УДК 519.711.72

Белецкий А.Я.
(Национальный авиационный университет, Киев)

МАТРИЧНЫЕ ЦИКЛИЧЕСКИЕ ГРУППЫ МАКСИМАЛЬНОГО ПОРЯДКА, ПОРОЖДАЕМЫЕ ОБОБЩЕННЫМИ ПРЕОБРАЗОВАНИЯМИ ГРЕЯ

Введение

В работах [1,2] предлагается строить блочные криптографические шифры на основе обратимых матриц над полем $GF(2)$. Если $\boldsymbol{X}$, $\boldsymbol{Y}$ – векторы, представляющие соответственно открытый и зашифрованный текст, а $\boldsymbol{M}$ - шифрующая матрица, то зашифрование задается уравнением $\boldsymbol{Y} = \boldsymbol{M} \cdot \boldsymbol{X}$, а расшифрование – уравнением $\boldsymbol{X} = \boldsymbol{M}^{-1} \cdot \boldsymbol{Y}$. Для обмена сеансовыми ключами в системе авторы предлагают использовать протокол Диффи – Хэллмана (DH) [3] в циклической группе матриц $\langle \boldsymbol{M} \rangle$, причем матрица считается общедоступной. Предполагается, что пользователь А вырабатывает случайный показатель x, вычисляет матрицу $\boldsymbol{M}^x$ и посылает ее пользователю В. В свою очередь пользователь В вырабатывает случайный показатель y, вычисляет матрицу $\boldsymbol{M}^y$ и посылает ее пользователю А. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу (ключ шифрования) $\boldsymbol{M}^{xy} = \boldsymbol{M}^{yx}$. Поскольку мощность группы, образующим элементом которой являются невырожденные двоичные матрицы $\boldsymbol{M}$ (рекомендуемый порядок должен быть не менее чем 100), велико, то вычисление ключа, как утверждают авторы (кстати, без доказательства), имеет переборную сложность.

Очевидно, что одной из важных проблем, которая возникает в ходе реализации матричных алгоритмов DH, состоит в формировании шифрующих матриц $\boldsymbol{M}$. Матрицы $\boldsymbol{M}$ должны быть невырожденными, что естественно. К ним также предъявляется еще такое требование. Порядок циклической группы, образуемой степенями $\boldsymbol{M}$ в кольце вычетов по mod 2, должен быть по возможности максимальным. Или, другими словами, последовательность элементов указанной группы, которую для простоты мы будем называть $\boldsymbol{M}$ – группой, должна обладать свойствами m-последовательности.

Целью данной статьи является разработка алгоритмов синтеза гарантированно невырожденных двоичных матриц высокого порядка, последовательность степеней которых в кольце вычетов по mod 2 образует циклическую группу максимальной длины (m-последовательность). В основу синтеза таких матриц положен метод обобщенных преобразований Грея [4], являющийся расширением классических кодов Грея [5].

Общие соотношения

Пусть L_n есть мощность (число элементов) $\boldsymbol{M}$ - группы. Степени $\boldsymbol{M}$ образуют m-последовательность, если

$$L_n = 2^n - 1, \qquad (1)$$

где n – порядок матрицы $\boldsymbol{M}$.

Матрицы $\boldsymbol{M}$, период цикла которых удовлетворяет условию (1), будем называть *n-полными*. Соответственно, последовательности, образуемые степенями n-полных матриц $\boldsymbol{M}$ в циклической группе, также будем именовать n-полными последовательностями. Приведем другие примеры n-полных последовательностей. Таковыми является натуральные последовательности n-битных двоичных чисел, или последовательности элементов расширенных полей Галуа $GF(2^n)$ без нулевого элемента и т. д.

Далее мы покажем, что если M есть n-полная матрица, то порядок p (длина в битах) случайных двоичных векторов x и y, участвующих в формировании матриц зашифрования M_{cr} и расшифрования M_{dc}, может быть выбран равным

$$p = n/2. \quad (2)$$

В самом деле, пусть выполняется условие (2). Это означает, что десятичные эквиваленты векторов x и y (обозначим их L_x и L_y соответственно) не будут превышать значения

$$L = 2^{n/2} - 1. \quad (3)$$

Принимая во внимание ограничение (3), запишем матрицу зашифрования в виде

$$M_{cr} = (M^{L_x})^{L_y} = M^{L_x \cdot L_y} = M^{L_M}. \quad (4)$$

Согласно соотношениям (3) и (4)

$$L_M \le \left(2^{n/2} - 1\right)^2,$$

то есть,

$$L_M \le 2^n - 2^{n/2+1} + 1. \quad (5)$$

Из сопоставления выражений (1) и (5) очевидно, что

$$L_M < L_n,$$

а из этого следует, что для n-полных матриц M в качестве двоичных векторов x и y вполне можно использовать $(n/2)$ – битные векторы.

Обобщенные коды Грея

В известной (классической) схеме [5] процесс формирования прямых и обратных кодов Грея (КГ) развивается по направлению слева направо. По этой причине, а также в силу того, что можно построить систему преобразования, подобную кодам Грея, но по направлению формирования справа налево, классические коды Грея названы нами *левосторонними*.

Обозначим разряды числа, представленного в позиционном коде, через $x_{n-1}, x_{n-2}, ..., x_1, x_0$ (старший разряд слева), а разряды того же числа, выраженного в коде Грея, через $y_{n-1}, y_{n-2}, ..., y_1, y_0$, где n – число разрядов в кодовых векторах x и y. Системы счисления пары x и y имеют одинаковое двоичное основание.

Процесс преобразования вектора x в вектор y (классический код Грея) на примере пятибитных кодовых комбинаций показан на рис. 1. На этом рисунке отрезки дуг символизируют операцию суммирования по mod 2.

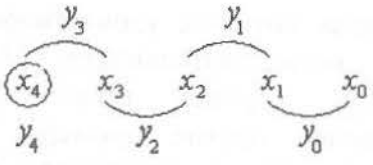

Рис.1. Схема формирования классических кодов Грея

Правило преобразования компонент вектора x в компоненты вектора y достаточно просто и имеет вид:

$$y_i = x_{i+1} \overset{2}{\oplus} x_i, \quad i = \overline{n-1, 0}, \quad x_n = 0, \tag{6}$$

где $\overset{2}{\oplus}$ – операция поразрядного сложения по mod 2, которую для операндов a и b мы будем записывать и в такой форме $c = (a+b)_2$.

Изложение материала по кодовым преобразованиям целесообразно вести, опираясь на структурные схемы формирования кодов. Такой подход к пояснению сути алгоритма кодирования удобен тем, что делает материал не только более понятным для инженеров, но существенно упрощает задачу формального математического описания процедуры кодирования.

Для того чтобы придать структурным схемам законченную форму, ограничим (без потери общности) порядок системы уравнений (6), полагая $n = 4$. Тогда

$$\begin{aligned} y_3 &= x_3; \\ y_2 &= (x_3 + x_2)_2; \\ y_1 &= (x_2 + x_1)_2; \\ y_0 &= (x_1 + x_0)_2. \end{aligned} \tag{7}$$

Структурная схема, соответствующая алгоритму преобразования (7), показана на рис. 2.

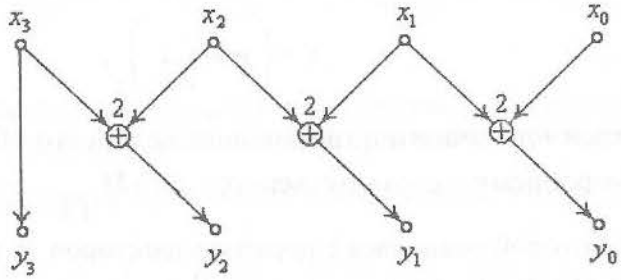

Рис.2. Структурная схема алгоритма формирования прямого двоичного кода Грея левостороннего

Преобразование (7) можно представить в матричной форме:

$$y = \left(x M_{\overset{\rightarrow}{\text{ÊÃ}}} \right)_2,$$

где x и y – вектор-строки двоичного позиционного кода и его изображения по коду Грея прямому левостороннему соответственно, а $M_{\overset{\rightarrow}{\text{ÊÃ}}}$ – квадратная матрица прямого левостороннего преобразования Грея n-го порядка. В частности, для системы уравнений (7) матрица $M_{\overset{\rightarrow}{\text{ÊÃ}}}$ имеет вид:

$$M_{\overset{\rightarrow}{\text{ÊÃ}}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

К *обратному* левостороннему (классическому) преобразованию Грея приходим, решая обычными алгебраическими приемами систему модульных уравнений (7) относительно разрядов x_i исходной кодовой комбинации x. В частности, из соотношений (7) имеем:

$$\begin{aligned} x_3 &= y_3 ; \\ x_2 &= (y_3 + y_2)_2 ; \\ x_1 &= (y_3 + y_2 + y_1)_2 ; \\ x_0 &= (y_3 + y_2 + y_1 + y_0)_2 . \end{aligned} \qquad (8)$$

В системе уравнений (8) учтено, что $(-1)_2 = 1$.

Преобразованию (8) отвечает структурная схема, показанная на рис. 3.

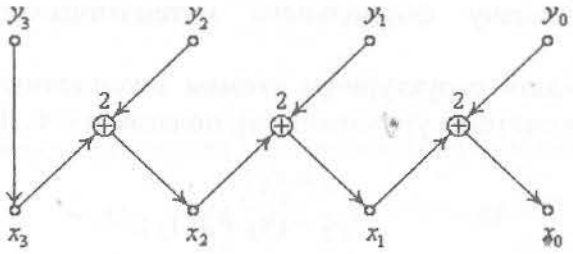

Рис.3. Структурная схема алгоритма формирования обратного двоичного кода Грея левостороннего

Обратные левосторонние преобразования Грея двоичных кодовых комбинаций (как и прямые преобразования) можно представить в матричной форме

$$\boldsymbol{x} = \left(\boldsymbol{y}\, \boldsymbol{M}_{\overset{\circ}{\underset{\text{ÎÊÃ}}{\rightarrow}}} \right)_2 ,$$

где $\boldsymbol{y}$ и $\boldsymbol{x}$ есть вектор-строки двоичного позиционного кода и его обратного преобразования по коду Грея левостороннему соответственно, а $\boldsymbol{M}_{\overset{\circ}{\underset{\text{ÎÊÃ}}{\rightarrow}}}$ – квадратная матрица преобразования, порядок которой совпадает с порядком векторов $\boldsymbol{x}$ и $\boldsymbol{y}$.

Системе уравнений (8) отвечает матрица обратного левостороннего преобразования Грея

$$\boldsymbol{M}_{\overset{\circ}{\underset{\text{ÎÊÃ}}{\rightarrow}}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} .$$

Рассмотренные алгоритмы преобразования двоичных кодовых комбинаций из пространства оригиналов в пространство изображений (коды Грея), в равной степени, как и алгоритмы преобразования двоичных кодовых комбинаций из пространства изображений в исходный позиционный код, соответствуют классической трактовке формирования прямого и обратного кодов Грея, достаточно хорошо изученных и описанных в многочисленных научных публикациях и технической литературе. Вместе с тем, не было обращено внимание на возможность генерации кодов, подобных классическим (левосторонним) прямым и обратным кодам Грея, процесс формирования которых выполняется от младших разрядов кода к старшим, т.е. развивается по направлению справа налево. В таком классе преобразований Грея, который назван *правосторонним*, при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа.

К структурной схеме алгоритма формирования прямого кода Грея двоичного правостороннего (рис. 4) приходим, развернув на 180° вокруг центральной вертикальной оси

структурную схему алгоритма формирования прямого кода Грея левостороннего (рис. 2), сохраняя при этом неизменным положение операндов преобразования.

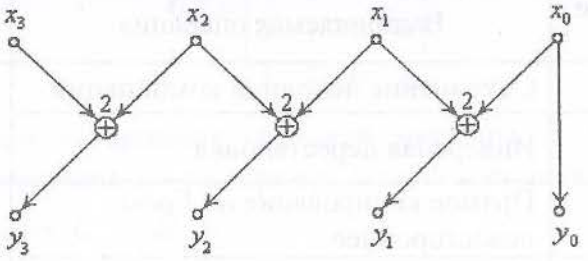

Рис.4. Структурная схема алгоритма формирования прямого двоичного кода Грея правостороннего

Аналогичным образом конструируется структурная схема алгоритма формирования обратного двоичного кода Грея правостороннего (рис. 5).

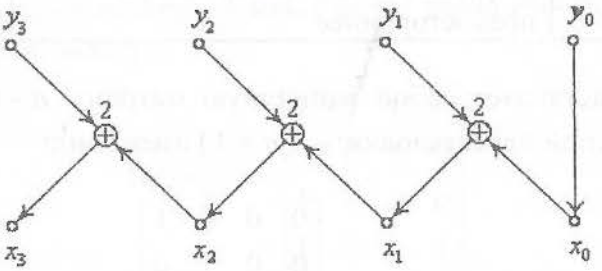

Рис.5. Структурная схема алгоритма формирования обратного двоичного кода Грея правостороннего

Правосторонние преобразования Грея можно представить в матричных формах, а именно

$$y = \left(x M_{\overleftarrow{\text{ÊÃ}}} \right)_2 \quad \text{и} \quad x = \left(y M_{\overleftarrow{\text{ÎÊÃ}}} \right)_2,$$

причем

$$M_{\overleftarrow{\text{ÊÃ}}} = M^T_{\overrightarrow{\text{ÊÃ}}}; \quad M_{\overleftarrow{\text{ÎÊÃ}}} = M^T_{\overrightarrow{\text{ÎÊÃ}}}.$$

Следовательно

$$M_{\overleftarrow{\text{ÊÃ}}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}; \quad M_{\overleftarrow{\text{ÎÊÃ}}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Введем для основных операторов (матриц) преобразований Грея символьное обозначение g_i, полагая, что индексы $i = 2, 3, 4$ и 5 отвечают прямым (2, 4) и обратным (3, 5) лево- (2, 3) и правосторонним (4, 5) кодам. Дополнив перечисленную совокупность операторов операторами сохранения исходной комбинации g_0 и инверсной перестановки g_1, приходим к полной группе (табл.1) *простых операторов Грея.* В дальнейшем для обозначения операторов вместо символов кодов будем использовать также их цифровые индексы.

Таблица 1. Полная группа простых операторов Грея

Обозначение оператора	Выполняемая операция	Аббревиатура оператора
e (или 0)	Сохранение исходной комбинации	–
1	Инверсная перестановка	ИП
2	Прямое кодирование по Грею левостороннее	$\overset{\circ\rightarrow}{}$ КГ
3	Обратное кодирование по Грею левостороннее	$\overset{\circ\rightarrow}{}$ ОКГ
4	Прямое кодирование по Грею правостороннее	$\overset{\leftarrow\circ}{}$ КГ
5	Обратное кодирование по Грею правостороннее	$\overset{\leftarrow\circ}{}$ ОКГ

Оператор g_0 представляет собой единичную матрицу $n-$го порядка, а матричная форма оператора инверсной перестановки g_1 ($n=4$) имеет вид:

$$1 = g_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Из элементов полной группы простых операторов Грея можно сформировать так называемые *составные коды Грея* (СКГ), образуемые произведением простых (элементарных) кодов Грея.

Аналитически СКГ можно представить соотношением

$$G = \prod_{j=1}^{k} g_j ,$$

где g_j – простой КГ, выбираемый из полной группы $\{\overline{g_0, g_5}\}$, а k – порядок СКГ.

Как простые, так и составные коды Грея обладают рядом замечательных свойств. Во-первых, отвечающие им матрицы преобразования являются невырожденными и в силу этого оказываются обратимыми. И, во-вторых, существуют достаточно простые алгоритмы обращения СКГ.

Подтвердим последнее утверждение на простом примере. Пусть $n=4$ и $G=4251$. Выбранному СКГ отвечает матрица преобразования

$$G = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \quad (9$$

Пусть, кроме того, задана степень $k=2$ матрицы G. Согласно (9) имеем

$$G^2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \qquad (10)$$

В общем случае для вычисления обратной матрицы $k-$й степени образующего элемента G циклической группы $L-$го порядка можно воспользоваться, по крайней мере, такими способами. Поскольку $G^L \equiv E$, то:

Вариант 1. $\overline{G^k} = G^{L-k}$;

Вариант 2. $\overline{G^k} = G^k \cdot G^{L-2k}$.

Порядок циклической группы L, порождаемой матрицей G в (9), равен семи. Это означает, что $G^7 = E$. Каждый из приведенных выше вариантов оценок обратной матрицы приводит к одинаковому результату

$$\overline{G^2} = G^5 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \qquad (11)$$

Перемножив матрицы прямого (10) и обратного (11) преобразований, получим единичную матрицу, как и должно быть.

Вариант 3, касающийся СКГ, заданных в символической аналитической форме. Он состоит их двух этапов. На первом этапе символическая запись кода переписывается в обратном порядке. На втором этапе каждый простой оператор Грея заменяется соответствующим ему обратным оператором. Например, если $G = 24135$, то $\overline{G} = 42153$. В самом деле,

$$G \cdot \overline{G} = 2413\overline{5 \cdot 42}153 = E. \qquad (12)$$

В конструкции (12) симметрично относительно знака умножения находятся взаимно обратные простые коды (две пары таких кодов, для примера, выделены связующими линиями), произведение которых равно единичной матрице. И, следовательно, полное произведение множителей в средней части выражения (12) также равно E, что и подтверждает корректность определения обратного СКГ по третьему варианту.

Можно воспользоваться еще одним (четвертым, но далеко не последним) вариантом обращения СКГ. Поясним его на примере обращения кода G, заданного матрицей (9). Система линейных модульных уравнений прямого преобразования Грея, отвечающая матрице преобразования (9), имеет вид:

$$y_3 = x_1;$$
$$y_2 = (x_2 + x_1 + x_0)_2;$$
$$y_1 = (x_3 + x_2 + x_0)_2;$$
$$y_0 = x_0.$$

Решив данную систему относительно переменных x_i, $i = \overline{0,3}$, получим

$$x_3 = (y_3 + y_2 + y_1)_2;$$
$$x_2 = (y_3 + y_2 + y_0)_2;$$
$$x_1 = y_3;$$
$$x_0 = y_0.$$

Данной системе уравнений соответствует матрица обратного преобразования

$$\overline{G} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}. \qquad (13)$$

Перемножив матрицы (9) и (13), приходим к единичной матрице, что подтверждает правильность выполненных вычислений.

Синтез *n*-полных матриц

Перейдем теперь непосредственно к задаче синтеза невырожденных *n*-полных матриц M. Как показали результаты компьютерных расчетов, интересными свойствами обладают матрицы, отвечающие СКГ типа $1g$, где $g = \overline{2,5}$. Замечательная особенность таких матриц состоит в том, что порядок L_n циклических групп, порождаемых операторами $1g$, за небольшим исключением (названных нами артефактом), определяется соотношением:

$$L_n = 2^m - 1, \quad m \le n, \qquad (14)$$

где n – порядок матрицы.

В табл. 2 приведены оценки L_n, полученные прямыми компьютерными вычислениями.

Таблица 2. Порядок циклических групп, отвечающих СКГ $G = 1g$

n	L_n	n	L_n	n	L_n	n	L_n
		9	2^9-1	17	$2^{12}-1$	25	2^8-1
2	2^2-1	10	2^6-1	18	87381	26	$2^{26}-1$
3	2^3-1	11	$2^{11}-1$	19	$2^{12}-1$	27	$2^{20}-1$
4	2^3-1	12	$2^{10}-1$	20	$2^{10}-1$	28	2^9-1
5	2^5-1	13	2^9-1	21	2^7-1	29	$2^{29}-1$
6	2^6-1	14	$2^{14}-1$	22	$2^{12}-1$	30	$2^{30}-1$
7	2^4-1	15	2^5-1	23	$2^{23}-1$	31	2^6-1
8	2^4-1	16	2^5-1	24	$2^{21}-1$	32	2^6-1

Из анализа данных, представленных в табл.2, приходим к таким выводам. Во-первых, подтверждается форма оценки L_n, заданная соотношением (14). Исключение (артефакт) проявляется лишь в точке $n = 18$, в которой

$$L_{18} = 87381_{10} = 10101010101010101_2 = (2^{18} - 1)/3.$$

Попробуем разобраться более подробно с отмеченным «недоразумением», т.е. артефактом. Двоичный эквивалент десятичного числа $2^{18} - 1$ представляет собой последовательность из 18-ти единичек. Умножив двоичный вектор L на три, как раз и получим значение $L_{18} = 2^{18} - 1$. Таким образом, на числовом отрезке длиной $2^{18} - 1$ укладывается три интервала периода $L = 87381$. А это означает, что как степень 87381, так и степень $2^{18} - 1$ обращают M в единичную матрицу. Этим и объясняется появление артефакта.

Во-вторых, существуют такие значения порядка n (в табл. 2 они выделены затенением), для которых элементы групп, порождаемые степенями матриц M, составляют последовательность максимальной длины, равную $2^n - 1$.

Одним из важнейших результатов, к которому мы приходим на основании анализа табл.2, состоит в том, что период цикла группы $1g$, представляет собою *степенную величину*. Это обстоятельство, во-первых, дает нам возможность существенно сократить затраты машинного времени, необходимые для вычисления оценок L_n. И, во-вторых, наталкивает на мысль, о целесообразности поиска других выражений для СКГ (отличных от $1g$), которые порождают n-полные матрицы M. И такие СКГ были найдены. Часть из них, для примера, представлена в табл. 3.

Таблица 3. Составные коды Грея, доставляющие двоичным матрицам свойство n-полноты

Порядок матрицы (n)			
32	64	128	256
2244424	22533435	2425535	22533435
2442224	22534335	2433534	22534335
12242253	24334225	2435334	24334225
12242443	25224334	22524224	25224334
12252242	222524424	22533334	2222535224

Свойства *n*-полных матриц

Пусть M есть n-полная двоичная матрица, отвечающая СКГ G. Относительно n-полных матриц M легко доказать (методом непосредственной проверки) следующее положение.

Утверждение. *n-полнота матриц M инвариантна к группам линейных преобразований Ω над СКГ G и преобразований Q над строками и столбцами матриц M.*

В состав Ω – группы входят такие операторы линейных преобразований над G: циклического сдвига, обращения (I), инверсии (R) и сопряжения (C), а также произвольные комбинации этих операторов.

Кратко поясним суть преобразований, входящих в Ω группу. Введем (табл. 4) символику для операторов Ω – группы преобразований. Стрелки оператора циклического сдвига указывают направление прокрутки СКГ G, а нижний индекс k- задает число разрядов прокрутки. Например, $\overleftarrow{1}_3$ означает, что СКГ подвергается циклическому сдвигу по

часовой стрелке на три разряда (символа) кода. Если $k=1$, то нижний индекс цифрового символа оператора циклического сдвига будем для простоты опускать.

Таблица 4. Символическое обозначение операторов преобразования

Обозначение оператора	Тип преобразования
$\vec{1}_k$, $\overleftarrow{1}_k$	Циклический сдвиг
I	Обращение
R	Инверсия
C	Сопряжение

Преобразование типа «обращение» соответствует вычислению обратного СКГ. «Инверсия» означает запись операторов СКГ в порядке, обратному последовательности простых операторов в исходном СКГ. И, наконец, преобразованиям типа «сопряжение» отвечают вычисления простого g^* или составного G^* операторов, сопряженных операторам g или G, которые определяются соотношениями:

$$g^* = 1 \cdot g \cdot 1; \quad G^* = 1 \cdot G \cdot 1.$$

Будем называть преобразования, представленные в табл. 4, Ω – преобразованиями. Обозначим через F составной оператор преобразования из Ω – группы линейных преобразований. Например, $F = \vec{1}_k \cdot R \cdot C$ или $F = R \cdot I$ и т.д., а Ω – преобразования над G будем записывать в виде $F\{G\}$.

Предположим, что некая n-полная матрица M образована составным кодом $G = 25224334$. Фактически СКГ отвечает произведению (в кольце вычетов по mod 2) двоичных матриц n-го порядка. Это означает, что правила преобразования СКГ G совпадают с общими правилами преобразования над произведением матриц. Сведем в табл. 5 результаты простых преобразований P над этим произведением.

Таблица 5. Пример преобразований

Оператор преобразования	Результат преобразования
$\overleftarrow{1}_2$	22433425
I	52253343
R	43342252
C	25524434

В частности, $\vec{1}_3 C\{25224334\} = 55244342$ и т.д.

Q – группу линейных преобразований над n-полными матрицами M составляют операторы «дружной перестановки» строк и столбцов матрицы, частным случаем которых являются операторы «дружного циклического сдвига» строк и столбцов матрицы M.

Проиллюстрируем «дружную перестановку» строк и столбцов на примере матрицы M шестого порядка, сформированной СКГ $G = 12435$. Для удобства отобразим исходную матрицу в виде табл. 6. Выбрав «дружную перестановку» $\pi = 204153$, приходим к матрице, показанной в табл. 7. Исходная матрица, как и матрица, образованная «дружно

перестановкой» ее строк и столбцов (не имеет значение, как организована дружная перестановка: сначала по столбцам, а потом по строкам, или наоборот), являются образующими элементами циклических групп одинакового порядка.

Таблица 6. Исходная матрица

		0	1	2	3	4	5
0		1	1	1	1	1	0
1		0	0	0	0	1	0
2		0	0	0	1	0	0
3		0	0	1	0	0	0
4		0	1	0	0	0	0
5		1	1	0	1	0	1

Таблица 7. «Дружная перестановка» строк и столбцов исходной матрицы

		2	0	4	1	5	3
2		0	0	0	0	0	1
0		1	1	1	1	0	1
4		0	0	0	1	0	0
1		0	0	1	0	0	0
5		0	1	0	1	1	1
3		1	0	0	0	0	0

«Дружный циклический сдвиг» строк и столбцов матриц сводится к циклической прокрутке столбцов по часовой стрелке на заданное число разрядов, а затем к циклической прокрутке строк матрицы сверху вниз на тоже число разрядов (или наоборот, сначала прокручиваются строки, а затем столбцы матрицы).

Выводы

Целесообразность применения в криптографии и в других приложениях матриц, отвечающих составным кодам Грея, объясняется рядом замечательных свойств, которыми они обладают. Во-первых, матрицы, порождаемые СКГ любого порядка, чрезвычайно просто генерировать. Во-вторых, такие матрицы являются гарантированно невырожденными. В-третьих, для них легко вычисляются обратные матрицы. В-четвертых, как установлено на основании компьютерного моделирования, для произвольных порядков n матриц существуют такие СКГ, которые доставляют соответствующим матрицам свойство n- полноты. Это свойство проявляется в том, что порядок циклических групп, формируемых этими матрицами, достигает максимального значения, равного $2^n - 1$. И, наконец, в-пятых, если некоторая матрица $\boldsymbol{M}$ является n-полной, то это свойство сохраняется инвариантным к группам линейных $\boldsymbol{Q}$ – преобразований над строками и столбцами матриц $\boldsymbol{M}$ и $\boldsymbol{\Omega}$ – преобразований над СКГ $\boldsymbol{G}$.

Список литературы

1.*Ерош И.Л.* Адресная передача сообщений с использованием матриц над полем GF(2) / Ерош И.Л., Скуратов В.В. // Проблемы информационной безопасности. Компьютерные системы. 2004, №1. – С. 72-78.

2.*Ерош И.Л.* Скоростное шифрование разнородных сообщений / Ерош И.Л., Сергеев М.Б // Проблемы информационной безопасности. 2004. № 1. С. 72 – 78.

3.*Diffie W., Hellman M.E., "New Directions in Cryptography"*, IEEE Transactions on Information Theory, **v. IT-22**, no. 6, November 1976, 644-654.

4.*Белецкий А.Я.* Преобразования Грея. Монография в 2-х томах / Белецкий А.Я., Белецкий А.А., Белецкий Е.А. Т.1. Основы теории. – К.: Кн. изд-во НАУ, 2007. – 506 с., Т.2. Прикладные аспекты. – К.: Кн. изд-во НАУ, 2007. – 644 с.

5.*Gray F.* Pulse code communication. – Pat USA, № 2632058, 1953.

На основі узагальнених кодів Грея розробляються алгоритму синтезу гарантовано невироджених двійкових матриць, послідовність степенів яких в кільці залишків за mod 2 створює послідовність максимальної довжини.

Ключові слова: мультиплікативна група, узагальнені коди Грея, послідовність максимальної довжини.

На основе обобщенных кодов Грея разрабатываются алгоритмы синтеза гарантированно невырожденных двоичных матриц, последовательность степеней которых в кольце вычетов по mod 2 образует циклическую группу максимального порядка.

Ключевые слова: мультипликативная группа, обобщенные коды Грея, последовательности максимальной длины.

Based on the generalized Gray codes developed algorithms for synthesis guaranteed nonsingular binary matrices, the sequence of degrees are in the ring of residues mod 2 form a cyclic group of maximum order.

Keywords: the multiplicative group, the generalized Gray codes, the sequence of maximum length.

Рецензент:д.т.н., проф.Скрипник Л.В.
Надійшла 06.10.2010

УДК: 004.056.5

Карпінець В. В., Яремчук Ю. Є. (ВНТУ)

АНАЛІЗ ВПЛИВУ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ НА ЯКІСТЬ ВЕКТОРНИХ ЗОБРАЖЕНЬ

Вступ

На сьогодні в системах передавання інформації все більшого поширення отримують цифрові зображення векторного формату, що використовуються для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв'язку з цим виникає проблема, пов'язана з можливістю нелегального копіювання та розповсюдження векторних зображень, які мають свого правовласника.

Для вирішення задачі захисту авторських прав цифрових векторних зображень використовуються стеганографічні стеганосистеми цифрових водяних знаків (ЦВЗ), що дають змогу маркувати об'єкти захисту для подальшого виявлення неправомірного використання зображення. Підтвердження права власності на векторне зображення у випадку спорів досягається витягненням ЦВЗ, який може містити інформацію про власника, час та місце створення, фірмовий логотип.

Залежно від того, яка інформація потрібна системі для того, щоб виявити ЦВЗ - оригінал зображення, ЦВЗ, секретний ключ чи додаткова інформація, вони поділяються на чотири типи: конфіденційні, напівконфіденційні, напіввідкриті та відкриті стеганосистеми [1]. Найбільш перспективними є відкриті стеганосистеми, які для своєї роботи, окрім секретного ключа, не вимагають ні знання оригінального зображення, ні вбудованого ЦВЗ, що полегшує процедуру підтвердження авторських прав. Проте для відкритих стеганосистем, на відміну від конфіденційних чи напівконфіденційних, існує проблема необхідності більшої зміни зображення при вбудовуванні ЦВЗ для забезпечення можливості розпізнавання бітів ЦВЗ без оригіналу зображення, а тільки на основі самого зміненого зображення та стегоключа.