УДК 512.623.3

СИНТЕЗ ОБОБЩЕННЫХ ПРИМИТИВНЫХ ПОЛИНОМОВ

А.Я. Белецкий, *д-р техн. наук, профессор,*
Национальный авиационный университет, г. Киев

Получены аналитические оценки числа образующих элементов, придающих свойство примитивности произвольным неприводимым двоичным полиномам, в том числе и не являющихся примитивными по классическому определению. Показано, что количество таких образующих элементов однозначно определяется лишь степенью неприводимого полинома. Приведен алгоритм синтеза порождающих матриц Галуа и Фибоначчи над обобщенными примитивными полиномами и рассмотрены прикладные аспекты их применения.

Ключевые слова: *синтез, произвольный неприводимый двоичный полином, порождающие матрицы Галуа и Фиббоначи.*

ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

В теории полей Галуа, составляющих основу алгебраической теории помехоустойчивого кодирования и современной теории криптографии, ключевым является понятие неприводимого полинома (НП). Исходя из того, что в данной статье мы будем рассматривать переменные и функции, принадлежащие исключительно двоичному пространству, обозначаемому в теории полей Галуа $GF(2^n)$, приведем частное, отвечающее полю $GF(2^n)$, определение НП.

Полином

$$\varphi_n(x) = \sum_{i=0}^{n} \alpha_{n-i} x^{n-i}, \qquad \alpha_i \in \{0, 1\}, \tag{1}$$

степени n над полем $GF(2^n)$ называется *неприводимым*, если он не делится ни на какой полином меньшей степени над данным полем [1].

Полином (1), записанный в *алгебраической* форме, может быть однозначно представлен бинарной строкой (двоичным вектором) своих коэффициентов (в *бинарной* форме)

$$\varphi_n = \{\alpha_n, \alpha_{n-1}, \ldots, \alpha_i, \ldots, \alpha_0\}, \alpha_i \in \{0, 1\}.$$

Например, бинарному вектору

$$\varphi_8 = 100011011$$

соответствует алгебраическая форма полинома

$$\varphi_8(x) = x^8 + x^4 + x^3 + x + 1. \tag{2}$$

Введем одну из главных характеристик НП, называемую показателем полинома. *Показатель* неприводимого полинома равен наименьшему положительному числу e, при котором НП $\varphi_n(x)$ делит двучлен $x^e - 1$ без остатка [2]. Физический смысл такой характеристики состоит в том, что он определяет *порядок* (иначе называемый мощностью) мультипликативной группы (равный числу элементов группы), образованной степенями *примитивного элемента* θ группы по mod φ_n.

Множество неприводимых полиномов $\{\varphi_n\}$ содержит важное (например, для криптографических приложений, информатики, электроники и других направлений науки и техники) подмножество так называемых примитивных полиномов (ПрП). В алгебре, теории чисел и полей Галуа двоичный полином $\varphi_n(x)$ степени n называется *примитивным*, обозначим его $\varphi_n^*(x)$, если он неприводим, а наименьший показатель e, при котором $\varphi_n^*(x)$ делит двучлен $\Phi(x) = x^e - 1$ без остатка, определяется выражением $e = 2^n - 1$ [2].

Приведем другой (авторский) вариант определения примитивного полинома. Неприводимый полином $\varphi_n(x)$ степени n относится к подмножеству примитивных полиномов $\varphi_n^{(\omega)}(x)$ при выполнении следующих условий. Во-первых, полином должен быть неприводимым. Во-вторых, последовательность степеней некоторого k – разрядного бинарного вектора (тоже полинома) ω, называемого *образующим* (примитивным) элементом, приведенных к остатку по модулю $\varphi_n^{(\omega)}$, составляет последовательность максимальной длины (иначе, m – последовательность).

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

Второе определение НП математически можно отобразить соотношением $GF^*(2^n) = \langle\omega\rangle$. Здесь $GF^*(2^n)$ означает полное множество n-битных векторов, за исключением нулевого вектора, т.е. мощность (число элементов) этого множества равна $e = 2^n - 1$, а $\langle\omega\rangle$ есть мультипликативная группа порядка $2^n - 1$.

В теории полиномов постулируется утверждение, согласно которому все примитивные полиномы являются неприводимыми, тогда как обратное не всегда соблюдается, т. е. совсем не обязательно, чтобы каждый неприводимый полином обладал свойствами примитивности.

Основная задача данного исследования заключается в доказательстве того, что, во-первых, любой НП φ_n степени n соответствующим подбором образующих элементов ω приводится к примитивному полиному $\varphi_n^{(\omega)}$; и, во-вторых, число элементов ω, доставляющих произвольному неприводимому полиному φ_n свойство примитивности, есть величина постоянная, определяемая только значением n.

В заключительном разделе работы предлагается достаточно простой алгоритм синтеза образующих матриц Галуа и Фибоначчи, посредством которых формируются m-последовательности n – разрядных двоичных кодовых комбинаций для выбранных примитивных над элементами ω

полиномов $\varphi_n^{(\omega)}$. Также кратко обсуждаются возможности применения обобщенных примитивных полиномовдля построения генераторов бинарных псевдослучайных последовательностей и криптопримитивов нелинейной подстановки (так называемых S-блоков).

ОСНОВНЫЕ СООТНОШЕНИЯ

Приведенное ранее первое определение примитивного полинома $\varphi_n^*(x)$ можно отобразить такими эквивалентными соотношениями:

$$\varphi_n(x) \mid x^e - 1; \tag{3}$$

$$x^e \equiv 1 \pmod{\varphi_n(x)}, \tag{4}$$

при условии, что

$$\min e = 2^n - 1. \tag{5}$$

Предлагаемое обобщение понятия примитивного полинома сводится к следующему. Заменим основание x одночлена x^e в формулах (3) и (5) произвольным полиномом $\omega_m(x)$ степени m такой, что $1 \le m < n$. Тем самым представим данные выражения в виде

$$\varphi_n(x) \mid [\omega_m(x)]^e - 1; \tag{6}$$

$$[\omega_m(x)]^e \equiv 1 \bmod \varphi_n^{(\omega)}(x), \tag{7}$$

при соблюдении условия (5).

Полином $\omega_m(x)$ назовем *образующим элементом* (ОЭ)ПрП, подобный ранее введенному образующему элементу θ. Дальнейшие пояснения упростятся, если от алгебраических форм полиномов $\varphi_n(x)$ и $\omega_m(x)$ перейти к их бинарным формам. В классическом варианте (3) или (4) одночлен x^e можно записать в виде числового (бинарного) эквивалента $(10)^e$, поскольку основание x есть полином первой степени с минимальным весом, т.е. x=10. В то же время ОЭ ω_m может быть отличным от полинома $x = 10$ и принимать значения 11, 110, 101 и др.

Неприводимый полином (2) выбран разработчиками криптографического алгоритма Rijndaelв качестве базового для построения примитива нелинейной подстановкив шифреAES (Advanced Encryption Standard), принятого в качестве американского Стандарта симметричной блочной криптографической защиты информации [3]. Относительно НП (2) можно сказать следующее. Во-первых, этот полином не является примитивным; его показатель равен 51. Во-вторых, как справедливо отмечается в [4], полином $\varphi_8(x)$, заданный выражением (2), является первым НП восьмой степени, упоминающийся в большинстве справочников, т.е. его выбор достаточно произволен.

Как известно, S-блоки могут быть реализованы *только* на примитивных полиномах. Проблему непримитивности полинома авторы алгоритма Rijndael обошли простой заменой одночлена x двучленом $x+1$. Такая замена привела к тому, что исходный непримитивный полином показателя 51 приобрел свойство примитивности с показателем 255.

Проведенный краткий анализ неприводимых и примитивных полиномов как раз и подтверждает возможность и целесообразность перехода от классического представления примитивного полинома в виде

соотношений (3) или (4) к обобщенному представлению выражениями (6) или (7) соответственно.

ОБРАЗУЮЩИЕ ЭЛЕМЕНТЫ ПРИМИТИВНЫХ ПОЛИНОМОВ

Введем ряд обозначений, необходимых для дальнейших выкладок. Пусть $L_n = 2^n - 1$ есть общее число n-битных векторов, за исключением нулевого вектора; $L_n^{(\omega)}$ – число образующих элементов ω, доставляющих НП φ_n свойство примитивности.

Число $L_n^{(\omega)}$ определяется функцией Эйлера φ аргумента L_n, т.е.

$$L_n^{(\omega)} = \varphi(L_n). \tag{8}$$

В самом деле, в любой абелевой группе по умножению порядка L_n число ее элементов, взаимно простых с L_n (а только такие элементы могут быть выбраны в качестве образующих) составляет величину, являющуюся функцией Эйлера аргумента L_n. Тем самым мы и приходим к выражению (8).

Неприводимый полином φ_n (который становится примитивным, если в качестве образующего элемента мультипликативной группы выбран некоторый подходящий элемент ω) будем именовать *примитивным над* ω полиномом и обозначать, как мы уже приняли выше, $\varphi_n^{(\omega)}$.

МАТРИЧНЫЕ ФОРМЫ m – ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Безусловно, что мультипликативную группу $\langle\omega\rangle$ можно сформировать последовательным возведением в степень образующего элемента ω с дальнейшим приведением степени ОЭ к остатку по модулю $\varphi_n^{(\omega)}$. В данном разделе работы мы покажем, что эту же m-последовательность $\langle\omega\rangle$ можно получить на основе простейших модулярных матричных вычислений.

Пусть $M_n^{(\omega)}$ обозначает матрицу, формирующую $\langle\omega\rangle$. Введем n-битный вектор V_k, определяемый соотношением

$$V_k = \omega^k \bmod \varphi_n^{(\omega)}. \tag{9}$$

Наша задача заключается в том, чтобы найти такую матрицу $M_n^{(\omega)}$, с помощью которой можно было бы реализовать преобразование

$$V_{k+1} = V_k \otimes M_n^{(\omega)}, \quad k = \overline{0, L_n}, V_0 = V_{L_n} = 1, \tag{10}$$

и тем самым получить m-последовательность n-битных чисел, образуемую степенями ОЭ ω по модулю ПрП $\varphi_n^{(\omega)}$.

Изложим идею построения матриц преобразования $M_n^{(\omega)}$ на примере примитивного над ОЭ $\omega = 111$ полинома $\varphi_8^* = 100101101$.

Процесс синтеза матрицы $M_8^{(111)}$ разбивается на два этапа. На первом этапе составляется так называемая *стартовая таблица*, содержащая

стартовую матрицу восьмого порядка M, однозначно определяемую ее ОЭ ω (табл. 1, в которой стартовая матрица выделена затенением).

Таблица 1 – Стартовая таблица

$\varphi\rightarrow$	1	0	0	1	0	1	1	0	1
	Мет-								
	ки	8	7	6	5	4	3	2	1
8		1							
7		1	1						
6		1	1	1					
5			1	1	1				
4				1	1	1			
3					1	1	1		
2						1	1	1	
1	V_1						1	1	1

Вектор V_1 порождает диагональное заполнение элементов стартовой матрицы M. Предполагается, что в незаполненных ячейках матрицы M находятся нули. Для простоты восприятия эти ячейки оставлены пустыми.

Проверим корректность предлагаемого алгоритма составления стартовой матрицы. Для векторов V_k таких, что номер старшего разряда, в котором стоит 1, не превышает $n-m$, где m – степень ОЭ, мы можем двумя способами вычислить вектор V_{k+1}. При первом способе (назовем его *аналитическим*) вектор V_{k+1} определяется соотношением

$$V_{k+1} = (V_k \otimes \omega) \bmod \varphi_n^*. \qquad (11)$$

Пусть $V_k = 110101$. Для принятых значений параметров преобразования, а именно, $n=8$, $\omega = 111$ и $\varphi_8^* = 100101101$, по формуле (11) получим

$$V_k = 10001011. \qquad (12)$$

Второй способ вычисления вектора V_{k+1} (назовем его *графическим*) сводится к поразрядному сложению по $\bmod 2$ элементов тех строк стартовой матрицы, номера которых совпадают с номерами разрядов вектора V_k, содержащих 1. Отметим звездочками строки стартовой матрицы, отвечающие вектору $V_k = 110101$, как это показано в табл. 2.

Таблица 2 - Графический способ вычисления произведения (12)

$\varphi\rightarrow$	1	0	0	1	0	1	1	0	1
	Метки								
		8	7	6	5	4	3	2	1
8		1							
7		1	1						
6	*	1	1	1					
5	*		1	1	1				
4				1	1	1			
3	*				1	1	1		
2						1	1	1	
1	*						1	1	1

Выполнив поразрядное сложение элементов выделенных в табл. 2 строк, получим кодовую комбинацию 10001011, совпадающую с ранее аналитически полученным результатом (12).

Аналогичным образом можно удостовериться в том, что диагональная расстановка элементов стартовой матрицы, приведенная в табл. 1, дает возможность правильно вычислить V_{k+1} для всех входных векторов V_k, у которых номер старшего разряда, содержащего 1, не превышает 6.

На втором этапе синтеза матрицы $M_8^{(111)}$ нам остается уточнить значения элементов в седьмой и восьмой строках табл. 1. С этой целью отметим сначала звездочками нижние семь строк стартовой матрицы, сформировав тем самым входной вектор $V_k = 1111111$. По формуле (11) получим (воспользовавшись аналитическим методом) вектор V_{k+1}, равный 01010000. Если же произвести поразрядное сложение элементов строк табл. 1 (т.е. воспользовавшись графическим методом) с первой по седьмую, то приходим к вектору $V = 01111101$. Из сопоставления векторов V_{k+1} и V следует, что они различаются в первом, третьем, четвертом и шестом разрядах. Инвертируя соответствующие разряды в седьмой строке в матрице M табл. 1, устраняем расхождение в векторах V_{k+1} и V, что отражено в табл. 3.

Таблица 3 - К вычислению седьмой строки матрицы M

φ →	1	0	0	1	0	1	1	0	1
	Мет-								
	ки	8	7	6	5	4	3	2	1
8		1							
7	*	1	1	1	0	1	1		1
6	*	1	1	1					
5	*		1	1	1				
4	*			1	1	1			
3	*				1	1	1		
2	*					1	1	1	
1	*						1	1	1

Выполнив аналогичную корректировку восьмой строки табл. 3, приходим к окончательной форме матрицы преобразования, которую обозначим $G_\varphi^{(111)}$.

$$G_\varphi^{(111)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (13)$$

Легко убедиться в том, что матрица (13) порождает последовательность восьмибитных кодов, совпадающую с последовательностью, образуемой степенями $\omega = 111$ по модулю

$\varphi = 100101101$. На этом основании матрицы $G_{\varphi}^{(\omega)}$ (и ей подобные) будем называть *образующими* матрицами.

Матрицам $G_{\varphi}^{(\omega)}$ отвечают так называемые *сопряженные* матрицы $F_{\varphi}^{(\omega)}$, связанные с $G_{\varphi}^{(\omega)}$ оператором правостороннего транспонирования (т.е. транспонирования относительно вспомогательной диагонали матрицы), который мы обозначим $^{\perp}$. Имеем

$$G \xleftrightarrow{\perp} F, \qquad \text{иначе} \quad F = G^{\perp}, \quad \text{или} \quad G = F^{\perp}.$$

В частности, для матрицы (13) получим сопряженную ей образующую матрицу

$$F_{\varphi}^{(111)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (14)$$

Матрицы (13) и (14) есть матрицы Галуа и Фибоначчи соответственно.

ПРИКЛАДНЫЕ АСПЕКТЫ

Кратко обсудим некоторые направления применения образующих матриц. Одним из них является построение линейных регистров сдвига с линейными обратными связями (ЛРС), широко используемых для программной или аппаратной реализации генераторов псевдослучайных последовательностей (ПСП)[5]. Такие регистры строят, как правило, на D-триггерах, отклик которых после подачи синхроимпульса повторяет сигнал (0 или 1), подведенный к входу триггера.

Обозначим $\varepsilon_{i,j}$, $i,\ j = \overline{1,\ n}$, элемент G- или F-образующей матрицы. Напомним, что строки матриц нумеруются снизу вверх, а столбцы – справа налево. Функция f_k возбуждения $k-$го триггера (разряда регистра, которые тоже условимся нумеровать справа налево), определяется соотношением

$$f_k = \oplus_{i=1}^{n} \varepsilon_{i,\ k} \cdot i, \ k = \overline{1,\ n}, \qquad (15)$$

где символ $\oplus$ есть оператор сложения по модулю 2.

Для примера, функции возбуждения G-генератора ПСП, вычисленные по формуле (15) на основании матрицы (13), и F-генератора ПСП, вычисленные на основании матрицы (14), сведены в табл. 4. Такие ЛРС-генераторы ПСП носят названия генераторов по схемам Галуа и Фибоначчи соответственно [5].

Таблица 4 - Функции возбуждения триггеров генераторов ПСП

f_k	G – генератор ПСП	F – генератор ПСП
1	$1\oplus 7\oplus 8$	$1\oplus 2\oplus 3\oplus 4\oplus 6\oplus 7\oplus 8$
2	$1\oplus 2\oplus 8$	$1\oplus 2\oplus 3\oplus 5\oplus 6\oplus 8$
3	$1\oplus 2\oplus 3\oplus 7\oplus 8$	$1\oplus 2\oplus 3$
4	$2\oplus 3\oplus 4\oplus 7$	$2\oplus 3\oplus 4$
5	$3\oplus 4\oplus 5\oplus 8$	$3\oplus 4\oplus 5$
6	$4\oplus 5\oplus 6\oplus 7\oplus 8$	$4\oplus 5\oplus 6$
7	$5\oplus 6\oplus 7\oplus 8$	$5\oplus 6\oplus 7$
8	$6\oplus 7\oplus 8$	$6\oplus 7\oplus 8$

На основании таблиц функций возбуждения триггеров регистра легко составляется структурная схема ЛРС. Покажем это на примерах регистров восьмого порядка, построенных на основании ПрП восьмой степени, общую форму которых представим в виде

$$\varphi_8 = 1u_8u_7u_6u_5u_4u_3u_21,$$

где $u_k \in \{0, 1\}$, $k = \overline{2, 8}$.

Для ОЭ $\omega = 11$ образующие матрицы представлены соотношениями

$$G_{\varphi_8}^{(11)} = \begin{bmatrix} 1\oplus u_8 & u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}; \qquad (16)$$

и

$$F_{\varphi_8}^{(11)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & u_2 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & u_3 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & u_4 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & u_5 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & u_6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & u_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\oplus u_8 \end{bmatrix}. \qquad (17)$$

Выберем полином $\varphi_8^* = 110100011$, примитивный над $\omega = 11$. Такому ПрП, согласно матрицам преобразования (16) и (17), соответствуют структурные схемы ЛРС, показанные на рис. 1 и 2 соответственно.

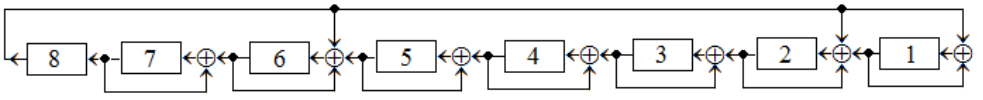

Рисунок 1 – Структурная схема ЛРС по схеме Галуа

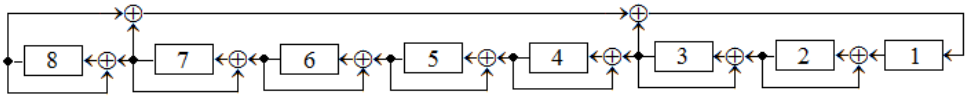

Рисунок 2– Структурная схема ЛРС по схеме Фибоначчи

Не менее перспективным является применение обобщенных ПрП для оптимизации S-блоков, простейшая форма которого, выбранная для шифра AES, описывается выражением

$$y = x^{-1} \otimes A \oplus \beta , \qquad (18)$$

где x и y есть входной и выходной байты преобразования соответственно; x^{-1} – байт, мультипликативно обратный байту x по модулю НП (2) над ОЭ $\omega = 11$; β – аддитивная компонента, равная 01100011; и, наконец, A – невырожденная циркулянтная матрица восьмого порядка

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

Существуют различные критерии оптимизации преобразования (18). В основу оптимизации положим эмпирический критерий *равномерности рассеивания*, суть которого состоит в следующем. Разобьем интервал от 0 до 255, в который укладываются обе переменные x и y в соотношении (18), на k эквидистантных отрезков, причем k и k^2 должны быть делителями числа 256. При таком способе разбиения осей декартовых координат x и y образуется таблица, содержащая k^2 квадратов (элементов), размер каждой стороны которых равен k. Последовательно придавая переменной x в формуле (18) значения от 0 до 255, подсчитаем *частоту* $n^*_{i,j}$ вхождений переменной y в (i, j)-й элемент таблицы. Обозначим $p^*_{i,j} = n^*_{i,j} / 256$ и назовем эту оценку *статистической частостью* (i, j) – го квадрата. В идеальном случае, когда каждый элемент таблицы содержит одинаковое число $256 / k^2$ откликов y, частости всех элементов таблицы также будут одинаковыми и равными $p = 1 / k^2$.

Выберем в качестве меры отклонения статистического показателя $p^*_{i,j}$ S-блока от идеального значения p, при котором обеспечивается абсолютная равномерность рассеивания, величину

$$U = \sum_{i,j=1}^{k} (p^*_{i,j} - p)^2 . \qquad (19)$$

Как показали результаты компьютерных расчетов, критерий (19) инвариантен к аддитивной компоненте β в (18). Параметрами, влияющими на меру (19), являются: полином φ_8^*, примитивный над образующим элементом ω, и матрица преобразования A. При этом оказалось, что параметры ω, φ_8^* и матрица A, использованные в S-блоке (18) шифра AES, далеки от оптимальных значений.

ВЫВОДЫ

В классической полиномиальной теории считается устоявшимся представление относительно того, что множество двоичных неприводимых полиномов $\varphi_n(x)$ степени n включает подмножество примитивных $\varphi_n^*(x)$ полиномов, показатель которых составляет максимально возможную величину L_n, равную $2^n - 1$. При этом принимается как постулат, что все примитивные полиномы неприводимые, тогда как обратное не всегда верно. Данные утверждения абсолютно справедливы, если только образующим (примитивным) элементом ω мультипликативной группы порядка L_n, формируемой степенями ω по mod $\varphi_n^*(x)$, является элемент $\omega = x$, т.е. минимальный по весу полином первой степени, бинарная форма которого $\omega = 10$.

Основной результат данной работы состоит в том, что в ней введено понятие *обобщенного примитивного полинома*, расширяющее классический термин примитивного полинома. Показано, во-первых, что *все* неприводимые полиномы, в том числе и те, которые в классическом понимании не являются примитивными, приобретают свойство примитивности соответствующим выбором образующего элемента. Таким способом, в частности, разработчики криптоалгоритма Rijndael заменой образующего элемента $\omega = 10$ элементом $\omega = 11$ обратили выбранный ими для построения S-блока непримитивный полином (2) в примитивный. Во-вторых, число образующих элементов, посредством которых *все* неприводимые полиномы степени n становятся примитивными, есть величина постоянная, равная функции Эйлера аргумента L_n.

Кроме того, предложен достаточно простой алгоритм синтеза G- и F-образующих матриц, с помощью которых непосредственно формируются мультипликативные группы порядка L_n по выбранным параметрам φ_n^* и ω, а также определяются функции возбуждения n-разрядных линейных регистров сдвига с линейными обратными связями по схемам Галуа и Фибоначчи.

SUMMARY

SYNTHESIS OF PRIMITIVE POLYNOMIALS

Ja. Beletsky

The number of generators, which give the property of primitiveness to arbitrary irreducible binary polynomials, including non-primitive on the classical definition has been analized. It's been shown that the number of such generators is uniquely determined only by the power of an irreducible polynomial. An algorithm for synthesis of generating Galois and Fibonacci matrices over the generalized primitive polynomials and applied aspects of their applicationhas been considered.

Key words: *synthesis, polinomial, non-primitive, irreducible, Galois and Fibonacci matrices.*

СПИСОК ЛИТЕРАТУРЫ

1. Лидл Р. Конечные поля: пер. с англ./ Р. Лидл, Г. Нидеррайтер. – Т. 1. – М.: Мир, 1988. – 432 с.
2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
3. csrc.nist.gov/publications/fips/fips197/fips-197.pdf
4. Зензин О. С. Стандарт криптографической защиты AES. Конечные поля / О. С. Зензин, М. А. Иванов / под ред. М. А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.
5. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

Поступила в редакцию 20 сентября 2011 г.