где WX – шифр сообщения X. Более того, алгоритм построения системы защиты информации с открытым ключом на основе рюкзака $\tilde{A}$ полностью совпадает с алгоритмом построения систем защиты информации с обобщённым рюкзаком $\tilde{A}_P$ [4].

Отметим, что данная теорема допускает все параметры обобщённой рюкзачной системы защиты информации с открытым ключом. При этом необходимо сделать ещё следующее замечание: процедура восстановления открытого текста, в целом, не зависит от самих компонент рюкзачного вектора $\tilde{A}$, она зависит только от размера самого рюкзака и способа первоначального кодирования элементарных сообщений открытого текста. Данное замечание относится ко всем существующим открытым рюкзачным системам.

Совершенно ясно, если для нестандартного рюкзака $\tilde{A}$ полагать что $m_1=m_2=...=m_n=p-1$, то все рассмотренные выше рассуждения относительно РСЗИ останутся в силе, что, в свою очередь, означает: их можно перенести на случай обобщённых рюкзаков $\tilde{A}_P$ с заданным максимальным числом $p-1$ повторений всех его компонентов. Если же полагать $m_1=m_2=...=m_n=1$, то мы соответственно получим РСЗИ со стандартным рюкзаком.

В обоих случаях рюкзаки без повторений, т.е. $k_1=k_2=...=k_n=1$. Очевидно, когда компоненты рюкзачного вектор $\tilde{A}$ с повторениями [5], т.е. хотя бы один элемент из множества $ZK_t=\{k_1,k_2,...,k_t\}$ больше единицы или то же самое, что $t<n$, то $\tilde{A}$ в данном случае сверхрастущим быть не может, и потому невозможно рассмотреть лёгкую задачу укладки рюкзака и, тем более, задачу построения СЗИ, использующей такой рюкзак.

В заключение подчеркнём, что для больших значений параметров нестандартных рюкзачных векторов, криптостойкость соответствующих систем защиты информации сравнительно выше, чем криптостойкость аналогичных стандартных СЗИ. В самом деле, если обозначить через $N(K)$ – количество всех вариантов выбора ключей, то для стандартного рюкзака оно равно $N(K)=2^n$, для обобщённого рюкзака – $N(K)=P^n$, а для нестандартного рюкзака $\tilde{A}$ – $N(K)=(m_1+1)(m_2+1)\ldots(m_n+1)$, где n – длина рюкзака.

СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 320 с.
2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
3. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001. – 260 с.
4. Осипян В.О. Об одном обобщении рюкзачных криптосистем // Известия вузов. Сев.-Кавк. регион. Техн. науки. – 2003. – Прилож. № 5. – С. 18–25.
5. Осипян В.О. О криптосистемах с заданным рюкзаком // Информационное противодействие угрозам терроризма. – 2004. – № 3. – С. 53–56.

УДК 681.326

ИСПРАВЛЕНИЕ ОДИНОЧНЫХ ОШИБОК В МНОГОФАЗНЫХ КОДАХ

Л.А. Белицкая

ФГУП «Научно-производственный центр «Полюс», г. Томск
E-mail: polus@online.tomsk.net

Предлагается использовать систематический код для исправления одиночных ошибок в многофазных кодах. С использованием теории цифро-векторных множеств строятся многомерные таблицы истинности и на их основе – геометрические образы исправленных сигналов.

Многофазный код является естественным кодом целого ряда устройств, где используются многофазные напряжения [1]. Он применяется в инверторах напряжения электроприводов переменного тока и других устройствах преобразовательной техники, в преобразователях угла в код и пересчетных схемах, в том числе и для выполнения всех арифметических операций [2]. Многофазный код наиболее исследован, и для него решена задача обнаружения и исправления ошибок исходя из его особой физической структуры. Эта особенность основана на контроле и сохранении непрерывности множеств логических нулей и единиц [2]. При этом можно исправлять не только одиночные ошибки, но и двойные, тройные и т.д., а также различные их пачки. Данные возможности возрастают с увеличением числа фаз кода, но наиболее ценно исправление именно одиночных ошибок. Недостаток многофазного кода в том, что ошибки, возникающие на границе единиц и нулей, не исправляются.

Рассмотрим многофазный код в многомерном цифровом пространстве с добавлением контрольных разрядов.

Особенность его заключается в том, что при последовательном прохождении кодовых комбина-

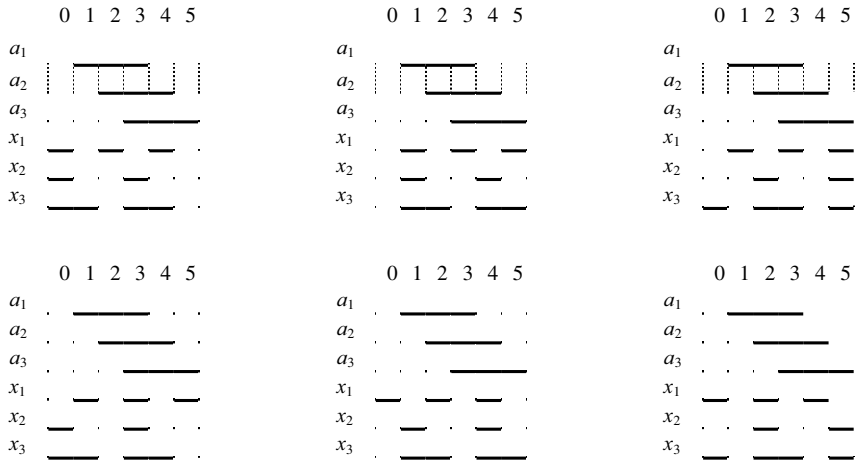

Рис. 1. *Зависимости трехфазных сигналов с контрольной частью*

ций кодовое расстояние между соседними равно 1, а все остальные имеют кодовое расстояние 2 и более. Для исправления всех одиночных ошибок достаточно добавить к многофазным сигналам три контрольных. Это позволяет получить кодовое расстояние не менее 3, что вполне достаточно для исправления всех одиночных ошибок.

Зависимости трехфазных сигналов a_1, a_2, a_3 с эквивалентными цифрами контрольной части x_1, x_2, x_3 представлены на рис. 1.

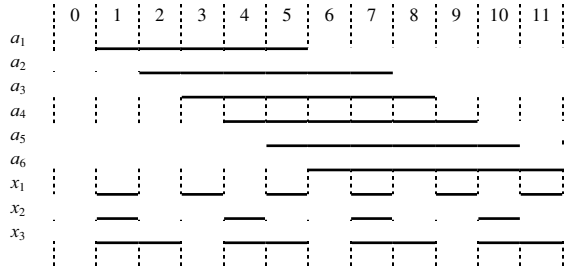

Рис. 2. *Зависимость шестифазных сигналов с контрольной частью*

При увеличении сигналов многофазного кода, кратных 3, кодовые последовательности циклически повторяются. Пусть $m=3p$ – количество фаз многофазного кода, где $p=1, 2, 3$ и т.д. Тогда последовательность 0, 7, 1, 4, 3, 5 с многофазным кодом связана следующими зависимостями:

$$x_1=a_1\oplus a_2\oplus a_3\oplus a_4\oplus a_5\oplus\ldots\oplus a_{m-1}\oplus a_m;$$

$$x_2=a_1\oplus a_2\oplus\ldots\oplus a_{k+1}\oplus a_{k+2}\oplus a_{k+4}\oplus a_{k+5}\ldots\oplus a_{m-2}\oplus a_{m-1};$$

$$x_3=a_1\oplus a3\oplus\ldots\oplus a_{k+1}\oplus a_{k+3}\oplus a_{k+4}\oplus a_{k+6}\ldots\oplus a_{m-2}\oplus a_m,$$

где $k=3i$, $i=0,1,2,\ldots,p-1$.

Проведем синтез исправления одиночных ошибок, например, шестифазного кода при использовании трех контрольных сигналов.

Выберем кодовую последовательность, где многофазные сигналы кода (a_1–a_6) связаны с эквивалентными цифрами контрольной части кода (x_1, x_2, x_3) зависимостью, показанной на рис. 2.

Контрольные сигналы в данном случае определяются зависимостями:

$$\begin{aligned} x_1&=a_1\oplus a_2\oplus a_3\oplus a_4\oplus a_5\oplus a_6;\\ x_2&=a_1\oplus a_2\oplus a_3\oplus a_4\oplus a_5; \qquad (1)\\ x_3&=a_1\oplus a_2\oplus a_3\oplus a_4\oplus a_6. \end{aligned}$$

В соответствии с выражениями (1) распределение цифр 0–11 при одиночных ошибках в многофазных и контрольных разрядах кода показано на рис. 3.

Неполное заполнение ячеек пространства (рис. 3) свидетельствует о несовершенстве и неплотности кода.

Учитывая, что $a_1=\{1,2,3,4,5,6\}$, $a_2=\{2,3,4,5,6,7\}$, $a_3=\{3,4,5,6,7,8\}$, $a_4=\{4,5,6,7,8,9\}$, $a_5=\{5,6,7,8,9,10\}$, $a_6=\{6,7,8,9,10,11\}$, покрытие геометрических образов множеств, подчиненных этим соотношениям в пространстве координат $(a_1,a_2,a_3,a_4,a_5,a_6)$ (x_1,x_2,x_3), определяет исправленные многофазные сигналы a_1'–a_6'.

Геометрический образ исправленного сигнала a_1' в многомерном пространстве показан на рис. 4.

Здесь и далее R – безразличное состояние ячеек пространства, используется для удобства покрытий, * – сигнал $a_1'=\{1,2,3,4,5,6\}$. На основании этого геометрического образа записываются логические выражения. Для сигнала a_1' имеем:

$1=a_4a_3a_2a_1\bar{x}_1$	$7=\bar{a}_4\,\bar{a}_3a_2a_1x_3\bar{x}_2\bar{x}_1$	$13=\bar{a}_6\,\bar{a}_5\,\bar{a}_4a_3a_2\bar{x}_3\bar{x}_2x_1$
$2=\bar{a}_6\bar{a}_5a_2a_1\,\bar{x}_1$	$8=a_6a_4a_3a_2a_1\bar{x}_2x_1$	$14=a_6a_5a_4a_3a_2\bar{x}_3\,\bar{x}_2\,\bar{x}_1$
$3=\bar{a}_6\,\bar{a}_5\,\bar{a}_4a_1x_1$	$9=\bar{a}_6a_5a_4a_1x_3\bar{x}_2x_1$	$15=\bar{a}_6a_5a_4a_3a_2x_3\bar{x}_2x_1$
$4=\bar{a}_6a_3a_2a_1x_1$	$10=a_6a_5a_4a_1\bar{x}_3\,\bar{x}_2\,\bar{x}_1$	$16=\bar{a}_4a_3a_2a_1\bar{x}_3\bar{x}_2x_1$
$5=\bar{a}_6\,\bar{a}_5x_3x_2\bar{x}_1$	$11=\bar{a}_6\,\bar{a}_5a_4\bar{a}_3\bar{a}_2a_1x_3\bar{x}_2$	
$6=\bar{a}_4\,\bar{a}_3\,\bar{a}_2a_1x_3x_2x_1$	$12=\bar{a}_6\,\bar{a}_5\,\bar{a}_4\,\bar{a}_3a_2x_3\bar{x}_2\bar{x}_1$	

Один из вариантов функциональной схемы исправления ошибок сигнала a_1 приведен на рис. 5.

Аналогично происходит исправление ошибок и в остальных сигналах многофазного кода.

Рассмотрим обнаружение и исправление ошибок, возникающих только на границе шестифазного кода, предполагая, что остальные ошибки уже исправлены по мажоритарному принципу [3].

Способ исправления одиночных ошибок, возникающих в любом разряде кода, поясняется рис. 6, где в ячейках 9-мерного пространства они проставлены в соответствии с зависимостью сигналов ше-

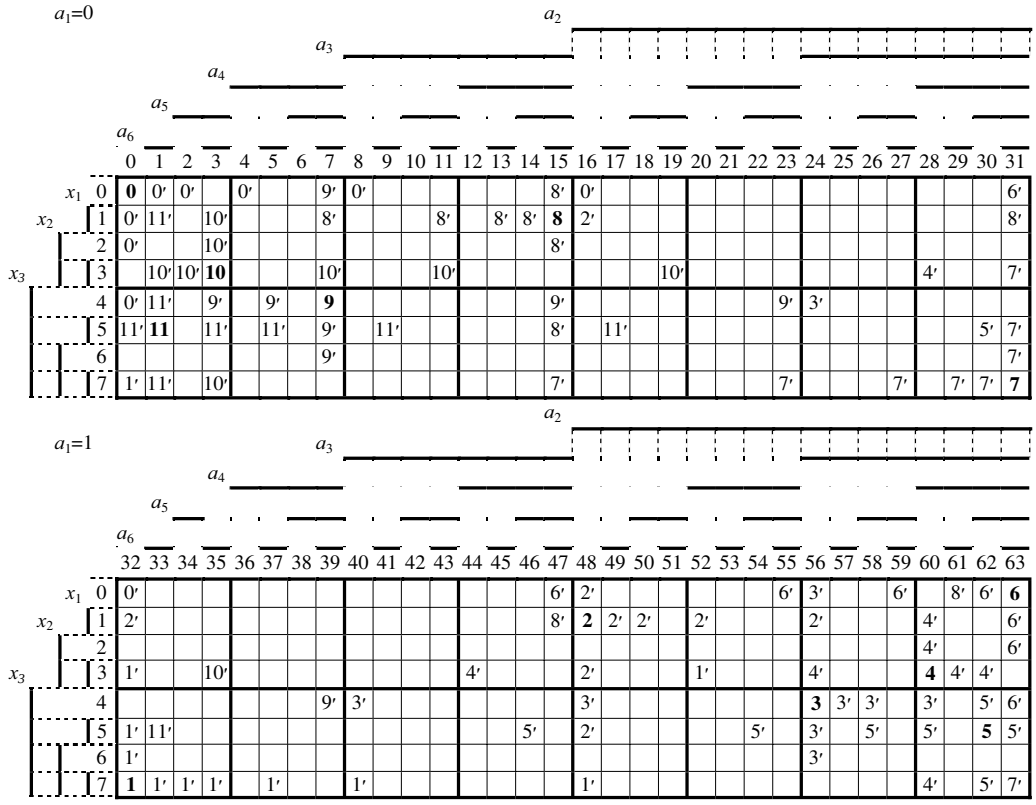

Рис. 3. *Одиночные ошибки в ячейках 9-мерного пространства*

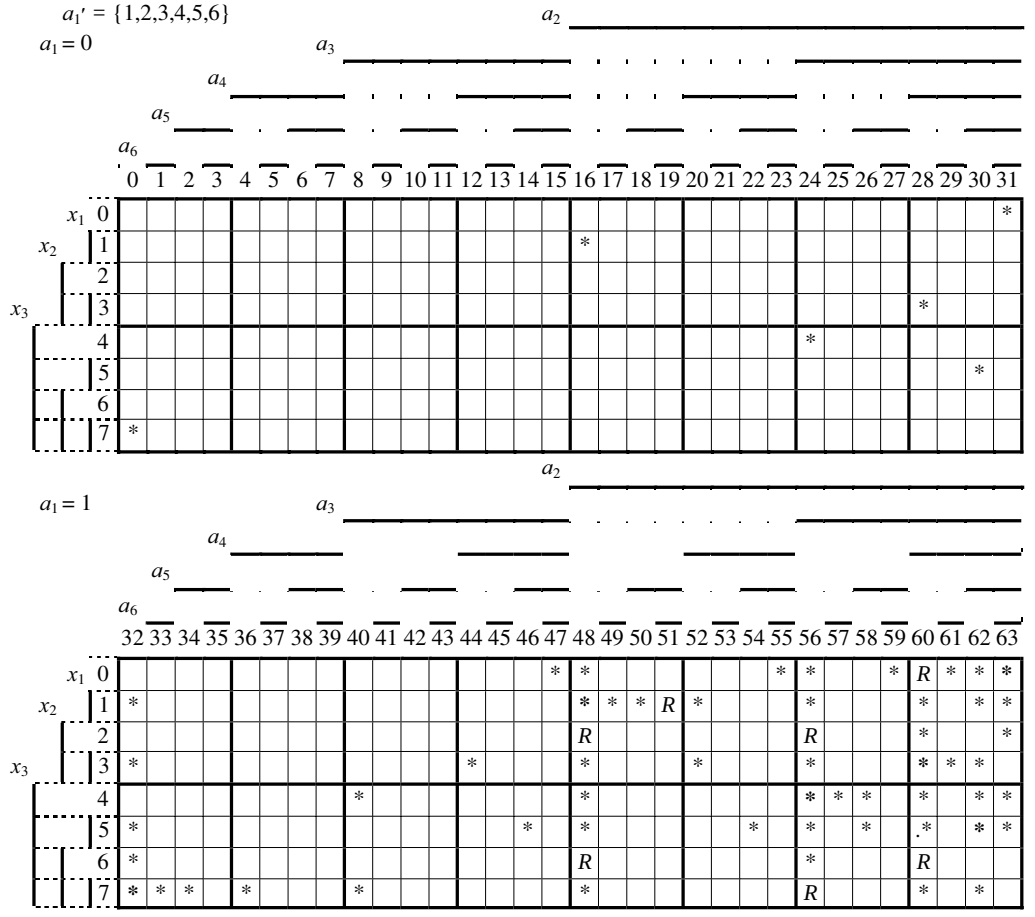

Рис. 4. *Геометрический образ сигнала* a_1'

стифазного кода a_1–a_6 от сигналов обычного цифрового кода. Для каждого геометрического образа сигналов a_1'–a_6' выбираются ячейки пространства, которые однозначно включаются в эти сигналы. Это позволяет получить в многомерном пространстве геометрические образы для сигналов многофазного кода a_1'–a_6', оптимальное покрытие которых определяет функции блока исправления ошибок.

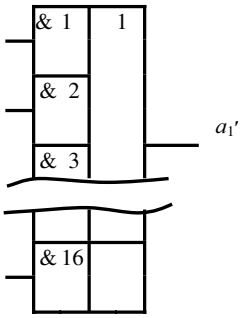

Рис. 5. *Функциональная схема исправления одиночных ошибок сигнала a_1*

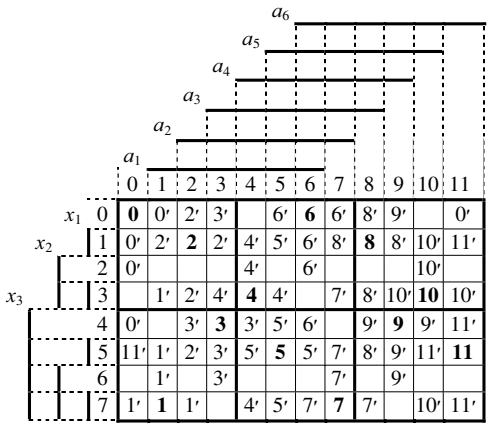

Рис. 6. *Одиночные ошибки в ячейках 9-мерного пространства, возникающие на границе шестифазного кода*

$a_1' = \{1,2,3,4,5,6\}$

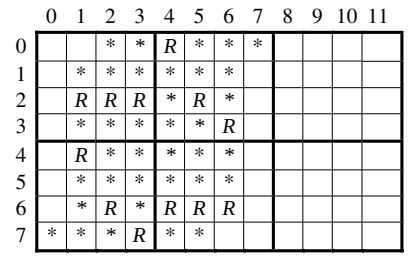

Рис. 7. *Геометрический образ сигнала a_1*

Геометрический образ исправленного сигнала a_1' в многомерном цифровом пространстве показан на рис. 7.

Логическая функция исправления ошибок в первой фазе имеет следующий вид:

$$a_1' = a_2\bar{x}_1\,\bar{x}_2\,\bar{x}_3 \vee a_1x_1\bar{x}_2\,\bar{x}_3 \vee a_1\bar{x}_1x_2\,\bar{x}_3 \vee a_1\bar{x}_1x_2x_3 \vee$$
$$\vee\, a_1x_1\bar{x}_2\,\bar{x}_3 \vee a_2x_1x_2\bar{x}_3 \vee a_1\bar{x}_1x_2x_3 \vee \bar{a}_6x_1x_2x_3. \qquad (2)$$

Обозначим конъюнкции выражения (2) следующим образом:

$1=a_2\bar{x}_1\,\bar{x}_2\,\bar{x}_3$	$4=a_1\bar{x}_1x_2x_3$	$7=a_1\bar{x}_1x_2x_3$
$2=a_1x_1\bar{x}_2\,\bar{x}_3$	$5=a_1x_1\bar{x}_2\,\bar{x}_3$	$8=\bar{a}_6x_1x_2x_3$
$3=a_1\bar{x}_1x_2\,\bar{x}_3$	$6=a_2x_1x_2\bar{x}_3$	

Аналогичным образом строятся в многомерном цифровом пространстве геометрические образы для сигналов a_2'–a_6' и для исправленных контрольных сигналов x_1'–x_3'.

Логическое выражение (2) позволяет построить весьма простую принципиальную схему, работающую в режиме реального времени, для исправления одиночных ошибок в первом разряде многофазного кода.

Функциональная схема исправления одиночных ошибок сигнала a_1 показана на рис. 8.

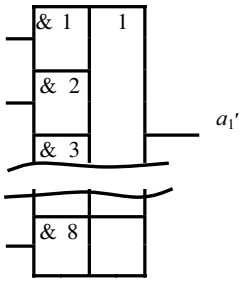

Рис. 8. *Функциональная схема исправления одиночных ошибок сигнала a_1*

Из двух представленных вариантов синтеза видно, что построение устройств исправления ошибок многофазного кода возможно на основе ряда установленных логических функций. Однако первый вариант (рис. 5) требует больших аппаратурных затрат для их реализации, второй – уменьшает эти затраты, но увеличивает число уровней схемы исправления ошибок в два раза и более и, следовательно, время на преобразование.

Таким образом, изложенная методика исправления одиночных ошибок с использованием теории цифро-векторных множеств позволяет создавать резервированные устройства, работающие в многофазном коде с максимальным быстродействием и повышенной надежностью. Результаты целесообразно использовать в цифровых системах управления, функционирующих в режиме реального времени, когда необходимо обеспечить высокую надежность и помехозащищенность.

СПИСОК ЛИТЕРАТУРЫ

1. Четти П. Проектирование ключевых источников электропитания. – М.: Энергоатомиздат, 1990. – 240 с.
2. Кочергин В.И. Теория многомерных цифро-векторных множеств в приложениях к электроприводам и системам электропитания. – Томск: Изд-во ТГУ, 2002. – 400 с.
3. А.с. 987681 СССР. МКИ G11C 19/00. Регистр / В.И. Кочергин. Заявлено 28.08.1980; Опубл. 07.01.1983, Бюл. № 1. – 6 с.: ил.