают максимальной мощностью и максимальной корректирующей способностью среди кодов с заданным числом единиц в кодовом слове. Доказан ряд свойств таких кодов, не описанных ранее в литературе. Построена криптосистема с простыми алгоритмами кодирования и декодирования и возможностью смены кода одной подстановкой.

ЛИТЕРАТУРА

1. **Мак-Вильямс Ф.Д.** Теория кодов, исправляющих ошибки / Ф.Д. Мак-Вильямс, Н.А. Слоэн – М.: Связь, 1979. – 744 с.
2. **Блейхут Р.** Теория и практика кодов, контролирующих ошибки / Р.Блейхут – М.: Мир, 1986. – 576 с.
3. **Берлекэмп Э.** Алгебраическая теорія кодирования / Э. Берлекэмп – М.: Мир, 1971. – 480 с.
4. **David J.C.** Information Theory, Inference, and Learning Algorithms / J.C. David, MacKay. − Cambridge University Press. − 2003.
5. **Ткаченко В.Г.** Перечисление типов монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – Одеса, 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. **Ткаченко В.Г.** Построение криптосистемы на основе треугольных кодов / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – 2012. – № 1. – С. 72 – 82.
8. **Tkachenko V.G.** Construction of cryptosystem on the basis quadrangular codes / Tkachenko V.G., Sinyavsky O.V. // Nauka i Studia. Przemyśl. – 2013. – т. 35 (103). – С. 18-28
9. **Холл М.** Комбинаторика / М. Холл – М.*:* Мир, 1970. – 424 с.
10. ***Камерон П.*** Теория графов, теория кодирования и блок-схемы / П. Камерон, Дж. ван Линт – М.: Наука, 1980. – 144 с.
11. **Картеси Ф.** Введение в конечные геометрии / Ф. Картеси – М.*:* Наука, 1980. – 320 с.

V.G. Tkachenco*, O.V. Sinyavsky**
* Odessa National Academy of Telecommunications named after O.S. Popov, str. Kovalska 1, 65029, Odessa
** Military Academy, str. Fontansky road, 10, 65009, Odessa

THE CRYPTOSYSTEM CONSTRUCTION ON THE POLYGONAL CODES BASIS

The polygonal block nonlinear codes are defined in the article. The methods of certain polygonal codes constructing is considered and effective universal recursive method of codes of great length constructing on the basis of Steiner systems for cryptosystems with error correction is proposed. Cryptosystem with correction code based on this code is developed. The advantages of this cryptosystem are speed encryption and decryption, as well as the ability to change the code quickly without encryption and decryption tables changing.

Keywords: *Correcting Codes - Nonlinear polygonal codes – Cryptosystem – Steiner system – Affine plane – Projective plane.*

REFERENCES

1. **McWilliams F.D.** Teoriya kodov, ispravlyaushih oshibki / F.D. McWilliams, N.A. Sloan – M.: Svyaz', 1979. – 744 s.
2. **Blahut R.** Teoriya i praktika kodov, kontrolirushih oshibki / R.Blahut – M.: Mir, 1986. – 576 s.
3. **Berlekamp E.** Algebraicheskaya teoriya kodirovaniya / E. Berlekamp – M.: Mir, 1971. – 480 s.
4. **David J.C.** Information Theory, Inference, and Learning Algorithms / J.C. David, MacKay. − Cambridge University Press. − 2003.
5. **Tkachenco V.G.** Perechislenie tipov monotonnih bulevih funkciy pri sinteze cifrovih shem / V.G. Tkachenco // Naukovi praci ONAZ iv. O.C.Popova. – Odesa, 2008. – №2. – S. 54 – 69.
6. **Tkachenco V.G.** Postroenie korrektirushego koda dlya kriptosistem na osnove tipov monotonnih bulevih funkciy / V.G. Tkachenco, O.V. Sinyavsky // Naukovi praci ONAZ iv. O.C.Popova. – Odesa, 2010. – № 1. – S. 85 – 92.
7. **Tkachenco V.G.** Postroenie kriptosistemi na osnove treugolnih kodov / V.G. Tkachenco, O.V. Sinyavsky // Naukovi praci ONAZ iv. O.C.Popova. – Odesa, 2012. – № 1. – S. 72 – 82.
8. **Tkachenco V.G.** Construction of cryptosystem on the basis quadrangular codes / Tkachenco V.G., Sinyavsky O.V. // Nauka i Studia. Przemyśl. – 2013. – t. 35 (103). – S. 18-28
9. **Holl M.** Kombinatorika / M. Holl – M.*:* Mir, 1970. – 424 s.
10. **Kameron P.** Teoriya grafov, teoriya kogirovaniya I blok-shemi / P. Kameron, J. van Lint – M.: Nauka, 1980. – 144 s.
11. **Kartesi F.** Vvedenie v konechnie geometrii / F. Kartesi – M.: Nauka, 1980. – 320 s.

Отримана в редакції 18.03.2014, прийнята до друку 29.04.2014