УДК 511.512

ПРИМИТИВНЫЕ МАТРИЦЫ ГАЛУА В КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Анатолий Белецкий

В статье рассмотрены вопросы формирования обобщенных примитивных матриц Галуа произвольного порядка n, элементы которых принадлежат простому полю $GF(2)$. Синтез матриц базируется на использовании неприводимых полиномов f_n степени n и примитивных элементов расширенного поля $GF(2^n)$, порождаемого полиномами f_n. Предложены способы построения сопряженных примитивных матриц Галуа и однозначно связанных с ними правосторонним транспонированием матриц Фибоначчи. Обсуждаются способы применения таких матриц в криптографических приложениях для решения задачи построения обобщенных линейных генераторов псевдослучайных последовательностей Галуа максимального периода. Проведен анализ псевдослучайных бинарных последовательностей, формируемых линейными генераторами Галуа, в обратных связях регистров которых используются примитивные полиномы малой степени в диапазоне от четырех до шести.

Ключевые слова: *неприводимые и примитивные полиномы, примитивные матрицы, линейные регистры сдвига, генераторы псевдослучайных последовательностей Галуа.*

Введение и постановка задачи. В теории и практике криптографической защиты информации одной из ключевых проблем является проблема формирования двоичных псевдослучайных последовательностей (ПСП) максимальной длины ($m-$последовательностей) с приемлемыми статистическими характеристиками. Генераторы ПСП реализуют, как правило, посредством линейных регистров сдвига (ЛРС) с линейными обратными связями [1]. Только ЛРС с особо подобранными функциями обратных связей могут проходить через все ненулевые внутренние состояния – это так называемые *регистры максимального периода*. Для того чтобы ЛРС был регистром максимального периода, соответствующий полином обратной связи должен быть *примитивным полиномом* [2].

В статье расширяется понятие ЛРС и показано, что в качестве полиномов обратной связи могут быть использованы произвольные *неприводимые полиномы* (НП) f_n степени n, совсем не обязательно примитивные.

Основная задача, которая ставится в данной статье, состоит в разработке алгоритмов построения *обобщенных примитивных матриц Галуа и Фибоначчи* $n-$го порядка над полем $GF(2)$, а также их *сопряженных* эквивалентов. Синтезируемые примитивные матрицы однозначно определяют как структуру соответствующих обобщенных $n-$разрядных линейных регистров сдвига с линейными обратными связями (ЛРСЛОС) максимального периода, так и формируемых ими (регистрами) псевдослучайных бинарных последовательностей максимальной длины.

I. Понятийно-терминологические определения. Термины «матрица Галуа» и связанная с ней оператором правостороннего транспонирования «матрица Фибоначчи» заимствованы из теории криптографии и кодирования [3], в которых широко используются генераторы двоичных ПСП по схемам Галуа и Фибоначчи, основанные на ЛРСЛОС. Будем называть такие генераторы ПСП *линейными генераторами* Галуа и Фибоначчи соответственно. Каждому генератору ставится в соответствие однозначно с ними связанные матрицы Галуа и Фибоначчи, посредством которых можно вычислить те же самые последовательности, что и последовательности, формируемые линейными генераторами ПСП. В данном разделе работы 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 $GF(p^n)$ характеристики p. В свою очередь, примитивным является такой элемент α поля, который порождает мультипликативную группу $\langle\alpha\rangle$ максимального порядка (периода). Это означает, что последовательность степеней примитивного элемента α, начиная с нулевой степени, в кольце вычетов по модулю f_n содержит все ненулевые элементы поля расширенного поля Галуа.

В криптографических источниках, например [5], понятие ПрП вводится следующим образом. Примитивным является такой неприводимый полином (многочлен) $f_n(x)$ с коэффициентами $\alpha_n = 1,\ \alpha_k \in GF(p),\ k = \overline{0, n-1}$, который делит без остатка двучлен $x^e - 1$, при условии, что минимальное натуральное e определяется выражением

$$\min e = p^n - 1. \qquad (1)$$

И, наконец, в классической теории конечных полей, например [6], понятие примитивного многочлена определяется так: многочлен f_n степени n является примитивным многочленом над $GF(p)$ в том и только в том случае, если он – *нормированный* (унитарный или приведенный) 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 поясним далее, уточняя физический смысл термина «примитивный полином».

Использованные ранее обозначения f_n и $f_n(x)$ соответствуют двум формам (векторной и алгебраической) представления НП. Например, бинарному вектору

$$f_8 = 100011011$$

соответствует алгебраическая форма двоичного неприводимого полинома

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

Согласно приведенным выше определениям, полином $f_n(x)$ 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, удовлетворяет соотношению (1).

Пусть $L = p^n - 1$ есть общее число ненулевых элементов поля $GF(p^n)$, а L^* – число примитивных элементов $\omega \in \Omega$ этого поля, определяемое формулой $L^* = \varphi(L)$, где φ – функция Эйлера. В табл. 1 приведены полные множества (Ω) примитивных элементов поля $GF(2^4)$, порождаемые всеми НП четвертой степени, при этом первые два полинома являются примитивными, тогда как третий – таковым не является.

Обратим внимание на то, что для ПрП 10011 и 11001 минимальным примитивным элементом соответствующих полей Галуа оказывается элемент 10, совпадающий с характеристикой поля $GF(2^4)$.

Таблица 1

Примитивные элементы поля $GF(2^4)$

f_4	Множество (Ω) примитивных элементов							
10011	10	11	100	101	1001	1011	1101	1110
11001	10	100	110	111	1001	1100	1101	1110
11111	11	101	110	111	1001	1010	1011	1110

В табл. 2 сведены все НП восьмой степени и минимальные примитивные элементы $\omega_{\min}$ расширенных полей Галуа $GF(2^8)$, порождаемых соответствующими неприводимыми полиномами.

Таблица 2

Неприводимые полиномы восьмой степени над $GF(2)$

Значение полинома	$\omega_{\min}$	Значение полинома	$\omega_{\min}$	Значение полинома	$\omega_{\min}$
100011011	11	101101001	10	110110001	110
100011101	10	101110001	10	110111101	111
100101011	10	101110111	11	111000011	10
100101101	10	101111011	1001	111001111	10
100111001	11	110000111	10	111010111	111
100111111	11	110001011	110	111011101	111
101001101	10	110001101	10	111100111	10
101011111	10	110011111	11	111110011	110
101100011	10	110100011	101	111110101	10
101100101	10	110101001	10	111111001	11

Для простоты и удобства введем для неприводимого полинома понятие, которое назовем *характеристикой p полинома* f_n, совпадающее с характеристикой p простого поля Галуа $GF(p)$, которому принадлежат коэффициенты u_i, $i \in \overline{0, n}$, полинома. Характеристика p неприводимого полинома, как и поля Галуа, должна быть простым числом.

Основание m произвольной системы счисления (ОСС) записывается в виде 10. Тогда для любого ОСС p и, следовательно, для любого расширенного поля Галуа $(k+1)$–я степень минимального примитивного элемента $\omega = 10$ поля, которую (степень) можно представить соотношением $\omega^{k+1} = \omega^k \cdot \omega$, образуется смещением значения ω^k на один разряд влево (как результат умножения на p – ичное число 10). Если при этом окажется, что старшая ненулевая цифра числа ω^{k+1} смещается в $(n+1)$–й разряд (первый разряд – крайний правый), то число ω^{k+1} приводится к остатку по модулю f_n.

Исходя из вышеизложенного, введем такое, эмпирически подтверждаемое данными табл. 1 и 2, определение ПрП.

Примитивным является неприводимый над $GF(p)$ полином f_n степени n (*необходимое усло-*

вие), порождающий расширенное поле Галуа $GF(p^n)$, минимальный примитивный элемент которого $\omega_{\min}$ совпадает с характеристикой поля p (*достаточное условие*) [7, 8].

Возможен другой вариант определения.

Примитивным над полем $GF(p)$ называется неприводимый полином f_n степени n, формирующий циклическую группу $\langle\omega\rangle$ максимального порядка p^n-1, причем минимальный образующий элемент (ОЭ) $\omega_{\min}$ группы совпадает с характеристикой поля p, т.е. $\langle\omega_{\min}\rangle=\langle p\rangle$. Такими определениями непосредственно раскрывается *физический смысл* термина «примитивный полином».

В качестве примера в табл. 3 приведены все унитарные НП четвертой степени f_4 над $GF(3)$ и соответствующие им минимальные примитивные элементы $\omega_{\min}$.

Таблица 3

Неприводимые полиномы четвертой степени над $GF(3)$

f_4	$\omega_{\min}$	f_4	$\omega_{\min}$	f_4	$\omega_{\min}$
10012	10	11002	10	12002	10
10022	10	11021	11	12011	11
10102	110	11101	101	12101	101
10111	11	11111	12	12112	10
10121	12	11122	10	12121	11
10202	11	11222	10	12212	10

Примитивными в табл. 3 являются те полиномы, для которых $\omega_{\min}=10$, что совпадает с известными (см., например, [9]) результатами.

Перейдем к пояснению термина «примитивная матрица» [10]. 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 считается *невырожденной* 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 d выполняется в кольце вычетов по модулю p, при этом каждый элемент матрицы A^d приводится к неотрицательному остатку по модулю p. Последовательность степеней матрицы A, начиная с нулевой степени, для которой $A^0=E$, образует *циклическую группу* $\langle A\rangle$ порядка e.

Матрицу A, $a_{i,j}\in GF(p)$, будем называть *примитивной*, если наименьшее натуральное e, при котором $A^e=E$, удовлетворяет соотношению (1). Суть термина «примитивная» матрица подобен, в определенной мере, термину «примитивный элемент» расширенного поля $GF(p^n)$.

II. Классические генераторы ПСП Галуа и Фибоначчи. Как уже было отмечено выше, для того чтобы ЛРС являлся регистром максимального периода, соответствующий полином обратной связи должен быть примитивным полиномом. На рис. 1 показана, в качестве примера, структурная схема генератора в конфигурации Галуа, линейные обратные связи которого образованы ПрП $f_8=101001101$.

Классический генератор Галуа, представленный на рис. 1, сопоставляет каждому ненулевому элементу поля $GF(2^8)$ соответствующую степень примитивного элемента $\omega=10$ по модулю примитивного полинома $f_8=101001101$.

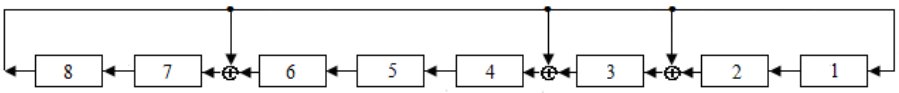

Рис. 1. Структурная схема генератора Галуа над ПрП $f_8=101001101$

Элемент $\oplus$ в ЛРС осуществляет операцию сложения по модулю 2 (операцию XOR). Как следует из структурной схемы генератора обратные связи в простых (классических) регистрах (генераторах) Галуа однозначно определяются выбранным примитивным полиномом 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_n, соответствует номер 1, как и младшему разряду ($D-$триггеру) регистра.

Обозначим через G матрицу, с помощью которой введем рекуррентное вычисление состояний $S(t)$ регистра Галуа в момент времени t по формуле:

$$S(t)=S(t-1)\cdot G,\ S(0)=00000001,\ t=1,2,\cdots.$$

Вектором $S(0)$ выделяется нижняя строка (припишем ей номер 1) матрицы G. Следовательно, в нижней строке матрицы G необходимо записать значение $S(1)$, совпадающее с минимальным ОЭ $\omega_{\min}=10$ поля $GF(2^8)$ над ПрП $f_8=101001101$. Продолжая подобным образом операции преобразований, приходим к окончательному выражению для матрицы

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

В соответствии с (2) алгоритм синтеза матриц Галуа G может быть сформулирован следующим образом. Пусть f_n- векторная форма ПрП степени n такая, что $f_n=\{1,u_{n-1},u_{n-2},\dots\ \dots,u_2,u_1,1\}$, $u_i\in\{0,1\}$, $i=\overline{1,n-1}$, и $\omega=10-$ минимальный образующий элемент ω поля $GF(2^n)$. Поместим образующий полином ω справа нижней строки матрицы G и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы G, кроме элементов верхней строки, запишем нули. В верхней строке матрицы G следует ожидать появления $(n+1)-$битного вектора 100…0. Но это недопустимо, так как порядок матрицы равен n. Приведя этот $(n+1)-$битный вектор к остатку по модулю f_n, приходим к тому, что в верхней строке матрицы G следует поместить примитивный полином f_n, исключая его старшую единицу, т.е. $n-$битный вектор $u_{n-1},u_{n-1},\cdots\ \cdots u_2,u_1,1$.

На основании предложенного правила, назовем его *правилом диагонального заполнения*, получим общую форму матрицы Галуа $n-$го порядка:

$$G=\begin{pmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \qquad (3)$$

Из сопоставления матрицы (3) и соответствующей ей структурной схемы линейного генератора (рис. 1) легко приходим к значениям функций возбуждения $\nu_k(t)$ триггеров классических генераторов ПСП в конфигурации Галуа в любой момент времени t.

Пусть $s_k(t)$ есть состояние $k-$го разряда ($D-$триггера) регистра Галуа. Состояние регистра $S(t)=\{s_n(t),s_{n-1}(t),s_2(t),s_1(t)\}$ в начальный момент времени $t=0$ таково: $S(0)=\{0,0,\cdots,0,1\}$. Тогда для каждого момента времени $t\ge 1$ функции возбуждения $\nu_k(t)$ $k-$го разряда регистра будут определяться выражениями

$$\nu_1(t)=s_n(t-1);\ \nu_k(t)=s_{k-1}(t-1)\oplus u_k\cdot s_n(t-1),$$

$$k=\overline{2,n},\quad t=1,2,\cdots.$$

В дополнении к матрицам Галуа можно ввести также *матрицы Фибоначчи* F над примитивными полиномами f_n, отвечающие линейным регистрам сдвига по схеме Фибоначчи (линейным генераторам псевдослучайных последовательностей Фибоначчи). Матрицы Фибоначчи F взаимно-однозначно связаны с матрицами Галуа G *оператором правостороннего транспонирования* $\perp$ (транспонирования относительно вспомогательной диагонали [11]), т.е.

$$F\xleftrightarrow{\perp}G. \qquad (4)$$

К общей форме матрицы Фибоначчи $n-$го порядка, представленной соотношением (5), можно прийти в результате правостороннего транспонирования матрицы (3). Структурная схема генератора ПСП в конфигурации Фибоначчи, соответствующая матрице (5) для ПрП $f_8=101001101$, приведена на рис. 2.

$$F=\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{pmatrix}. \qquad (5)$$

III. Сопряженные генераторы Галуа и Фибоначчи. В теории групп элемент x^* некоторой группы X является *сопряженным* элементу x той же группы, если существует некоторый элемент $z\in X$ такой, что

$$x^*=z^{-1}\cdot x\cdot z. \qquad (6)$$

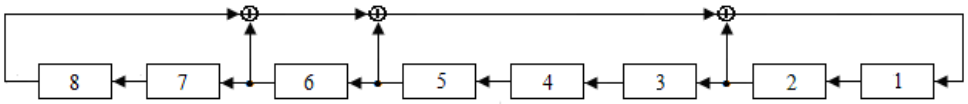

Рис. 2. Структурная схема генератора Фибоначчи над ПрП $f_8 = 101001101$

Говорят также, что x^* получается на x *трансформированием* при помощи элемента z [12].

По аналогии с (6) введем формальное определение *сопряженных матриц* Галуа и Фибоначчи по форме

$$M^* = P^{-1} \cdot M \cdot P, \qquad (7)$$

где M есть одна из матриц G или F, а P – невырожденная матрица, того же порядка, что и матрица M, которая носит название *матрицы перехода* от M к M^*.

Как следует из соотношения (7), матрицы M^* являются матрицами, *подобными* M [13] и, в силу этого, сохраняющими основные свойства матриц M. Отметим, что матрицы G^* и F^* названы *сопряженными матрицам* G и F на основании формального сходства преобразований (6) и (7). В качестве матрицы P выбрана *матрица инверсной перестановки* (ИП), которую условно обозначим цифрой 1

$$1 := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \qquad (8)$$

Соотношением (8) определена, в качестве примера, матрица ИП четвертого порядка. Матрицы ИП являются *инволютивными*, т.е. обратными сами себе. Это означает, что $1 \cdot 1 = 1^2 = E$.

Таким образом,

$$\begin{aligned} G^* &= 1 \cdot G \cdot 1, \qquad G = 1 \cdot G^* \cdot 1; \\ F^* &= 1 \cdot F \cdot 1, \qquad F = 1 \cdot F^* \cdot 1. \end{aligned} \qquad (9)$$

Систему (9) можно компактно представить так

$$M^* \overset{1}{\longleftrightarrow} M, \quad M \in \{G, F\}. \qquad (10)$$

Умножение квадратной матрицы M на матрицу ИП слева эквивалентно инверсии строк матрицы M, а справа – инверсии столбцов этой матрицы. Следовательно, сопряженная матрица M^* образуется из матрицы M в результате совместной инверсии ее строк и столбцов, выполняемых в любой последовательности, т.е.

$$M^* = M^{T\perp} = M^{\perp T}.$$

Согласно взаимно-однозначному соответствию (10) любая из рассматриваемых матриц Галуа и Фибоначчи (базовая M или сопряженная M^*) может быть получена в результате *преобразования подобия* из другой матрицы. Общие формы классических сопряженных матриц n-го порядка, в соответствии с (3) и (5), имеют вид:

$$G^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & u_1 & u_1 & \cdots & u_{n-2} & u_{n-1} \end{pmatrix}; \qquad (11)$$

$$F^* = \begin{pmatrix} u_{n-1} & 1 & 0 & \cdots & 0 & 0 \\ u_{n-2} & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ u_2 & 0 & 0 & \cdots & 1 & 0 \\ u_1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \qquad (12)$$

Согласно значениям (11) и (12) для сопряженных матриц G^* и F^* над примитивным полиномом $f_8 = 101001101$ приходим к структурным схемам сопряженных восьмиразрядных генераторов псевдослучайных последовательностей Галуа и Фибоначчи, представленных на рис. 3 и 4 соответственно.

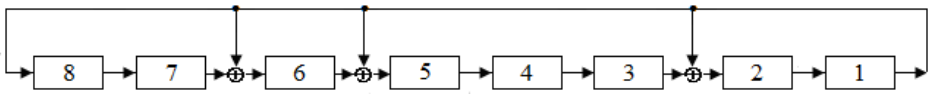

Рис. 3. Структурная схема сопряженного генератора Галуа над ПрП $f_8 = 101001101$

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

Функции возбуждения $D-$триггеров классических $n-$разрядных сопряженных генераторов ПСП Галуа и Фибоначчи (начальные состояния регистров для обоих генераторов одинаковы и таковы: $s_1(0)=1,\ s_k(0)=0,\ k=\overline{2,n}$, при том, что $n=8$) определяются выражениями

$$v_n(t)=s_1(t-1);\ v_k(t)=s_{k+1}(t-1)\oplus u_{n-k}\cdot s_1(t-1),\ k=\overline{1,n-1},$$

– для генератора Галуа и

$$v_k(t)=s_{k+1}(t-1),\ k=\overline{1,n-1};\ v_n(t)=s_1(t-1)\overset{n}{\underset{k=2}{\oplus}}u_{k-1}\cdot s_k(t-1),$$
$$t=1,2,...$$

– для генератора Фибоначчи соответственно.

IV. Обобщенные генераторы ПСП Галуа и Фибоначчи. В данном разделе статьи предлагается алгоритм построения примитивных матриц Галуа и других, связанных с ними матриц, в качестве образующих элементов которых применяются примитивные элементы $\omega>p=2=10$ поля $GF(2^n)$ над произвольными неприводимыми полиномами f_n (совсем не обязательно примитивными) степени n.

Для решения задачи синтеза примитивных матриц воспользуемся *обобщенным правилом диагонального заполнения*, суть которого состоит в следующем. Первоначально в нижней строке матрицы G записывается ОЭ ω, являющийся примитивным элементом поля $GF(2^n)$ над выбранным НП f_n. Элементы строки, расположенные левее ω, заполняются нулями.

Последующие строки матрицы (по направлению снизу вверх) образуются сдвигом предыдущей строки на один разряд влево. Если при этом старший ненулевой разряд строки выходит за пределы матрицы, то векторы, отвечающие таким строкам, приводятся к остатку по модулю НП f_n и, тем самым, строка матрицы также становятся $n-$разрядной.

Пусть $n=6$, $f_6=101011$ и $\omega=11001$. Приходим к примитивной матрице Галуа,

$$G_{f,\omega}=\begin{pmatrix}0&1&1&0&1&1\\0&1&0&0&0&1\\1&0&0&1&0&1\\1&1&1&1&1&1\\1&1&0&0&1&0\\0&1&1&0&0&1\end{pmatrix}. \qquad (13)$$

Обобщенной матрице Галуа G соответствует *обобщенная матрица Фибоначчи* F, формируемая, согласно (4) оператором правостороннего транспонирования $\perp$ матрицы (13), т.е.

$$F_{f,\omega}=\begin{pmatrix}1&0&1&1&1&1\\0&1&1&0&0&1\\0&0&1&1&0&0\\1&0&1&0&0&1\\1&1&1&0&1&1\\0&1&1&1&0&0\end{pmatrix}. \qquad (14)$$

Оператором $1\circ 1$, где $\circ$ – одна из матриц G или F, матрицы (13) и (14) легко преобразуются в обобщенные сопряженные матрицы G^* и F^*.

Рассмотрим пример синтеза обобщенных примитивных матриц и генераторов Галуа, выбрав в качестве неприводимого двоичный полином четвертой степени $f_n=11111$, не являющийся примитивным, и примитивный ОЭ ω полинома f_n, равный 111. Матрицы, отвечающие выбранным параметрам, имеют вид:

$$G=\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix};\qquad F=\begin{pmatrix}1&0&1&0\\1&1&1&1\\1&1&0&1\\0&1&0&0\end{pmatrix}. \qquad (15)$$

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

Структурная схема обобщенного базового четырехразрядного генератора Галуа показана на рис. 5. Вертикально расположенные регистры генераторов, отмеченные сверху символом $\otimes$, реализуют операцию поразрядного умножения, а регистры, отмеченные символом $\oplus-$операцию сложения содержимого регистра по модулю 2.

Генератор Галуа (рис. 5) преобразуется в генератор Фибоначчи заменой содержимого регистров столбцами матрицы F системы (15). Схема сопряженного Галуа генератора ПСП показана на рис. 6.

Если в регистрах умножения (рис. 6) разместить элементы столбцов матрицы F^* системы (15), то получим сопряженный генератор ПСП в конфигурации Фибоначчи.

Из сопоставления рис. 5 и 6 следует, что если в базовых генераторах Галуа и Фибоначчи обратные связи «закручены» по часовой стрелке, то в сопряженных – против часовой стрелки.

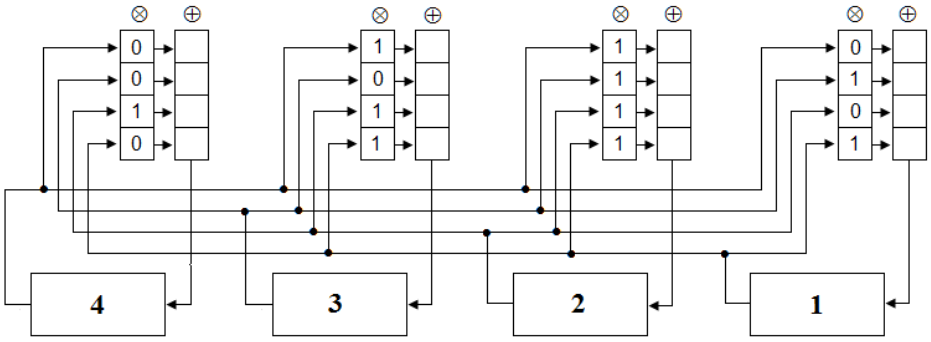

Рис. 5. Структурная схема обобщенных базовых генераторов ПСП Галуа/Фибоначчи

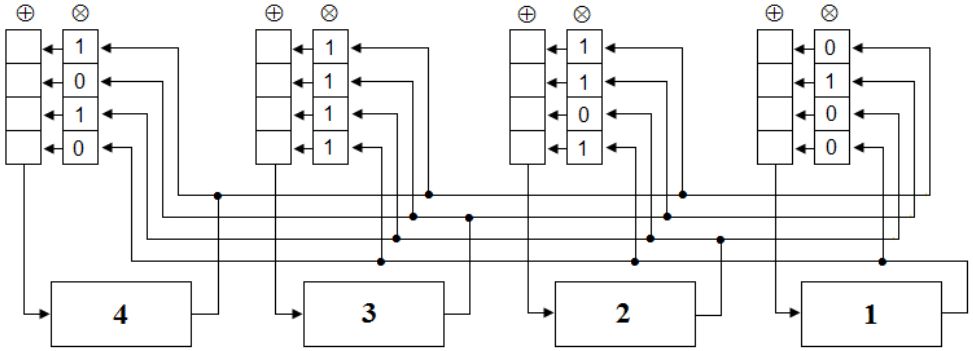

Рис. 6. Структурная схема обобщенных сопряженных генераторов ПСП Галуа/Фибоначчи

V. Изоморфизм матриц Галуа. Согласно изложенному ранее правилу диагонального заполнения на начальном этапе синтеза матрицы $G_{f,\omega}$ формирующий ее элемент ω размещается в младших (правых) разрядах нижней строки матрицы $n-$го порядка. Последующие строки матрицы (снизу вверх) образуются сдвигом на один разряд влево предшествующей строки, причем после сдвига в освободившийся правый разряд записывается 0. В том случае, если ненулевой старший элемент сдвигаемой строки выходит за пределы матрицы, то этот $(n+1)-$разрядный $p-$ичный вектор приводится к остатку по модулю f_n. Тем самым строка возвращается в границы матрицы и процесс заполнения ее строк продолжается по уже описанной схеме.

Из теории многочленов (полиномов) одной переменной известно, что умножение произвольного полинома $\omega_k(x)$ степени k на x эквивалентно сдвигу полинома на один разряд влево и, соответственно, увеличению на 1 степени полинома. Другими словами,

$$x\cdot\omega_k(x)\to\omega_{k+1}(x). \qquad (16)$$

Согласно (16)

$$G_{f,\omega}=\begin{pmatrix}x^{n-1}\cdot\omega\\ x^{n-2}\cdot\omega\\ \cdots\\ x\cdot\omega\\ \omega\end{pmatrix}(\mathrm{mod}\,f)=\omega\cdot\begin{pmatrix}x^{n-1}\\ x^{n-2}\\ \cdots\\ x\\ 1\end{pmatrix}(\mathrm{mod}\,f). \qquad (17)$$

Элементы x^l, $l=\overline{1,n-1}$, правого вектор-столбца в соотношении (17) являются полиномами $l-$й степени одной переменной, векторная форма которых имеет вид

$$x^l\to\underbrace{1,0,\cdots 0,0}_{l+1},\quad l=\overline{1,n-1}. \qquad (18)$$

С учетом замены (18) приходим к такому представлению вектор-столбца

$$\begin{pmatrix}x^{n-1}\\ x^{n-2}\\ \cdots\\ x\\ 1\end{pmatrix}=\begin{pmatrix}1&0&\cdots&0&0\\ 0&1&\cdots&0&0\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ 0&0&\cdots&1&0\\ 0&0&\cdots&0&1\end{pmatrix}=E, \qquad (19)$$

где $E-$единичная матрица $n-$го порядка.

Соотношения (17)-(19) дают возможность сформулировать заключение: матрица Галуа $G_{f,\omega}$ порядка n над НП f_n *изоморфна* ее образующему элементу ω, принадлежащему полю $GF(p^n)$, порожденному полиномом f_n. Следовательно, между матрицей $G_{f,\omega}$ и ее ОЭ ω существует взаимно-однозначное соответствие, которое отобразим отношением изоморфизма

$$G_{f,\omega}\leftrightarrow\omega. \qquad (20)$$

Кроме того, следует иметь в виду, что образующий элемент ω не может быть меньше характеристики p НП f_n, т.е. $\omega \geq p = 10$, так как в противном случае ОЭ становится одноразрядным, занимая при синтезе матрицы Галуа самую правую ячейку нижней строки матрицы. При этом матрица $G_{f,\omega}$ вырождается в диагональную матрицу, не зависящую от НП f_n, что недопустимо. Минимальное значение, равное 10, ОЭ ω принимает, как это имеет место в классических матрицах Галуа, *если только* НП *является примитивным.*

Из отношения изоморфизма (20) вытекают такие следствия:

Следствие 1. Для того чтобы возвести матрицу $G_{f,\omega}$ в степень k достаточно вычислить $\omega_k = \omega^k (\mathrm{mod}\, f_n)$ и по методу диагонального заполнения составить матрицу Галуа по модулю f_n, ОЭ которой является элемент ω_k.

Следствие 2. Минимальное ненулевое значение степени e, обеспечивающее равенство

$$G_{f,\omega}^e = E$$

совпадает с порядком элемента ω, образующего матрицу $G_{f,\omega}$.

Следствие 3. Матрица Галуа $G_{f,\omega}$ примитивна, если примитивным является образующий ее элемент ω.

VI. Анализ генераторов Галуа. В табл. 4 приведены бинарные ПСП, снимаемые с младшего (правого) разряда обобщенного генератора Галуа четвертого порядка.

Таблица 4

ПСП, формируемые обобщенным генератором Галуа над ПрП $f_4 = 10011$

Степень ОЭ	Примитивные образующие элементы							
	10	11	100	101	1001	1011	1101	1110
0	1	1	1	1	1	1	1	1
1	0	1	0	1	1	1	1	0
2	0	1	1	0	1	1	0	1
3	0	1	0	0	1	0	0	0
4	1	0	1	0	0	1	1	1
5	0	0	1	1	1	0	0	1
6	0	0	1	0	0	1	0	0
7	1	1	1	0	1	1	0	0
8	1	0	0	1	1	0	1	1
9	0	0	0	1	0	0	1	0
10	1	1	0	0	0	1	1	0
11	0	1	1	1	1	0	1	0
12	1	0	0	0	0	0	0	1
13	1	1	0	1	0	0	1	1
14	1	0	1	1	0	1	0	1

Назовем бинарную последовательность псевдослучайных чисел *прямой*, если она может быть получена из классической последовательности (первая колонка ОЭ табл. 4, для которой $\omega = 10$) в результате сдвига последней на некоторое число позиций. К прямым в табл. 4 относятся последовательности, которым соответствуют образующие элементы ω, равные 10, 11, 100 и 101. В частности, если ПСП~ $\omega = 11$ (символ ~ следует читать как «формируемой ОЭ») циклически сдвинуть вверх на $k = 3$ позиций, то приходим к ПСП~ $\omega = 10$. Для $\omega = 100$ и $\omega = 101$ параметр k равен 7 и 1 соответственно.

Последовательности бинарных чисел я $G_{f,\omega}^e = E$ вляются обратными (или *инверсными*), если направление формирования чисел генераторами ПСП обратно направлению формирования этих чисел генератором ПСП~ $\omega = 10$. К инверсным относятся последовательности, которым отвечают ОЭ ω, равные 1001, 1011, 1101 и 1110, т.е. ровно половина множества Ω ОЭ $\omega \in \Omega$ в табл. 4.

Как показали результаты анализа, подобными свойствами обладают генераторы ПСП, синтезируемые на основе ПРП 11001 и НП 11111. Эти генераторы, как и генераторы, порождаемые ПРП 10011, формируют четыре прямых и столько же инверсных ПСП, причем направление последовательностей генератора над НП 11111 определялось относительно последовательности ПСП, образуемой минимальным ОЭ $\omega_{\min} = 11$.

Аналогичными свойствами обладают ПСП, построенные на основе практически всех ПрП пятой степени. А именно, из 30-ти последовательностей, образуемых примитивными элементами поля $GF(2^5)$ над ПрП пятой степени, ровно по четыре из них, как и во множестве последовательностей, соответствующих ПрП четвертой степени, являются или прямыми, или инверсными. Из этого правила выпадают последовательности, образуемые примитивными элементами поля $GF(2^5)$ над ПрП $f_5 = 101001$. Множество из 30-ти последовательностей оказывается разбитым на шесть групп, каждая из которых содержит по пять одинаковых последовательностей, причем последовательности, входящие в группы, начиная со второй (к первой относится группа, порождаемая ОЭ $\omega = 10$), не являются ни прямыми, ни инверсными. Отмеченное явление может быть названо артефактом генератора ПСП, которое проявляется в том, что существуют различные примитивные элементы, образующие одинаковые (в группе) мультипликативные $m-$последовательности по $\mathrm{mod}\, 101001$.

Отмеченный артефакт иллюстрируется табл. 5.

Таблица 5

Подтверждение артефакта, проявляющегося в ПрП $f_5 = 101001$

№ ОЭ	Номер группы					
	I	II	III	IV	V	VI
1	10	11	110	111	1000	1001
2	100	101	1010	1011	10010	10011
3	1100	1101	1110	1111	11000	11101
4	10000	10001	10100	10101	11100	11101
5	11010	11011	10110	10111	11110	11111

Согласно данным этой таблицы нечетным группам соответствуют четные ОЭ, тогда как четным группам – нечетные образующие элементы, причем значения последних ОЭ ровно на единицу больше, чем значения предшествующих четных элементов.

И в заключение раздела отметим особенности $m-$последовательностей, образуемых примитивными элементами поля $GF(2^6)$. Так для ПрП $f_6 = 1000011$ из 36-ти последовательностей 11 являются инверсными и ни одной, которые бы относились к прямым последовательностям. Остальные ПрП формируют пять прямых и столько же инверсных последовательностей.

Выводы. В основу построения генераторов псевдослучайных последовательностей могут быть положены совсем не обязательно примитивные полиномы – требование, которое должно соблюдаться при синтезе классических генераторов Галуа или Фибоначчи. Обратные связи в ЛРС-генераторах ПСП в общем случае могут быть организованы любым НП f_n степени n. Достаточно лишь того, чтобы в качестве образующего элемента ω генератора ПСП был использован любой из примитивных элементов поля $GF(2^n)$, порождаемого НП f_n.

Заявляемое утверждение следует рассматривать как гипотезу, сформулированную по результатам анализа свойств ПСП, образуемых обобщенными генераторами, обратные связи в регистрах которых определялись неприводимыми полиномами малой степени, не превышающей шести. Для подтверждения (или опровержения) гипотезы в области криптографических значений степени НП, скажем, когда $n > 20$, потребуется более тщательный анализ.

Криптостойкость ключевых последовательностей, являющихся отрезками двоичных ПСП формируемых линейными генераторами, принято оценивать криптостойкостью априори неизвестных (противнику, атакующему ключ) ПрП, используемых для организации обратных связей в ЛРС-генераторах ПСП. Переход к генераторам ПСП на основе обобщенных ЛРСЛОС расширяет как множество НП, которые потенциально могут быть задействованы для организации линейных обратных связей, так и число $m-$последовательностей, формируемых генераторами для каждого выбранного значения НП f_n.

Если $n-$число разрядов обобщенного генератора ПСП, то $L^* = \varphi(2^n - 1)$. Если, кроме того, n является двоично рациональным числом, то $L^* = 2^{n-1}$ и совпадает с числом примитивных элементов поля $GF(2^n)$, порождаемого НП f_n.

Так, например, для 128 разрядного обобщенного линейного генератора ПСП только за счет выбора примитивного элемента поля Галуа, порождаемого 128-битным НП, существует возможность сформировать порядка 2^{127} различных сбалансированных бинарных последовательностей, каждая из которых может быть использована в качестве секретного 128-битного ключа шифрования.

На основании вышеизложенного приходим к заключению, что применение обобщенных генераторов псевдослучайных последовательностей Галуа потенциально может обеспечить возможность существенного повышения стойкости алгоритмов шифрования.

ЛИТЕРАТУРА

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

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

[3]. Асосков А. В. Поточные шифры. / А. В. Асосков, М. А. Иванов, А. А. Мирский и др. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

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

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

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

[7]. Белецкий А. Я. Примитивные матрицы и генераторы псевдослучайных последовательностей Галуа / А. Я. Белецкий, Е. А. Белецкий // Зб. нау-

ков праць «Інформаційні технології в освіті», 2014, вип. 18. – С. 14-29.
[8]. Білецький А. Я. Синтез і аналіз узагальнених примітивних поліномів / Білецький А.Я. // Наукоємні технології. – К.: НАУ. – 2012. – № 1 (13). – С. 35-38.
[9]. Сайт полиномов / [Электр. ресурс]. – Режим доступа: http://theory.cs.uvic.ca/gen/poly. html
[10]. Белецкий А. Я. Криптографические приложения примитивных матриц / Белецкий А.Я. // Сучасний захист інформації. – К.: ДУІКТ. – 2012. – № 4. – С. 4-24.
[11]. Мулложанов Р. В. Generalized transposition of matrices and linear structure of large-scale systems./ [Электронный ресурс]. – Режим доступа: http:nbuv.gov.ua/j-pdf/dnanu 2009 10 6.pdf
[12]. Математическая энциклопедия. Том 5. – М.: Изд-во «Советская энциклопедия», 1985. – 623 с.
[13]. Подобные матрицы. – Режим доступа: https://ru.wikipedia.org/wiki/Подобные матрицы

REFERENCES

[1]. Stream Ciphers. The results of the open foreign cryptology. – M., 1997. http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm
[2]. Ivanov V., A., Chugunkov I., V. Theory, Appl. and Evaluation of the Quality of Pseudorandom Sequences. – M.: KUDIC-OBRAZ, 2003. – 368 P.
[3]. Asoskov A.V., Ivanov A. M., Mirskiy A. A. Stream ciphers. – M.: KUDIC-OBRAZ, 2003. - 336 P.
[4]. Volkovich S. A., Geranin V. O., Movchan T. V., Pisarenko L. D. Introduction to the algebraic theory of error-correcting coding, Kiev, VPF UkrINTEI, 2002., 236 p.
[5]. Ivanov M.A. Cryptographic methods of information security in computer systems and fields., M.: KUDIC-OBRAZ, 2001, 368 P.
[6]. Lidl R., Niederreiter H. Finite Fields T. 1. – M.: Mir, 1988, 432 p.
[7]. Beletsky A. Ja., Beletsky E. A. Primitive Matrix and Pseudo-Random Sequences of Galois // Information Techn. in Education, 2014, p.p. 128-133.
[8]. Beletsky A. Ja. Synthesis and Analysis of Generalized Primitive Polynomials // High Tech Technology, 2012, № 1 (13), p.p. 35-38.
[9]. Website Polinomials. http//theory.cs.uvic./gen/pole.html
[10]. Beletsky A. Ja. Cryptographic Applications of Primitive Matrices. / Modern Data Protection K.: DUIKT, 2012., № 4., p.p. 4-24.
[11]. Mullozhanov R. V. Generalized transposition of matrices and linear structure of large-scale systems. http:nbuv.gov.ua/j-pdf/dnanu 2009 10 6.pdf
[12]. Encyclopedia of Mathematics. Volume 5 - M.: Publisher "Soviet encyclopedia", 1985, 623 p.
[13]. Matrix Similarity. http://en.wikipedia.org/wiki/Matrix_similarity

ПРИМІТИВНІ МАТРИЦІ ГАЛУА В КРИПТОГРАФІЧНИХ ЗАСТОСУВАННЯХ

Для ряду задач захисту інформації криптостійкість У статті розглянуті питання формування узагальнених примітивних матриць Галуа довільного порядку n, елементи яких належать простому полю $GF(2)$. Синтез матриць базується на використанні незвідних поліномів f_n ступеня n і примітивних елементів розширеного поля $GF(2^n)$, що породжується поліномами f_n. Запропоновано способи побудови сполучених примітивних матриць Галуа і однозначно пов'язаних з ними правостороннім транспонуванням матриць Фібоначчі. Обговорюються способи застосування таких матриць в криптографічних застосуваннях для вирішення завдання побудови узагальнених лінійних генераторів псевдовипадкових послідовностей Галуа максимального періоду. Проведено аналіз псевдовипадкових бінарних послідовностей, що формуються лінійними генераторами Галуа, в зворотних зв'язках регістрів яких використовуються примітивні поліноми малого ступеня в діапазоні від чотирьох до шести.
Ключові слова: незвідні і примітивні поліноми, примітивні матриці, лінійні регістри зсуву, генератори псевдовипадкових послідовностей Галуа.

PRIMITIVE MATRIX GALOIS IN CRYPTOGRAPHIC APPLICATIONS

The article discusses the formation of generalized Galois primitive matrices of arbitrary order n, the elements of which belong to the prime field $GF(2)$. Synthesis of matrices based on the use of irreducible polynomials of degree n and primitive elements of the extended field $GF(2^n)$, which generated by polynomials. The methods of constructing conjugate primitive matrices Galois and unambiguously related matrices Fibonacci. Discusses ways to use these matrices in cryptographic applications to solve the problem of the generalized linear generators of pseudo-random sequences Galois of maximal period. The analysis of the binary pseudo-random sequences generated by linear generators Galois in feedback registers that use primitive polynomials of small degree in the range of four to six.
Keywords: irreducible and primitive polynomials, primitive matrices, linear shift registers generators of pseudorandom sequences Galois.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net.
Білецький Анатолій Якович, доктор технічних наук, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, doctor of Technical Science, Professor of Department Electronics of National Aviation University.