УДК 511.623.3

Белецкий А.Я.

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ПРИМИТИВНЫХ МАТРИЦ

Предложены алгоритмы построения обобщенных примитивных матриц Галуа и Фибоначчи произвольного порядка n, элементы которых принадлежат простому полю $GF(p)$, $p \geq 2$. Рассмотрены примеры применения таких матриц в задачах синтеза обобщенных линейных регистров сдвига с линейными обратными связями и матричных аналогов протокола Диффи-Хеллмана.

Ключевые слова: неприводимые и примитивные полиномы, примитивные матрицы, генераторы псевдослучайных последовательностей, протокол обмена ключами шифрования.

Введение и постановка задачи. Пусть $A = (a_{i,j})$ является положительной невырожденной матрицей порядка $n > 1$ над полем целых неотрицательных чисел таких, что $a_{i,j} \in GF(p)$ для всех $i, j = \overline{1, n}$, и $E = (\delta_{i,j})$, где $\delta_{i,j}$ – символ Кронекера, есть единичная матрица того же порядка, что и A. Матрица A невырожденная в поле $GF(p)$, если ее определитель $\det A$ по модулю p не равен нулю, т.е. $\det A \,(\mathrm{mod}\, p) \in \overline{1, p-1}$, где p - простое число. Операция возведения матрицы A в некоторую степень t выполняется в кольце вычетов по модулю p, при этом каждый элемент матрицы A^t приводится к неотрицательному остатку по модулю p. Последовательность степеней матрицы A, начиная с нулевой степени, для которой $A^0 = E$, образует *циклическую группу* порядка e.

Матрицу A будем называть *примитивной*, если наименьшее натуральное e, при котором $A^e = E$, удовлетворяет соотношению

$$e = p^n - 1. \tag{1}$$

Параметр e в (1) называется *экспонентом* или *показателем примитивности матрицы* A. Параметр e совпадает с порядком (ord) циклической (мультипликативной) группы, *образующим элементом* которой является матрица A. Суть термина «примитивная» матрица подобна, в определенной мере, сути термина «примитивный элемент» поля $GF(2^n)$. Матрица E играет роль *единицы* в алгебре циклических групп, порождаемых примитивными матрицами A.

Простейшим примером двоичных примитивных матриц являются матрицы, адекватно отображающие процесс формирования псевдослучайных бинарных последовательностей посредством *линейных регистров сдвига* (ЛРС) *с линейными обратными связями по схемам* (конфигурациям) *Галуа* и *Фибоначчи* [1, 2]. ЛРС длиной n бит может находиться в одном из $2^n - 1$ ненулевых внутренних состояний S_k, $k = \overline{0, 2^n - 2}$. Только ЛРС с особо подобранными функциями обратных связей могут проходить через все $2^n - 1$ внутренние состояния – это так называемые *регистры максимального периода.* Для того чтобы ЛРС был регистром максимального периода, соответствующий полином обратной связи должен быть *примитивным полиномом* $\mathrm{mod}\, 2$.

Обратим внимание на то обстоятельство, что когда речь идет о классическом ЛРС, то под этим подразумевается, что разряды регистра (триггеры) могут находиться в одном из двух состояний: 0 или 1. Такие регистры являются двоичными ЛРС, и они приобретают свойства регистров максимального периода, если только обратные связи образуются примитивными полиномами над полем Галуа характеристики 2.

В данной статье мы расширим понятие ЛРС, полагая, что каждый его разряд (ячейка памяти регистра) может находиться в одном из p состояний $s \in GF(p)$. При этом обратные связи в *обобщенных регистрах* максимального периода, определяемого значением $p^n - 1$, формируются, в частном случае, примитивными полиномами над полем характеристики

$p \geq 2$. В более общем случае в качестве полинома обратной связи могут быть использованы произвольные *неприводимые полиномы* (НП) f_n, совсем не обязательно примитивные. Относительно таких НП будем говорить, что они *приобретают* свойство примитивности. Естественно, что для достижения неприводимым полиномом f_n указанного свойства достаточно в качестве образующего элемента ω мультипликативной группы максимальной длины использовать *примитивный элемент поля* $GF(p^n)$ над НП f_n.

Для простоты будем иногда именовать обобщенные ЛРС максимального периода и отвечающие им обобщенные примитивные матрицы Галуа и Фибоначчи *регистрами* и *матрицами Галуа* и *Фибоначчи* (определения приводятся ниже) *характеристики* p.

Основная задача, которая ставится в данной работе, состоит в разработке алгоритмов построения *обобщенных матриц Галуа и Фибоначчи* n – го порядка над полем $GF(p)$, $p \geq 2$, однозначно определяющих как структуру соответствующих обобщенных n – разрядных ЛРС максимального периода, так и формируемых ими (регистрами) псевдослучайных последовательностей чисел из множества $GF(p)$ длины $p^n - 1$.

Общие соотношения. В данном параграфе мы обсудим некоторые особенности понятия «примитивного полинома» (ПрП) и придадим ему трактовку, несколько отличающуюся от общепринятой. В литературе по теории помехоустойчивого кодирования, например [4], дается такое определение ПрП: неприводимый над $GF(p)$ полином f_n степени n называется *примитивным*, если его корень α является *примитивным элементом* расширенного поля $GF(p^n)$. В свою очередь, примитивным является такой элемент α поля $GF(p^n)$, который порождает мультипликативную группу максимального порядка $\langle\alpha\rangle = GF^*(p^n)$. Это означает, что последовательность степеней примитивного элемента α, начиная с нулевой, в кольце вычетов по модулю f_n содержит все ненулевые элементы поля $GF(p^n)$. В криптографических источниках, например [5], понятие ПрП вводится следующим образом: примитивным является такой неприводимый полином $f_n(x)$, который делит без остатка двучлен $x^e - 1$, при условии, что минимальное e задано соотношением (1). И, наконец, в классической математической литературе, например [6], понятие примитивности формулируется так: многочлен f_n степени n является примитивным многочленом над $GF(p)$ в том и только в том случае, если он – нормированный многочлен, такой, что $f_n \neq 0$ и $\mathrm{ord}\,(f_n) = p^n - 1$, где ord означает порядок многочлена.

Между приведенными определениями ПрП нет никакого противоречия. Фактически они означают одно и то же, что мы поясним далее, уточняя физический смысл термина «примитивный полином».

Использованные ранее обозначения f_n и $f_n(x)$, которые мы будем применять и в дальнейшем, соответствуют двум формам (векторной и алгебраической) представления НП. Например, бинарному вектору

$$f_8 = 100011011$$

соответствует алгебраическая форма двоичного неприводимого полинома

$$f_8(x) = x^8 + x^4 + x^3 + x + 1.$$

Итак, согласно приведенным выше определениям, полином $f_n(x)$ степени n над $GF(p)$ является примитивным, если он неприводим, а наименьший показатель e, при котором $f_n(x)$ делит двучлен $\Phi(x) = x^e - 1$ без остатка, определяется выражением $p^n - 1$. Данное определение (назовем его первым) примитивного полинома $f_n(x)$ можно отобразить такими эквивалентными соотношениями:

$$f_n(x) \mid x^e - 1; \tag{2}$$

или

$$x^e \equiv 1 \,(\mathrm{mod}\ f_n(x)), \tag{3}$$

при условии, что

$$\min e = p^n - 1. \tag{4}$$

Предложим второй (авторский) вариант определения примитивного полинома. Неприводимый полином $f_n^{(\omega)}$ степени n (совсем не обязательно примитивный) *приобретает свойство примитивности*, если последовательность степеней некоторого выбранного $m-$битного, $1 < m < n$, примитивного элемента ω_m поля $GF(p^n)$ над НП f_n, приведенных к остатку по модулю $f_n^{(\omega)}$, образует последовательность максимальной длины ($m-$последовательность), при этом число элементов последовательности удовлетворяет условию (4). Предлагаемое обобщение понятия примитивного полинома сводится к следующему. Заменим основание x одночлена x^e в формулах (2) и (3) произвольным полиномом $\omega_m(x)$ степени m такой, что $1 < m < n$. Тем самым представим эти выражения в виде:

$$f_n^{(\omega)}(x) \left| [\omega_m(x)]^e - 1; \right. \tag{5}$$

или

$$[\omega_m(x)]^e \equiv 1 \bmod f_n^{(\omega)}(x), \tag{6}$$

при соблюдении условия (4).

Следовательно, *примитивными являются такие неприводимые над простыми полями Галуа характеристики p полиномы n-й степени* (необходимые условия), *которые порождают циклические группы максимального порядка $p^n - 1$, причем минимальный образующий элемент группы совпадает с характеристикой поля* (достаточные условия).

Данное определение можно назвать «инженерным», не являющимся математически строгим, но которое послужит в дальнейшем основой построения предлагаемых *обобщенных примитивных полиномов*.

В табл. 1 приведен полный список двоичных неприводимых полиномов восьмой степени, согласно которой 16 полиномов являются примитивными ($\omega_{\min} = 10$), а оставшиеся полиномы приобретают свойство примитивности при различных минимальных значениях образующих элементов.

Безусловно, что $f_n^{(\omega)} \equiv f_n$, также как и $f_n^{(\omega)}(x) \equiv f_n(x)$. Верхний индекс (ω) используется нами исключительно лишь с целью подчеркнуть: НП в векторной f_n или алгебраической $f_n(x)$ формах приобретает свойство примитивности лишь при условии, что полином ω является примитивным элементом поля $GF(p^n)$ над выбранным НП. Таким образом, выражаясь болем точно, соотношениями (5) и (6) не вводится новое определение ПрП, а лишь подчеркивается, что НП приобретает свойство примитивности.

Введем ряд обозначений. Пусть $L_{n,\,p} = p^n - 1$ есть общее число n-разрядных векторов с элементами над $GF(p)$, за исключением нулевого вектора; $L_{n,\,p}^{(\omega)}$ - число образующих элементов ω, доставляющих НП f_n свойство примитивности, которое определяется [6] функцией Эйлера φ аргумента $L_{n,\,p}$, т.е.

$$L_{n,\,p}^{(\omega)} = \varphi(L_{n,\,p}). \tag{7}$$

Неприводимые полиномы восьмой степени Таблица 1

Номер полинома	Значение полинома	ω_{min}	Номер полинома	Значение полинома	ω_{min}
1	100011011	11	16	110001011	110
2	100011101	10	17	110001101	10
3	100101011	10	18	110011111	11
4	100101101	10	19	110100011	101
5	100111001	11	20	110101001	10
6	100111111	11	21	110110001	110
7	101001101	10	22	110111101	111
8	101011111	10	23	111000011	10
9	101100011	10	24	111001111	10
10	101100101	10	25	111010111	111
11	101101001	10	26	111011101	111
12	101110001	10	27	111100111	10
13	101110111	11	28	111110011	110
14	101111011	1001	29	111110101	10
15	110000111	10	30	111111001	11

В самом деле, в любой абелевой группе по умножению порядка $L_{n,\,p}$ число ее элементов ω, взаимно простых с $L_{n,\,p}$ (степени именно таких элементов формируют мультипликативную группу максимальной длины), составляет величину, являющуюся функцией Эйлера аргумента $L_{n,\,p}$. Тем самым мы и приходим к выражению (7).

В качестве примера в табл. 2 приведено полное множество образующих элементов, представленных в троичной форме, доставляющих свойство примитивности неприводимому полиному

$$f_4 = 12101 \tag{8}$$

над полем $GF(3^4)$. Полином (8) не является примитивным.

Примитивные элементы поля $GF(3^4)$ над НП $f_4 = 12101$ Таблица 2

j	***i***							
	1	2	3	4	5	6	7	8
0	101	102	120	122	201	202	210	211
8	1010	1012	1021	1022	1102	1111	1112	1122
16	1200	1211	1220	1222	2011	2012	2020	2021
24	2100	2110	2111	2122	2201	2211	2221	2222

Номер k образующего (примитивного) элемента (ОЭ) определяется суммой номера столбца i и значения строки j табл. 1, т.е. $k = i + j$. Последовательность максимальной длины, равной 80, формируемой примитивным элементом $\omega = 1102$ и выделенного затенением в табл. 1, сведена в табл. 3.

Непосредственной проверкой легко убедиться в том, что для любого примитивного полинома f_n минимальным ОЭ ω, порождающим мультипликативную группу $GF^*(p^n)$, является полином $\omega = p$ (в векторной форме), который в произвольной p-ичной системе счисления представим в виде $\omega = 10$. Следствием отмеченного факта является то, что $(k+1)$-я степень элемента ω образуется в результате сдвига на один шаг влево полинома ω^k. Если

при этом разрядность полинома ω^{k+1} превышает n и становится равной $n+1$, то он (полином ω^{k+1}) приводится к остатку по $\bmod f_n$.

Мультипликативная группа $GF^*(3^4)$ над НП (8) и $\omega = 1102$ Таблица 3.

j	*i*									
	1	2	3	4	5	6	7	8	9	10
0	0001	1102	1001	2211	1221	2001	0020	1111	2121	2122
10	0221	1222	0100	1021	0022	0012	1120	0211	2000	2221
20	0110	0210	1201	1220	1202	2022	2200	1200	0121	0201
30	0111	1012	2202	0101	2120	1020	2220	2011	2212	2020
40	0002	2201	2002	1122	2112	1002	0010	2222	1212	1211
50	0112	2111	0200	2012	0011	0021	2210	0122	1000	1112
60	0220	0120	2102	2110	2101	1011	1100	2100	0212	0102
70	0222	2021	1101	0202	1210	2010	1110	1022	1121	1010

Рассмотрим пример. Пусть $n = 2$ и $f_2 = 112$ есть примитивный над $F(3)$ полином.Если α – корень f_2, то $f_2(\alpha) = \alpha^2 + \alpha + 2 = 0$. Следовательно, $\alpha^2 = 2\alpha + 1$.

Разместим в табл. 4 элементы поля $GF^*(3^2)$ над ПрП $f_2 = 112$. В левой половине таблицы элементы поля представлены в виде степеней t корня α полинома f_2 (алгебраическая форма), а в правой – в виде степеней образующего элемента $\omega = 10$ (векторная форма).

Соответствие между различными формами представления элементов поля $GF^*(3^2)$ над ПрП $f_2 = 112$ Таблица 4

t	Алгебраическая форма		Векторная форма	
0	0	1	0	1
1	0	α	1	0
2	2α	1	2	1
3	2α	2	2	2
4	0	2	0	2
5	2α	0	2	0
6	α	2	1	2
7	α	1	1	1
8	0	1	0	1

Как следует из табл. 4, замена корня α на вектор $\omega = 10$ преобразует алгебраическую форму представления элементов поля $GF^*(3^2)$ в векторную. Точно к такому же результату приходим и в общем случае для элементов поля $GF^*(p^n)$ над произвольным примитивным элементом ω поля.

Подводя итоги данного параграфа, сформулируем предварительный вывод: примитивными являются такие неприводимые полиномы f_n, минимальный образующий элемент ω степеней которых ω^k, $k = 0, 1, \ldots$, по модулю f_n формирует последовательность максимальный длины (m -последовательность), совпадает с характеристикой $p = 10$ поля $GF(p^n)$, т.е. $\omega_{\min} = p$. В этом, собственно, и состоит физический смысл примитивных полиномов. Вместе с тем, как мы это уже отмечали выше, любому неприводимому

полиному, в том числе и такому, который не является примитивным по классическому определению, можно придать свойство примитивности, если принять следующее соглашение. Каждый НП f_n приобретает свойство примитивности над некоторым образующим элементом ω, если последовательность степеней этого элемента по модулю f_n формирует последовательность максимального периода $p^n - 1$. И, как известно, такими ОЭ являются примитивные элементы $GF(p^n)$.

Синтез примитивных матриц Галуа и Фибоначчи над *GF(2)*. Термины «матрица Галуа» и «матрица Фибоначчи» заимствованы из теории криптографии и кодирования [1, 2], в которых широко используются так называемые генераторы псевдослучайных последовательностей (ПСП) по схемам Галуа и Фибоначчи.

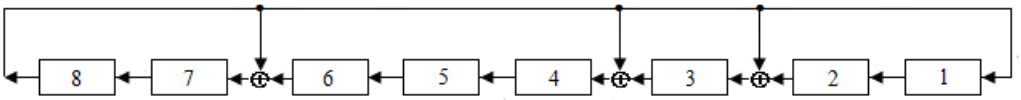

Рис. 1. Структурная схема генератора Галуа над ПрП $f_8 = 101001101$

На рис. 1 приведена структура устройства (генератора элементов поля $GF^*(2^8)$) в конфигурации Галуа (генератора Галуа), соответствующего ПрП $f_8 = 101001101$. В качестве элементов памяти разрядов ЛРС использованы двоичные D-триггеры, уровень сигнала на выходе которых (0 или 1) после подачи синхроимпульса повторяет уровень сигнала, подведенного к входу триггера. Элемент $\oplus$ в ЛРС осуществляет операцию сложения по модулю 2 (операцию XOR). Генератор Галуа, представленный на рис. 1, сопоставляет каждому ненулевому элементу поля $GF(2^8)$ соответствующую степень примитивного элемента $\omega = 10$ по модулю ПрП $f_8 = 101001101$.

Как следует из структурной схемы генератора (рис. 1) обратные связи в простых (классических) регистрах Галуа однозначно определяются выбранным ПрП f и формируются следующим образом: отклики каждого разряда поступают на входы последующих разрядов, являясь для них функциями возбуждения. Кроме того, отклик старшего разряда регистра подается (по схеме XOR) на входы тех и только тех разрядов регистра, номера которых совпадают с ненулевыми номерами мономов ПрП. При этом младшему моному, расположенному справа полинома f, соответствует номер 1, как и младшему разряду (D – триггеру) регистра.

На основании алгоритма функционирования ЛРС, показанного на рис. 1, легко вычислить последовательность состояний регистра S_k, начиная с $S_0 = 00000001$. Фрагмент последовательности S_k представлен в табл. 5.

Последовательность состояний ЛРС Галуа над $f_8 = 101001101$ Таблица 5

k	S_k	k	S_k	k	S_k	k	S_k
0	00000001	8	01001101	16	11111000	24	00000110
1	00000010	9	10011010	17	10111101	25	00001100
2	00000100	10	01111001	18	00110111	26	00011000
3	00001000	11	11110010	19	01101110	27	00110000
4	00010000	12	10101001	20	11011100	28	01100000
5	00100000	13	00011111	21	11110101	29	11000000
6	01000000	14	00111110	22	10100111	30	11001101
7	10000000	15	01111100	23	00000011	31	11010111

Обозначим G_f матрицу, которая допускает рекуррентное определение состояний ЛРС Галуа над ПрП f по формуле:

$$S_{k+1} = S_k \cdot G_f, \quad S_0 = 00000001. \tag{9}$$

Тем самым вектором S_0 выделяется нижняя строка (припишем ей номер 1) матрицы

$$G_{f_8} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{10}$$

Следовательно, в нижней строке матрицы G_{f_8} необходимо поместить значение S_1, совпадающее с минимальным образующим элементом $\omega = 10$ поля $GF^*(2^8)$ над ПрП $f_8 = 101001101$. Продолжая подобным образом операции преобразований, приходим к окончательному выражению (10) для матрицы G_{f_8}.

Исходя из соотношения (10), определим алгоритм формирования матриц Галуа G_{f_n} следующим образом. Пусть $f_n -$ векторная форма примитивного двоичного полинома степени n такая, что $f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\}$, $u_i \in \{0,1\}$, $i = \overline{1, n-1}$ и $\omega = 10 -$ минимальный образующий элемент поля $GF^*(2^n)$. Поместим ОЭ, равный вектору 10, справа нижней строки матрицы G_{f_n} и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы G_{f_n}, кроме элементов верхней строки, запишем нули. Согласно предложенному правилу (назовем его *правилом диагонального заполнения*) в верхней строке матрицы G_{f_n} следует ожидать появления $(n+1)$-битного вектора 100…0, что недопустимо, так как порядок матрицы равен n. Приводя этот $(n+1)$-битный вектор к остатку по модулю f_n, приходим к тому, что в верхней строке двоичной матрицы G_{f_n} необходимо поместить ПрП f_n, исключая его старшую единицу, т.е. $n -$ битный вектор $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

Общую форму матрицы Галуа $n -$ го порядка можно представить в виде:

$$G_{f_n} = \begin{pmatrix} u_{n-1} & u_{n-2} & u_{n-3} & \cdots & u_3 & u_2 & u_1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{11}$$

Элементарными вычислениями легко убедиться в том, что матрица (10) преобразованием (9) порождает ту же самую $m-$последовательность порядка 255, что и ЛРС, показанный на рис. 1. Из сопоставления матрицы (10) и соответствующей ей структурной схемы ЛРС (рис. 1) приходим к элементарным выражениям для функций возбуждения ν_k $D-$триггеров классических генераторов ПСП в конфигурации Галуа над двоичными примитивными полиномами $f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\}$. Пусть $s_k -$состояние $k-$го разряда (триггера) регистра. Тогда

$$\nu_1 = s_n;\ \nu_{k+1} = s_k \oplus u_k \cdot s_n,\ k = \overline{1, n-1}.$$

В дополнении к матрицам Галуа можно ввести также *матрицы Фибоначчи* F_f над ПрП f_n, отвечающие ЛРС по схеме Фибоначчи (генераторы ПСП Фибоначчи). Матрицы Фибоначчи взаимно однозначно связаны с матрицами Галуа G_f *оператором правостороннего транспонирования* $\perp$ (транспонирования относительно вспомогательной диагонали), т.е.

$$F_f \overset{\perp}{\longleftrightarrow} G_f. \tag{12}$$

Из соотношений (10) и (12) следует, что

$$F_{f_8} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{13}$$

Структура устройства (генератора элементов поля $GF^*(2^8)$) в конфигурации Фибоначчи, соответствующая матрице (13), приведена на рис. 2.

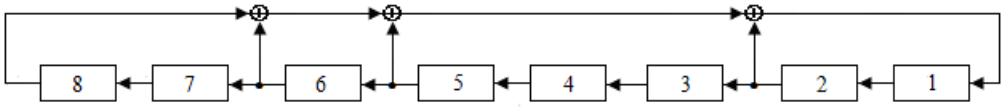

Рис. 2. Структурная схема генератора Фибоначчи над ПрП $f_8 = 101001101$

Общую форму матрицы Фибоначчи n-го порядка можно представить в виде:

$$F_{f_n} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & u_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & u_2 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & u_3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & u_{n-3} \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & u_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & u_{n-1} \end{pmatrix}. \tag{14}$$

Матрицы Галуа и Фибоначчи, введенные соотношениями (11) и (14), принадлежат подмножеству *матриц Фробениуса* [7], которые обычно записывают в такой форме:

$$\Phi = \begin{bmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -\alpha_{n-1} \end{bmatrix}.$$

Матрицу Фробениуса называют еще *сопровождающей матрицей* многочлена

$$f(x) = x^n - \alpha_{n-1}x^{n-1} - \alpha_{n-2}x^{n-2} - \cdots - \alpha_0 .$$

Если положить $f(x) = f_n(x)$, где

$$f_n(x) = x^n + u_{n-1}x^{n-1} + u_{n-2}x^{n-2} + \cdots + u_1 x + 1,$$

есть ПрП степени n, то матрица Фробениуса Φ преобразуется в матрицу Фибоначчи (14).

Функции возбуждения D – триггеров ЛРС Фибоначчи описываются выражениями:

$$\nu_1 = \bigoplus_{k=1}^{n} u_{n-k} \cdot s_k; \quad \nu_k = s_{k-1}, \ k = \overline{2, n}.$$

На основании алгоритма функционирования ЛРС Фибоначчи, показанного на рис. 2, можно легко вычислить последовательность состояний регистра S_k, начиная с состояния $S_0 = 00000001$. Фрагмент последовательности S_k представлен в табл. 6.

Последовательность состояний ЛРС Фибоначчи над $f_8 = 101001101$ Таблица 6

k	S_k	k	S_k	k	S_k	k	S_k
0	00000001	8	01011000	16	11001100	24	10110110
1	00000010	9	10110001	17	10011001	25	01101100
2	00000101	10	01100011	18	00110010	26	11011001
3	00001010	11	11000110	19	01100101	27	10110010
4	00010101	12	10001100	20	11001011	28	01100100
5	00101011	13	00011001	21	10010110	29	11001001
6	01010110	14	00110011	22	00101101	30	10010011
7	10101100	15	01100110	23	01011011	31	00100111

Кроме рассмотренных форм примитивных матриц Галуа G_f и Фибоначчи F_f каждой из них могут быть поставлены в соответствие так называемые сопряженные матрицы G_f^* и F_f^*, которые вводятся преобразованиями:

$$\begin{aligned} G_f^* &= 1 \cdot G_f \cdot 1; \quad G_f = 1 \cdot G_f^* \cdot 1; \\ F_f^* &= 1 \cdot F_f \cdot 1; \quad F_f = 1 \cdot F_f^* \cdot 1, \end{aligned} \tag{15}$$

где 1 - условное обозначение инволютивного оператора инверсной перестановки, представляющего собой квадратную матрицу n – го порядка, на вспомогательной диагонали которой стоят единицы, а в остальных элементах – нули, при этом $1^{-1} = 1$, $1^2 = E$.

Для иллюстрации ниже приведена матрица инверсной перестановки четвертого порядка

$$1:=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}. \qquad (16)$$

Как следует из (15), сопряженные матрицы G_f^* и F_f^*, образуются в результате инверсной перестановки строк и столбцов исходных (базовых) матрицы G_f и F_f. В частности, на основании матриц (11) и (14) по формулам (15) для сопряженных ЛРС получим:

$$G_{f_n}^*=\begin{pmatrix}0&1&0&\cdots&0&0\\0&0&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&1&0\\0&0&0&\cdots&0&1\\1&u_1&u_1&\cdots&u_{n-2}&u_{n-1}\end{pmatrix}; \qquad (17)$$

$$F_{f_n}^*=\begin{pmatrix}u_{n-1}&1&0&\cdots&0&0\\u_{n-2}&0&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\u_2&0&0&\cdots&1&0\\u_1&0&0&\cdots&0&1\\1&0&0&\cdots&0&0\end{pmatrix}. \qquad (18)$$

Согласно общим формам сопряженных матриц Галуа (17) и Фибоначчи (18) для ПрП $f_8=101001101$ приходим к структурным схемам восьмиразрядных генераторов ПСП, представленных на рис. 3 и 4 соответственно. Под рисунками приведены выражения для функций возбуждения $D-$триггеров генераторов.

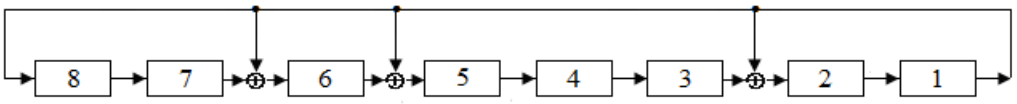

Рис. 3. Структурная схема сопряженного генератора Галуа над ПрП $f_8=101001101$

$$\nu_n=s_1;\quad \nu_k=s_{k+1}\oplus u_{n-k}\cdot s_1,\quad k=\overline{1,n-1}. \qquad (19)$$

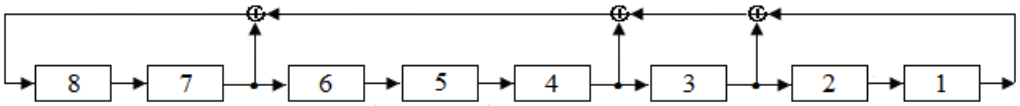

Рис. 4. Структурная схема сопряженного генератора Фибоначчи над ПрП $f_8=101001101$

$$\nu_k=s_{k+1},\quad k=\overline{1,n-1};\quad \nu_n=s_1\overset{n}{\underset{k=2}{\oplus}}u_{k-1}\cdot s_k. \qquad (20)$$

На основании алгоритмов функционирования сопряженных ЛРС Галуа и Фибоначчи, показанных на рис. 3 и 4, легко можно вычислить последовательности состояний регистров S_k генераторов ПСП. Фрагменты последовательностей S_k для генераторов ПСП

представлены в табл. 7 и 8 соответственно. К этим же значениям состояний можно прийти также по формулам (19) и (20).

Последовательность состояний сопряженного генератора Галуа над $f_8 = 101001101$ Таблица 7

k	S_k	k	S_k	k	S_k	k	S_k
0	00000001	8	00111110	16	11000000	24	11101011
1	10110010	9	00011111	17	01100000	25	11000111
2	01011001	10	10111101	18	00110000	26	11011010
3	10011110	11	11101100	19	00011000	27	11011010
4	01001111	12	01110110	20	00001100	28	01101101
5	10010101	13	00111011	21	00000110	29	10000100
6	11111000	14	10101111	22	00000011	30	01000010
7	01111100	15	11100101	23	10110011	31	00100001

Последовательность состояний сопряженного генератора Фибоначчи над $f_8 = 101001101$ Таблица 8

k	S_k	k	S_k	k	S_k	k	S_k
0	00000001	8	00110101	16	11100110	24	11000000
1	10000000	9	00011010	17	01110011	25	11100000
2	01000000	10	10001101	18	00111001	26	11110000
3	10100000	11	11000110	19	00011100	27	11111000
4	01010000	12	01100011	20	00001110	28	01111100
5	10101000	13	00110001	21	00000111	29	10111110
6	11010100	14	10011000	22	00000011	30	01011111
7	01101010	15	11001100	23	10000001	31	00101111

Из сопоставления базовых матриц Галуа G и Фибоначчи F, а также их сопряженных (подобных) вариантов G^* и F^* легко могут быть определены операторы преобразования одной из известных матриц, в любую другую матрицу. Пусть $M \in \{G, G^*, F, F^*\}$. Методом непосредственной проверки легко убедиться в том, что к сопряженным матрицам приходим в результате выполнения над исходной матрицей операций классического (левостороннего, T) и правостороннего ($\perp$) транспонирования, выполняемых в произвольной последовательности. Следовательно, оператор сопряжения $1 \circ 1$ можно представить совокупностью (произведением) операторов T и $\perp$, т.е.

$$1 \circ 1 \Rightarrow \mathrm{T}\perp = \perp \mathrm{T}.$$

Полный набор операторов преобразования сведен в табл. 9.

Операторы преобразование матриц Таблица 9

	G	F	G^*	F^*
G	—	$\perp$	$\perp$T	T
F	$\perp$	—	T	$\perp$T
G^*	$\perp$T	T	—	$\perp$
F^*	T	$\perp$T	$\perp$	—

В соответствии с табл. 9, если две матрицы принадлежат различным (G - и F -) группам (определение групп приводится ниже в тексте), причем одна из матриц является сопряженной, то они связаны оператором классического транспонирования Т. Покажем это на примере матриц G и F^*. В самом деле, осуществим сначала с помощью оператора сопряжения $\perp$Т преобразование матрицы G в матрицу G^*, которую на следующем шаге оператором правостороннего транспонирования $\perp$ преобразуем в матрицу F^*. Последовательность (произведение) операторов $\perp$Т и $\perp$ эквивалентна оператору левостороннего транспонирования Т, т.е.

$$G \overset{\mathrm{T}}{\longleftrightarrow} F^*, \quad \text{а так же} \quad G^* \overset{\mathrm{T}}{\longleftrightarrow} F,$$

что и необходимо было подтвердить.

Анализируя структурные схемы простых ЛРС частных генераторов ПСП над ПрП $f_8 = 101001101$, приведенных на рис. 1-4, можем выйти на общие правила (операторы, сведенные в табл. 10) преобразования схем линейных обратных связей известного генератора ПСП над заданным ПрП f_n к схемам обратных связей любого их оставшихся трех видов генераторов.

Операторы преобразования обратных связей Таблица 10

	G	F	G^*	F^*
G	—	$1\circ 1$	$\circ 1$	$1\circ$
F	$1\circ 1$	—	$1\circ$	$\circ 1$
G^*	$\circ 1$	$1\circ$	—	$1\circ 1$
F^*	$1\circ$	$\circ 1$	$1\circ 1$	—

В отличие от табл. 9, в которой символами G, F, G^* и F^* обозначены примитивные матрицы генераторов ПСП, в табл. 10 этими же символами условно обозначены схемы обратных связей в соответствующих генераторах.

Смысл термина «схемы обратных связей» G, F, G^* или F^* ЛРС генераторов ПСП (на примере генераторов, структурные схемы которых представлены на рис. 1-4) можно пояснить, обратившись к их стилизованному отображению, показанному на рис. 5.

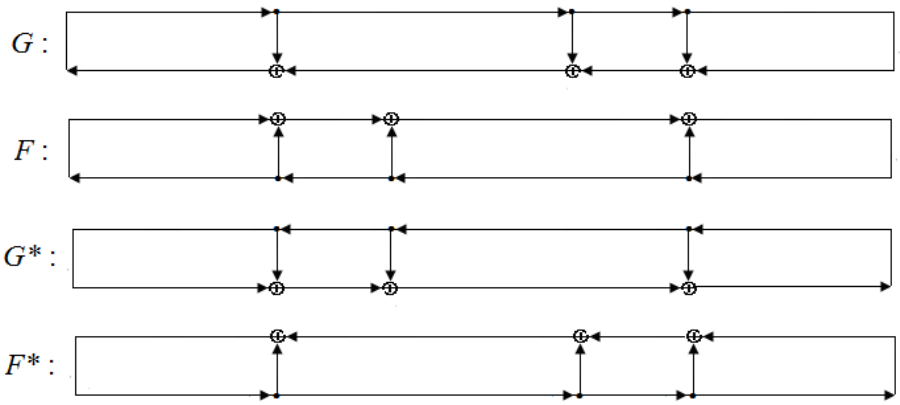

Рис. 5. Стилизованное представление обратных связей в ЛРС генераторах ПСП над $f_8 = 101001101$

Обратим внимание на такие особенности связей, представленных на рис. 5, в рассматриваемых генераторах ПСП. Обратные связи в базовых генераторах G и F

осуществляется по направлению часовой стрелки, тогда как в сопряженных генераторах G^* и F^* - против часовой стрелки.

Уточним физический смысл операторов преобразования в табл. 9. Оператор $\circ 1$ означает, что схема обратных связей, обозначенная символом $\circ$, претерпевает *вращение* на 180° относительно вертикальной оси. Такие преобразования происходят, как это следует из рис. 5, в парах генераторов (G, G^*) или (F, F^*). Операция $\circ 1$ подобна операции инверсной перестановки столбцов матрицы M, которая реализуется, если умножить ее справа на матрицу инверсной перестановки 1. Оператором $1\circ$ осуществляется вращение схемы обратных связей относительно горизонтальной оси. Таким образом, операция $1\circ$ подобна операции инверсной перестановки строк матрицы M, если умножить ее слева на матрицу инверсной перестановки. Указанные преобразования обратных связей имеют место в парах генераторов (G, F^*) или (F, G^*). И, наконец, оператор $1\circ 1$ означает, что схема обратных связей претерпевает вращение на 180° относительно как вертикальной, так и горизонтальной осей. Такие преобразования схем обратных связей выполняются в парах генераторов (G, F) или (G^*, F^*).

Обобщенные примитивные матрицы над *GF(2)*. В данном параграфе предлагаются алгоритмы построения примитивных матриц, в качестве образующих элементов которых применяются примитивные элементы $\omega > p = 2 = 10$ поля $GF(2^n)$ над произвольными неприводимыми двоичными полиномами f_n (совсем не обязательно примитивными) степени n. Пусть, как и в предыдущем параграфе, $n = 8$ и $f_8 = 101001101$. Примитивные элементы в 16-ричной системе счисления соответствующего поля Галуа сведены в табл. 11. Номер примитивного элемента ω поля $GF(2^8)$ над ПрП $f_8 = 101001101$ образуется конкатенацией цифр, стоящих в прямоугольных скобках левого столбца табл. 10 и цифры, расположенной в верхней строке таблицы.

Примитивные элементы поля $GF(2^8)$ над ПрП $f_8 = 101001101$ Таблица 11

Таблица ОЭ формирующих МГМП (НП = 101001101)

Hex	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	---	2	3	4	5	7	9	A	D	10
[1]	11	12	13	15	16	18	1A	1F	27	28
[2]	29	2A	2B	2C	2D	2E	2F	38	39	3C
[3]	3D	3E	41	42	44	48	49	4B	4C	4D
[4]	4E	4F	51	52	53	56	59	5C	5E	60
[5]	63	64	65	66	67	6A	6C	6E	6F	74
[6]	75	76	7F	80	84	85	86	87	89	8C
[7]	8D	8E	93	94	96	97	9E	A3	A5	A6
[8]	A7	A8	AA	AB	AD	AE	AF	B0	B4	B7
[9]	B9	BA	BB	BE	C0	C1	C2	C4	C5	C8
[10]	CB	CF	D0	D2	D5	D7	DA	DE	E0	E1
[11]	E2	E3	E5	E8	E9	EA	EB	EC	EE	EF
[12]	F0	F2	F3	F6	F8	F9	FC	FD	FF	

Выберем из табл. 11 образующий элемент $\omega = 2D = 101101$. Воспользовавшись обобщенным правилом диагонального заполнения (пояснения даны ниже), приходим к примитивной матрицы Галуа, показанной соотношением (21). Суть обобщенного правила

диагонального заполнения примитивной матрицы Галуа G заключается в следующем. Сначала ОЭ ω, являющийся примитивным элементом поля $GF(2^n)$ над выбранным НП f_n, следует записать в нижней (первой) строке матрицы G.

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \qquad (21)$$

Элементы этой строки, расположенные левее ω, заполняются нулями. Последующие строки матрицы G (по направлению снизу вверх) образуются циклическим сдвигом справа налево предыдущих строк матрицы. Если при этом левый элемент сдвигаемой строки равен 1, то выполняется обычный сдвиг строки на один разряд влево, а в правый освободившийся элемент строки записывается 0. Разрядность подобных строк становится на единицу больше порядка матрицы. Векторы, отвечающие таким строкам, приводятся к остатку по модулю НП f_n. Тем самым данные векторы также становятся $n-$битными.

Обобщенной матрице Галуа G соответствует *обобщенная матрица Фибоначчи* F, образуемая оператором правостороннего транспонирования $\perp$ (табл. 9) матрицы (21), т.е.

$$F = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}. \qquad (22)$$

Оператором $1 \circ 1$ (то же самое, что и оператором $\perp$ Т) матрицы (21) и (22) преобразуются в обобщенные сопряженные матрицы G^* и F^*, представленные соотношениями (23).

$$G^* = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}; \quad F^* = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \qquad (23)$$

Пусть $s_k(t),\ k = \overline{1,n},\ t = 0,1,\ldots -$состояние $k-$го разряда ($D-$триггера) ЛРС с обобщенными линейными обратными связями в дискретный момент времени t, причем $s_1(0) = 1,\ s_k(t) = 0,\ k = \overline{2,n}$. Кроме того, обозначим $h_{i,j}$ элемент $i-$й строки и $j-$го столбца, $i, j = \overline{1,n}$, любой из матриц G, F, G^* или F^*, лежащей в основе построения ЛРС с обобщенными линейными связями. Напомним, что строки матриц нумеруются снизу вверх, а столбцы – справа налево, начиная с номера 1. Состояние $k-$го разряда ЛРС $s_k(t+1)$ в

момент времени $t+1$ совпадает с функцией возбуждения этого разряда $\nu_k(t)$ в момент времени t и определяется соотношением:

$$s_k(t+1) = \nu_k(t) = \bigoplus_{i=1}^{n} h_{i,k} \cdot s_i(t). \qquad (24)$$

В соответствии с выражением (24) составим структурные схемы ЛРС для таких параметров регистров с обобщенными линейными связями: $n=4$; НП $f_4 = 11111$ и ОЭ $\omega_1 = 111$.

Обобщенная структурная схема базового четырехразрядного ЛРС Галуа, совпадающая с обобщенной схемой базового генератора Фибоначчи, показана на рис. 6. Вертикально расположенные регистры генераторов, отмеченные сверху символом $\otimes$, реализуют операцию поразрядного умножения, а регистры, отмеченные символом $\oplus$ – операцию сложения содержимого регистра по модулю 2.

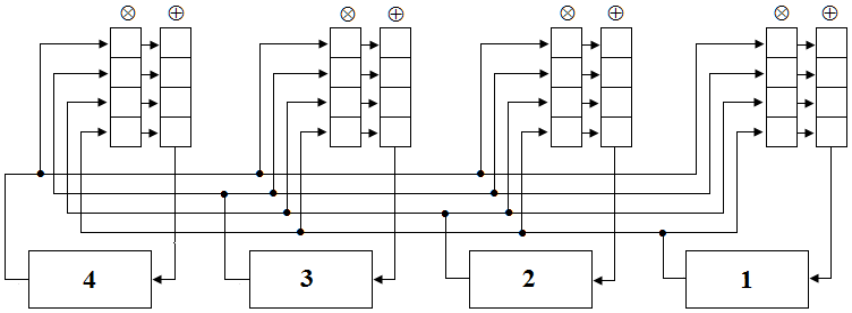

Рис. 6. Обобщенная структурная схема базовых генераторов Галуа/Фибоначчи

Если в регистрах умножения разместить элементы столбцов матрицы $G1$, то получим генератор ПСП по схеме Галуа. В том случае, когда в тех же регистрах будут расставлены элементы матрицы $F1$, то образуется генератор ПСП конфигурации Фибоначчи.

Схема сопряженных генераторов Галуа и Фибоначчи показана на рис. 7.

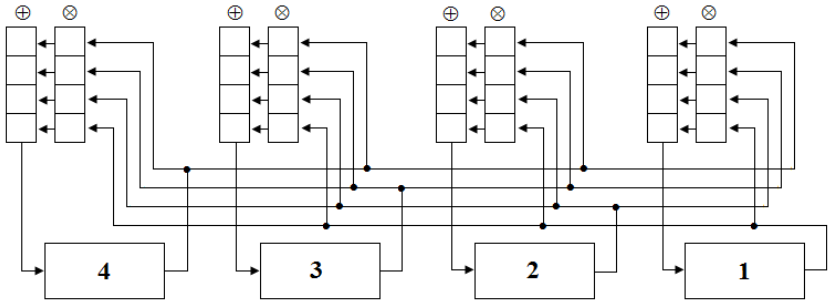

Рис. 7. Обобщенная структурная схема сопряженных генераторов Галуа/Фибоначчи

Примитивные матрицы, отвечающие выбранным параметрам генераторов, имеют вид:

$$G1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}; \quad F1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix};$$

$$G1^* = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}; \quad F1^* = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \qquad (25)$$

На основании матриц (25) по формуле

$$S_{k+1} = S_k \cdot M\ ,\ \ k = \overline{0,14}\ , \tag{26}$$

где M – одна из матриц $\left\{G1, G1^*, F1, F1^*\right\}$, вычислим состояния регистров генераторов ПСП. Результаты вычислений сведены в табл. 12.

Состояния четырехразрядных обобщенных генераторов ПСП Таблица 12

Номер состояния	Генераторы ПСП			
	$G1$	$F1$	$G1^*$	$F1^*$
0	0001	0001	0001	0001
1	0111	0100	0110	0101
2	1010	1111	1011	1110
3	1000	1100	0100	0110
4	0110	0101	0111	0100
5	1101	1011	1101	1011
6	0010	0011	1111	1000
7	1110	1001	0011	0010
8	1011	1110	1010	1111
9	1111	1000	0010	0011
10	1100	1010	1100	1010
11	0101	0111	1001	1101
12	0100	0110	1000	1100
13	0011	0010	1110	1001
14	1001	1101	0101	0111
15	0001	0001	0001	0001

Легко убедиться в том, что расчеты по формуле (26) совпадают с оценками состояний генераторов, которые можно получить непосредственно по структурным схемам базовых и сопряженных обобщенных генераторов ПСП, представленных на рис. 6 и 7 соответственно.

Обратим внимание на такие особенности структурных схем обобщенных генераторов. Обратные связи в базовых генераторах Галуа и Фибоначчи (рис. 6) «закручены» по часовой стрелке, тогда как в сопряженных генераторах (рис. 7) – против часовой стрелки, т.е. точно так же, как в простых генераторах ПСП, обратные связи которых отображены на рис. 5.

Обобщенные примитивные матрицы, принадлежащие одной и той же (Галуа или Фибоначчи) группе, обладают замечательным свойством *коммутативности*, суть которого можно пояснить следующим образом. Пусть $\omega_2 = 1011$ – второй примитивный элемент поля $G(2^4)$, отличный от ОЭ $\omega_1 = 111$. Образующему элементу ω_2 отвечает такая совокупность примитивных матриц:

$$G2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}; \qquad F2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix};$$

$$G2^* = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}; \qquad F2^* = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}. \tag{27}$$

В табл. 13 сведены признаки коммутативности всевозможных пар примитивных пар матриц, входящих в системы (25) и (27).

Признаки коммутативности примитивных матриц Таблица 13

	$G1$	$F1$	$G1^*$	$F1^*$	$G2$	$F2$	$G2^*$	$F2^*$
$G1$		–	+	–	+	–	+	–
$F1$	–		–	+	–	+	–	+
$G1^*$	+	–		–	+	–	+	–
$F1^*$	–	+	–		–	+	–	+
$G2$	+	–	+	–		–	+	–
$F2$	–	+	–	+	–		–	+
$G2^*$	+	–	+	–	+	–		–
$F2^*$	–	+	–	+	–	+	–	

Коммутативные пары матриц отмечены знаком +. Как следует из табл. 12 коммутативными являются любые пары матриц, принадлежащих одной из двух групп однородных примитивных матриц. Первую группу матриц составляют матрицы Галуа ($G-$группа), в которую входят примитивные матрицы $G=\left\{G1, G2, G1^*, G2^*\right\}$. Во вторую ($F-$группу) входят примитивные матрицы Фибоначчи $F=\left\{F1, F2, F1^*, F2^*\right\}$. Таким образом, например, матрица $G1$ коммутативна с любой из трех матриц $G2$, $G1^*$ или $G2^*$, но не коммутативна ни с одной из примитивных матриц, входящих в $F-$группу.

Отметим, кроме того, такое интересное свойство примитивных базовых матриц Галуа G над НП f и ОЭ $\omega \geq 2$. Структура степеней $G-$матриц, т.е. матриц G^k, такая же, как и структура базовой матрицы G, т.е. подчинена принципу диагонального заполнения строк матриц. А из этого следует, что для того, чтобы вычислить матрицу G^k, достаточно возвести в $k-$ю степень образующий элемент ω, привести к остатку по модулю f значение ω^k и далее воспользоваться правилом диагонального заполнения матриц, используя в качестве образующего элемент $\omega_k = (\omega^k) \bmod f$.

Синтез примитивных матриц над *GF(p), p > 2*. Примитивные матрицы над $GF(p)$, $p>2$, обладают теми же свойствами и синтезируются по тем же правилам (диагонального заполнения), что и матрицы над $GF(2)$. Выберем, для примера, $p=3$ и неприводимый над $GF(3)$ унитарный полином четвертой степени $f_4 = 12101$. Примитивные элементы ω поля $GF(3^4)$ над НП f_4 сведены в табл. 14.

Примитивные элементы поля $GF(3^4)$ над НП $f_4 = 12101$ Таблица 14

j	i							
	1	2	3	4	5	6	7	8
0	101	102	120	122	201	202	210	211
8	1010	1012	1021	1022	1102	1111	1112	1122
16	1200	1211	1220	1222	2011	2012	2020	2021
24	2100	2110	2111	2122	2201	2211	2221	2222

Номер $(i, j)-$го примитивного элемента табл. 14 определяется суммой номера столбца i и значения строки j.

Пусть $\omega = 1102$. Базовые G, F и сопряженные G^*, F^* обобщенные матрицы Галуа и Фибоначчи, соответствующие выбранным параметрам n, ω и f, имеют вид:

$$G = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 0 & 2 \end{pmatrix}; \qquad F = \begin{pmatrix} 2 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 1 & 2 & 1 & 1 \end{pmatrix}; \tag{28}$$

$$G^* = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix}; \qquad F^* = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 2 & 0 \\ 2 & 1 & 2 & 2 \end{pmatrix}.$$

Структурные схемы обобщенных ЛРС инвариантны к характеристике поля p. В частности, структурная схема четырехразрядного Галуа ЛРС, обратные связи в котором заданы матрицей G системы (27), показана на рис. 8, причем $\oplus$ есть оператор сложения по модулю $p = 3$.

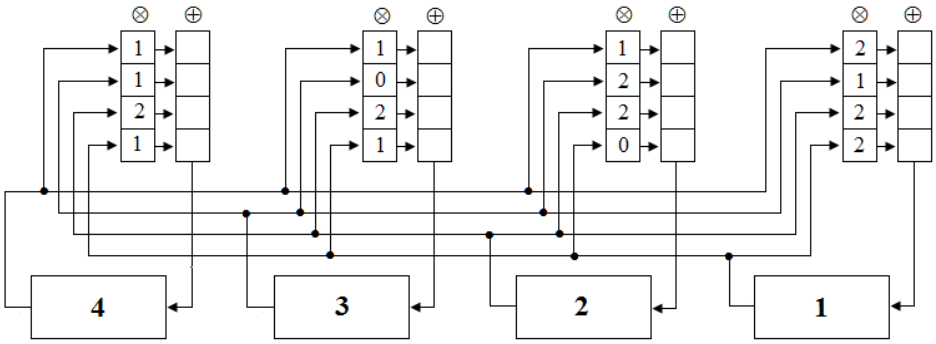

Рис. 8. Структурная схема обобщенного ЛРС Галуа

Воспользовавшись соотношением (26) и полагая $M = G$, вычислим множество состояний регистра в моменты времени $t = j \| i$ (табл. 14). Непосредственной проверкой легко убедиться в том, что последовательность состояний регистра, показанного на рис. 8, совпадает с последовательностью состояний, записанных в табл. 15.

Полная группа ненулевых состояний обобщенного ЛРС Галуа Таблица 15.

j	i									
	0	1	2	3	4	5	6	7	8	9
0	0001	1102	1001	2211	1221	2001	0020	1111	2121	2122
1	0221	1222	0100	1021	0022	0012	1120	0211	2000	2221
2	0110	0210	1201	1220	1202	2022	2200	1200	0121	0201
3	0111	1012	2202	0101	2120	1020	2220	2011	2212	2020
4	0002	2201	2002	1122	2112	1002	0010	2222	1212	1211
5	0112	2111	0200	2012	0011	0021	2210	0122	1000	1112
6	0220	0120	2102	2110	2101	1011	1100	2100	0212	0102
7	0222	2021	1101	0202	1210	2010	1110	1022	1121	1010

Структурная схема четырехразрядного сопряженного ЛРС Фибоначчи, обратные связи в котором заданы матрицей F^* системы (28), показана на рис. 9.

Из сопоставления рис. 6,7 и 8,9 следует, что структурные схемы базовых и сопряженных генераторов совпадают, т.е. инвариантны к оператору сопряжения.

Последовательность ненулевых состояний регистра (табл. 16), представленного на рис. 9, совпадает с последовательностью состояний, определяемых по формуле (26) для $M = F^*$ системы (28).

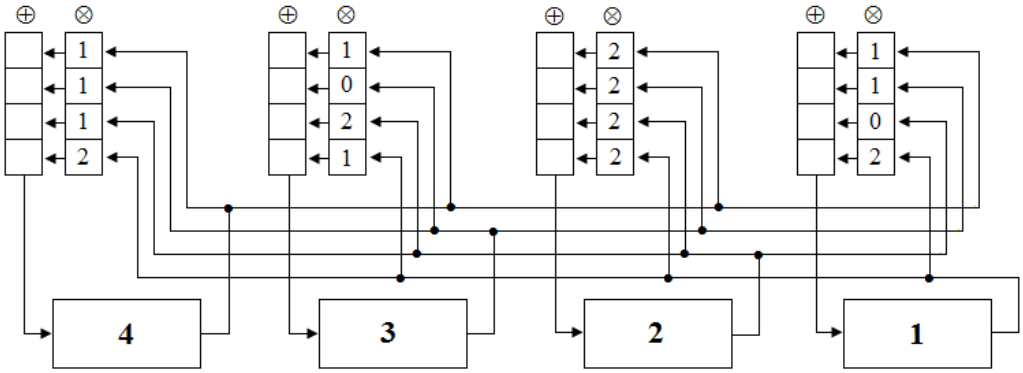

Рис. 9. Структурная схема обобщенного сопряженного ЛРС Фибоначчи

Полная группа ненулевых состояний обобщенного сопряженного ЛРС Фибоначчи. Таблица 16

j	i									
	0	1	2	3	4	5	6	7	8	9
0	0001	2122	0221	0211	2021	0111	1000	1121	0011	0012
1	2101	2022	2200	1221	1002	2002	0120	0101	0110	2211
2	1200	0100	1021	2020	1022	1112	1210	1020	0201	1101
3	1201	2222	1212	2201	0010	1220	2210	2111	0212	1110
4	0002	1211	0112	0122	1012	0222	2000	2212	0022	0021
5	1202	1011	1100	2112	2001	1001	0210	0202	0220	1122
6	2100	0200	2012	1010	2011	2221	2120	2010	0102	2202
7	2102	1111	2121	1102	0020	2110	1120	1222	0121	2220

Табл. 15 и 16 подтверждают, по крайней мере, тот факт, что генераторы над $GF^*(3^4)$, показанные на рис. 8 и 9, формируют последовательности максимальной длины, равные 80, а матрицы, заданные системой (27), являются примитивными.

И в заключение параграфа обратим внимание на следующие факты. Во-первых, генераторы ПСП, синтезированные посредством обобщенных двоичных ЛРС, не привносят каких-либо новых качеств последовательностям, по сравнению с последовательностями, образуемыми генераторами, построенными по классическим схемам Галуа или Фибоначчи. Постулаты Голомба [8] выполняются для обобщенных генераторов в такой же мере, как и для обычных двоичных генераторов ПСП. Во-вторых, если хотя бы одна из обобщенных G или F матриц над выбранным НП не примитивна (а это может произойти только в случае, если в качестве образующего элемента матрицы выбран элемент поля Галуа, не являющийся примитивным), то свойство примитивности и коммутативности матриц утрачивается. И, наконец, в-третьих, согласно соотношениям (15) сопряженные матрицы Галуа и Фибоначчи являются матрицами, образуемыми преобразованием подобия исходных (базовых) матриц G и F. В качестве матриц преобразования подобия P выступают матрицы инверсной перестановки 1. Как известно, подобные матрицы сохраняют все свойства исходных матриц. В силу указанной особенности, если матрицы G и F (простые или обобщенные) примитивны, то и соответствующие им сопряженные матрицы G^* и F^* также оказываются примитивными.

Прикладные аспекты. Далее обсуждается возможность применения двоичных обобщенных примитивных матриц Галуа и Фибоначчи для построения матричного аналога [9] – [12] протокола Диффи-Хеллмана ($DH-$протокола), предназначенного для передачи секретных ключей шифрования по открытым каналам связи [13].

В $DH-$ алгоритме предполагается, что абонентам компьютерной сети (Алисе и Бобу) известны открытые ключи p и q, причем p есть большое простое число, а $q-$ образующий элемент мультипликативной группы кольца вычетов по модулю p такой, что $1 <<< q < p$. Абонент Алиса генерирует случайное большое число $a < p$, вычисляет значение $A = q^a \bmod p$ и пересылает его Бобу. В свою очередь Боб генерирует случайное большое число $b < p$, вычисляет значение $B = q^b \bmod p$ и пересылает его Алисе. Далее, абонент Алиса возводит полученное от Боба число B в свою случайную степень a и вычисляет значение $K_a = B^a \bmod p = q^{ba} \bmod p$. Аналогично поступает Боб, вычисляя $K_b = A^b \bmod p = q^{ab} \bmod p$. Очевидно, что оба абонента получают одно и то же число K, поскольку $K_a \equiv K_b$. Это число K Алиса и Боб могут использовать в качестве секретного ключа, например, для симметричного шифрования, поскольку противник, перехвативший числа A и B, не сможет воспроизвести ключ K, так как встретится с практически неразрешимой (за разумное время) проблемой вычисления K, если только числа p, a и b были выбраны достаточно большими.

Процедура формирования ключа шифрования K в предлагаемом матричном аналоге $DH-$ протокола основывается на использовании двух открытых и по одному закрытому ключу у обоих абонентов сети. В качестве открытых ключей выбирают какой-либо двоичный вектор инициализации V $n-$ го порядка и произвольный неприводимый полином f_n степени n. Закрытыми ключами являются примитивные элементы ω поля Галуа $GF(2^n)$ над НП f_n, на основе которых абоненты Алиса и Боб формируют примитивные секретные матрицы преобразований $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$ соответственно.

Суть предлагаемого алгоритма обмена ключами шифрования по открытым каналам связи состоит в следующем. Абонент Алиса выбирает секретный примитивный ОЭ ω_a поля $GF(2^n)$ над НП f_n, формирует матрицу Галуа $G_{f_n}^{(\omega_a)}$, вычисляет вектор $V_a = V \cdot G_{f_n}^{(\omega_a)}$ и посылает его Бобу. В свою очередь Боб выбирает примитивный ОЭ ω_b, формирует матрицу $G_{f_n}^{(\omega_b)}$, вычисляет вектор $V_b = V \cdot G_{f_n}^{(\omega_b)}$ и посылает его Алисе. После этого оба абонента умножают векторы, полученные от партнера, на свои секретные матрицы Галуа. Тем самым будет образован общий секретный ключ K в силу того, что произведение примитивных матриц Галуа над одним и тем же НП f_n коммутативно, а из этого следует

$$K_a = V_b \cdot G_{f_n}^{(\omega_a)} = V \cdot G_{f_n}^{(\omega_b)} \cdot G_{f_n}^{(\omega_a)} \equiv K_b = V_a \cdot G_{f_n}^{(\omega_b)} = V \cdot G_{f_n}^{(\omega_a)} \cdot G_{f_n}^{(\omega_b)}.$$

Вместо базовых (как и сопряженных) матриц Галуа с равным успехом в матричном аналоге $DH-$ протокола могут быть использованы обобщенные двоичные матрицы Фибоначчи, обладающие теми же свойствами, что и матрицы Галуа.

Заключение. Основным результатом статьи является разработка алгоритмов синтеза обобщенных базовых и сопряженных матриц Галуа и Фибоначчи, элементы которых принадлежат простому полю $GF(p)$ характеристики $p \geq 2$. Данные матрицы обладают замечательными свойствами, такими как примитивность и коммутативность, что дало возможность построить на их основе обобщенные линейные регистры максимального периода, а также предложить матричный аналог протокола Диффи-Хеллмана. Структурные схемы обобщенных ЛРС оказались однородными и инвариантными как к порядкам регистров n, так и характеристикам p поля $GF(p^n)$.

Вместе с тем следует отметить, что обобщенные РСЛОС не привносят каких-либо новых свойств в двоичные последовательности, формируемые генераторами ПСП, синтезированными на основе данных РСЛОС. Для таких генераторов постулаты Голомба соблюдаются в такой же форме, как и для классических генераторов ПСП.

ЛИТЕРАТУРА

1. Поточные шифры. Результаты зарубежной открытой криптологии. – М., 1997. Эл. ресурс: http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm

2. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / Иванов М.А., Чугунков И.В. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

3. Нечаев В. И. Элементы криптографии (Основы теории защиты информации) / Нечаев В. И. – М.: Высш. шк., 1999. 109 с.

4. Волкович С. Л. Вступ до алгебраїчної теорії перешкодостійкого кодування / Волкович С. Л., Геранін В. О., Мовчан Т. В., Пісаренко Л. Д. – Київ, ВПФ УкрІНТЕІ, 2002. – 236 с.

5. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. / Иванов М. А. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

6. Лидл Р. Конечные поля / Лидл Р., Нидеррайтер Г. – Т. 1. – М.: Мир, 1988. – 432 с.

7. Фробениусова нормальная форма – Эл. ресурс: Википедия

8. Постулаты Голомба – Эл. ресурс: Википедия

9. Мегрелишвили Р.П. Однонаправленная матричная функция – быстродействующий аналог протокола Диффи-Хэллмана / Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М. – Збірник матеріалів 7-й МК «Інтернет-Освіта-Наука-2010». – Вінниця: ВНТУ, 2010. – С. 341-344.

10. Белецкий А.Я. Однонаправленная матричная функция / Белецкий А.Я., Мегрелишвили Р.П. – Праці Міжнародної молодіжної математичної школи «Питання оптимізації обчислень» (ПОО-XXXVII), смт. Куцівелі, Крим, 2011. – С. 21-22.

11. Білецький А.Я. Матричні аналоги протоколу Діффі-Хеллмана / Білецький А.Я., Білецький Є.А., Кандиба Р.Ю. – Матеріали І-ої МНТК «Захист інформації і безпека інформаційних систем». – Львів, Нац. ун-т «Львівська політехніка», 2012. – С. 68-69.

12. Белецкий А.Я. Синтез примитивных матриц над конечними полями Галуа и их приложения / Белецкий А.Я., Белецкий Е.А. – Материалы Международной научной конференции «Компьютерная алгебра и информационные технологи». – Одесса, Одесский национальный университет им. И.И. Мечникова, 2012. – С. 3-6.

13. Diffe W. New Directions in Cryptography / Diffe W., Hellman V.E. // IEEE Transact. On Information Theory, v. IT-22, no. 6, Nov, 1976, p. 644-654.

Надійшла: 12.09.2012

Рецензент: д.т.н., проф. Шелест М.Є.