УДК 512.623.3 Белецкий А.Я., Белецкий А.А., Навроцкий Д.А., Кандыба Р.Ю.
(Национальный авиационный университет)

ПРИМИТИВНЫЕ ПОЛИНОМЫ В КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

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 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

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

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

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

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

Например, бинарному вектору

$$\varphi_8 = 100011011$$

соответствует алгебраическая форма полинома

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

Отметим некоторые особенности неприводимых полиномов в бинарном представлении. Во-первых, старший $(n+1)$-й разряд НП φ_n равен 1 (по определению). Во-вторых, младший (первый) разряд НП φ_n также равен 1, иначе, в противном случае он будет четным и, следовательно, содержать в качестве делителя полином 10, в силу чего утрачивает свойство примитивности. И, наконец, в-третьих, *вес* НП, равный количеству не нулевых разрядов полинома, должен быть нечетным числом. Легко убедиться на примерах, что если вес полинома четный, то он содержит простой делитель 11 и также теряет свойство примитивности. Следует иметь в виду, что перечисленные условия, которым должны удовлетворять НП, являются *необходимыми*, но далеко еще не *достаточными*.

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. Физический смысл такой характеристики состоит в том, что он определяет *порядок* 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*, если он неприводим, а наименьший показатель e, при котором $\varphi_n(x)$ делит двучлен $\Phi(x) = x^e + 1$ без остатка, определяется выражением $e = 2^n - 1$.

Приведем другой (авторский) вариант определения примитивного полинома. Неприводимый полином φ_n степени n относится к подмножеству примитивных полиномов $\varphi_n^{(\omega)}(x)$, если последовательность степеней некоторого m-разрядного бинарного вектора ω_m, называемого *образующим* (примитивным) элементом, приведенных к остатку по модулю $\varphi_n^{(\omega)}(x)$, составляет последовательность максимальной длины (иначе, m-последовательность). Данное определение можно условно назвать «инженерным», не являющимся математически строгим, но которое послужит в дальнейшем основой построения предлагаемых обобщенных примитивных полиномов.

Второе определение ПрП 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 табл. 1 приведен в качестве примера полный список НП восьмой степени; примитивные полиномы (по классическому определению), показатель которых составляет 255, выделены затенением.

Таблица 1. Неприводимые полиномы восьмой степени

Номер НП	Бинарная форма НП	Показатель НП	Номер НП	Бинарная форма НП	Показатель НП
1	100011011	51	16	110001011	85
2	100011101	255	17	110001101	255
3	100101011	255	18	110011111	51
4	100101101	255	19	110100011	85
5	100111001	17	20	110101001	255
6	100111111	85	21	110110001	51
7	101001101	255	22	110111101	85
8	101011111	255	23	111000011	255
9	101100011	255	24	111001111	255
10	101100101	255	25	111010111	17
11	101101001	255	26	111011101	85
12	101110001	255	27	111100111	255
13	101110111	85	28	111110011	51
14	101111011	85	29	111110101	255
15	110000111	255	30	111111001	85

Основная задача данного исследования заключается в определении основных аспектов криптографических приложений неприводимых полиномов. В частности, разработан достаточно простой алгоритм вычисления матриц Галуа и Фибоначчи, посредством которых синтезируются линейные регистры сдвига с линейными обратными связями, а также предложена криптостойкая односторонняя функция.

Основные соотношения

Приведенное ранее первое определение примитивного полинома $\varphi_n(x)$ отображается такими эквивалентными соотношениями:

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

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

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 (4) произвольным полиномом $\omega_m(x)$ степени m такой, что $1 \leq m < n$. Тем самым представим данные выражения в виде:

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

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

при соблюдении условия (5).

Полином $\omega_m(x)$ назовем *образующим* (или примитивным) *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 представляет собой 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 Rijndael в качестве базового для построения примитива нелинейной подстановки в шифре AES (Advanced Encryption Standard), принятого в качестве американского Стандарта симметричной блочной криптографической защиты информации [1]. Относительно НП (2) можно сказать следующее. Во-первых, этот полином не является примитивным; его показатель равен 51. Во-вторых, как справедливо отмечается в монографии [2], полином $\varphi_8(x)$, заданный выражением (2), является первым НП восьмой степени, упоминающийся в большинстве справочников, т.е. его выбор достаточно произволен.

Как известно, Rijndael подобные S-блоки могут быть реализованы *только* на основе *m*-последовательностей, формируемых примитивными полиномами. Проблему приведения непримитивного полинома (2) к примитивному авторы алгоритма Rijndael решили простой заменой одночлена x двучленом $x+1$. Такая замена привела к тому, что исходный непримитивный полином показателя 51 приобрел свойство примитивности с показателем 255, как это следует из табл. 2.

Таблица 2. Степени ОЭ $\omega = 11$ по модулю 100011011

	Младший разряд степени (j)															
	1	3	5	F	1	3	5	F	A	E	2	6	1	8	3	5
	F	1	8	8	8	3	5	4	7	2	6	A	E	2	6	A
	5	4	C	4	7	9	B	6	A	E	9	0	0	B	6	1
	3	5	4	C	4	C	4	C	F	1	8	8	3	E	2	D
	C	4	7	9	0	B	D	7	2	6	1	8	8	8	8	8
	3	E	9	0	B	D	C	F	1	8	3	E	9	B	6	A
	5	4	7	9	0	0	0	0	B	D	7	9	B	6	1	3
	E	9	B	D	7	2	D	C	F	1	3	E	9	0	0	0
	B	6	A	E	2	D	7	2	D	7	2	6	A	5	F	1
	3	E	2	D	7	9	0	0	B	D	C	4	C	F	A	5
	F	A	5	4	C	F	A	E	2	D	C	F	A	E	9	0
	B	6	1	8	8	3	5	F	A	5	F	1	8	3	5	4
	C	F	1	3	5	4	7	9	B	D	7	9	0	B	6	A
	5	F	A	E	9	B	6	1	8	3	E	2	6	1	3	E
	2	6	A	E	9	B	D	C	F	A	5	4	7	2	D	7
	9	B	D	C	4	7	2	D	C	4	C	4	7	2	6	1

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). Полный список образующих элементов в 16-ричной форме, доставляющих свойство НП (2), приведен в табл. 4.

Отметим, в частности, что первым элементом в табл. 3 является элемент $\omega = 11$, выбранный разработчиками алгоритма Rijndael для приведения непримитивного полинома (2) к примитивному.

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 $\varphi_n^{(\omega)}$.

Таблица 3. Образующие элементы

Hex	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	---	3	5	6	9	B	E	11	12	13
[1]	14	17	18	19	1A	1C	1E	1F	21	22
[2]	23	27	28	2A	2C	30	31	3C	3E	3F
[3]	41	45	46	47	48	49	4B	4C	4E	4F
[4]	52	54	56	57	58	59	5A	5B	5F	64
[5]	65	68	69	6D	6E	70	71	76	77	79
[6]	7A	7B	7E	81	84	86	87	88	8A	8E
[7]	8F	90	93	95	96	98	99	9B	9D	A0
[8]	A4	A5	A6	A7	A9	AA	AC	AD	B2	B4
[9]	B7	B8	B9	BA	BE	BF	C0	C1	C4	C8
[10]	C9	CE	CF	D0	D6	D7	DA	DC	DD	DE
[11]	E2	E3	E5	E6	E7	E9	EA	EB	EE	F0
[12]	F1	F4	F5	F6	F8	FB	FD	FE	FF	

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

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

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. 4, в которой стартовая матрица выделена затенением).

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.

Таблица 4. Стартовая таблица

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

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

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

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

$$V_{k+1} = 10001011 . \tag{12}$$

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. 5.

Таблица 5. Графический способ вычисления произведения (11)

φ→	1	0	0	1	0	1	1	0	1
	Метки								
		8	7	6	5	4	3	2	1
8									
7									
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 звездочками в табл. 5, 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. 4, дает возможность правильно вычислить V_{k+1} для всех входных векторов V_k, у которых номер старшего разряда, содержащего 1, не превышает 6, а в общем случае – не превышает значения разности $n-m$ степеней НП φ_n и ОЭ ω_m.

На втором этапе синтеза матрицы $M_8^{(111)}$ нам остается уточнить значения элементов в седьмой и восьмой строках табл. 4. С этой целью отметим сначала звездочками нижние семь строк стартовой матрицы, сформировав тем самым входной вектор $V_k = 1111111$. По формуле (11) аналитически находим вектор V_{k+1}, равный 01010000. Если провести поразрядное сложение элементов строк табл. 4 с первой по седьмую (воспользовавшись графическим способом), приходим к вектору $V_{k+1}^* = 10111101$. Вычислив невязку векторов $\varepsilon = V_{k+1} \oplus V_{k+1}^*$, получим вектор $\varepsilon = 11101101$. Поместив невязку ε в седьмую строку матрицы $M_8^{(111)}$, устраняем расхождение между аналитической и графической оценками вектора V_{k+1} (табл. 6).

Таблица 6. К вычислению седьмой строки матрицы $M_8^{(111)}$

φ→	1	0	0	1	0	1	1	0	1
	Метк и								
		8	7	6	5	4	3	2	1
8									
7	*	1	1	1	0	1	1	0	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. 6, 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, 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) называют матрицами 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

$$f_k = \oplus_{i=1}^{n} \varepsilon_{i,k} \cdot i, \quad k = \overline{1, n}, \tag{15}$$

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. 7. Такие ЛРС-генераторы ПСП носят названия генераторов по схемам Галуа и Фибоначчи соответственно.

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

$$\varphi_8 = 1u_8u_7u_6u_5u_4u_3u_2 1,$$

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

Таблица 7. Функции возбуждения триггеров генераторов ПСП

f_k		G – генератор ПСП		F – генератор ПСП
1		$1\oplus7\oplus8$		$1\oplus2\oplus3\oplus4\oplus6\oplus7\oplus8$
2		$1\oplus2\oplus8$		$1\oplus2\oplus3\oplus5\oplus6\oplus8$
3		$1\oplus2\oplus3\oplus7\oplus8$		$1\oplus2\oplus3$
4		$2\oplus3\oplus4\oplus7$		$2\oplus3\oplus4$
5		$3\oplus4\oplus5\oplus8$		$3\oplus4\oplus5$
6		$4\oplus5\oplus6\oplus7\oplus8$		$4\oplus5\oplus6$
7		$5\oplus6\oplus7\oplus8$		$5\oplus6\oplus7$
8		$6\oplus7\oplus8$		$6\oplus7\oplus8$

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

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

и

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

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.

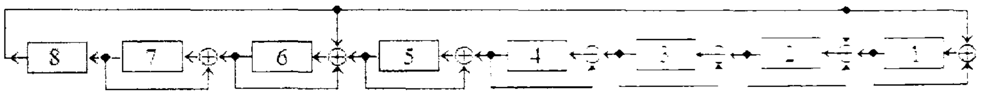

Рисунок 1 – Структурная схема ЛРС по схеме Галуа

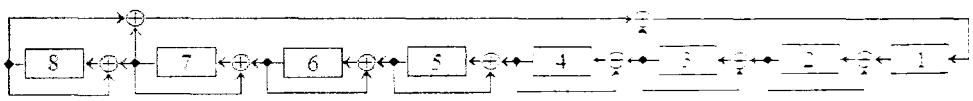

Рисунок 2 – Структурная схема ЛРС по схеме Фибоначчи

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

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

где x и y есть входной и выходной байты преобразования соответственно; x^{-1} – байт, мультипликативно обратный байту x по модулю примитивного над ОЭ $\omega = 11$ полинома (2); 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.

Синтез односторонних функцій

Один из подходов к формированию односторонних функций (ОФ) на основе двоичных примитивных матриц M изложен в [3]. Суть протокола обмена данными по открытому каналу связи между двумя абонентами компьютерной сети (Алисой) A и (Бобом) B, в ходе которой образуется секретный ключ криптографической защиты информации K, сводится к следующему. Пусть V и M - открытые n-битная вектор-строка (вектор инициализации) и примитивная матрица порядка n соответственно. Абонент A вырабатывает случайный показатель x, вычисляет вектор $V_a=V\cdot M^x$ и посылает его абоненту B. В свою очередь абонент B вырабатывает случайный показатель y, вычисляет вектор $V_b=V\cdot M^y$ и посылает его абоненту A. Затем Алиса вычисляет ключ $K_a=V_b\cdot M^x$, а Боб вычисляет ключ $K_b=V_a\cdot M^y$. Вполне очевидно, что по завершении протокола оба абонента будут располагать одним и тем же секретным ключом K, так как

$$K_a=V\cdot M^y\cdot M^x=K_b=V\cdot M^x\cdot M^y=K . \qquad (20)$$

Появлению данного протокола обмена секретными ключами по открытому каналу связи предшествовал матричный алгоритм формирования ключей шифрования [4], основная идея которого состоит в следующем. Если X, Y – векторы, представляющие соответственно открытый и зашифрованный текст, а M - шифрующая матрица, то зашифрование задается уравнением $Y=M\cdot X$, а расшифрование – уравнением $X=M^{-1}\cdot Y$. Для обмена сеансовыми ключами в системе авторы (Ерош и Скуратов) предлагают использовать протокол Диффи – Хэллмана в циклической группе матриц $\langle M\rangle$, причем матрица считается общедоступной. Предполагается, что пользователь A вырабатывает случайный показатель x, вычисляет матрицу M^x и посылает ее пользователю B. В свою очередь пользователь B вырабатывает случайный показатель y, вычисляет матрицу M^y и посылает ее пользователю A. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу (ключ шифрования) $M^{xy}=M^{yx}$. Поскольку мощность мультипликативной группы, образующим элементом которой являются невырожденные примитивные двоичные матрицы M (рекомендуемый порядок должен быть не менее чем 100), велико, то вычисление ключа, как утверждают авторы (кстати, без доказательства), имеет переборную сложность. Как показано в [5], изложенный выше алгоритм не обеспечивает заявленной стойкости шифрования, а ключ достаточно легко взламывается.

Протокол формирования ключей шифрования Мегрелишвили [3], кратко представленный соотношением (20), наследует некоторые черты алгоритма Ероша-Скуратова [4], поэтому вопрос его криптостойкости остается открытым.

Предлагаемый алгоритм формирования ОФ основан на применении обобщенных ПрП. Идея алгоритма построения ОФ состоит в следующем. В качестве открытых ключей принимаются двоичный $n-$разрядный вектор инициализации V и произвольный НП φ_n. Каждый из абонентов A и B вырабатывают по два секретных ключа, которые обозначим $(\omega_\alpha, P_\alpha)$ и (ω_β, P_β) соответственно, где $P-$перестановочные матрицы $n-$го порядка. Параметры ω являются случайными $n-$битными числами. На основании НП φ_n и ОЭ ω Алиса и Боб вычисляют примитивные матрицы Галуа, которые обозначим $G_{\omega,\alpha}$ и $G_{\omega,\beta}$, а затем с помощью секретного ключа P формируют подобные матрицы $G_\alpha = P_\alpha \cdot G_{\omega,\alpha} \cdot P^{-1}$ и $G_\beta = P_\beta \cdot G_{\omega,\beta} \cdot P^{-1}$ соответственно. Алиса определяет вектор $V_\alpha = V \cdot G_\alpha$ и посылает его Бобу. В свою очередь Боб определяет вектор $V_\beta = V \cdot G_\beta$ и посылает его Алисе. Затем Алиса вычисляет ключ $K_\alpha = V_\beta \cdot G_\alpha$, а Боб – ключ $K_\beta = V_\alpha \cdot G_\beta$. В силу того, что произведение матриц Галуа коммутативное, у обоих абонентов появляется общий секретный ключ K, так как $K_\alpha = K_\beta$.

Относительно предлагаемого алгоритма формирования ОФ можно выдвинуть гипотезу, что единственной для него атакой является лобовая атака. Криптостойкость данной ОФ можно усилить за счет ведения еще одного (третьего) ключа шифрования, с помощью которого Алиса и Боб образуют так называемые полиномиальные G^*_α и G^*_β матрицы соответственно. Алгоритм построения таких матриц состоит в следующем. Алиса выбирает примитивный над ОЭ ω_α полиномом $\varphi^*_n(x)$, отличный от полинома $\varphi_n(x)$ и замещает в полиноме $\varphi^*_n(x)$ аргумент x матрицей G_α, формируя тем самым полиномиальную матрицу G^*_α. Аналогичным образом поступает также и Боб. Матрицы G^*_α и G^*_β оказываются коммутативными и примитивными и, следовательно, могут быть задействованы в протоколе формирования закрытых ключей шифрования.

Все три рассмотренных выше ОФ относятся к подклассу матричных односторонних функций. Кратко проанализируем их криптостойкость. Алгоритм Ероша-Скуратова основан на использовании двух ключей: открытой матрицы M и секретных показателей x и y абонентов A и B соответственно. Противнику доступны как матрица M, так и матрицы M^x и M^y. А это дает возможность, как показал Ростовцев [5], по китайской теореме об остатках достаточно легко взломать ключ шифрования M^{xy}. В алгоритме Мегрелишвили [3] для построения односторонней функции задействованы уже три ключа, причем два из них являются открытыми: вектор инициализации V и матрица M той же размерности, что и вектор V. Закрытым ключом являются случайные показатели x и y абонентов A и B соответственно. Кроме открытых ключей противнику доступны векторы $V_a = V \cdot M^x$ и $V_b = V \cdot M^y$, содержащие информацию о матрицах M^x и M^y, что, на основании простоты взлома протокола Ероша-Скуратова, дает основание усомниться в возможности обеспечения экспоненциальной сложности его взлома. Наши сомнения базируются на следующих предположениях. Поскольку вектор V и матрица M являются общедоступными данными, то на основании перехваченных векторов V_a и V_b противник, воспользовавшись китайской теоремой об остатках, может вычислить показатели x, y и, тем самым, взломать ключ шифрования. Такие опасения вполне оправданы, так как существуют лишь единственные значения x и y, которые связывают открытые и перехваченные данные.

И, наконец, в предлагаемой односторонней функции, основанной на применении обобщенных ПрП, протокол формирования секретного ключа шифрования в открытых каналах связи, базируется на применении четырех ключей. В качестве открытых ключей выступают n-битный вектор инициализации V и любой неприводимый полином φ_n степени n. Секретными являются n-размерные ключи $(\omega_\alpha, P_\alpha)$ и (ω_β, P_β) абонентов A и B соответственно. Передаваемая по открытым каналам связи информация (векторы V_α и V_β) гораздо более сложно (и не однозначно) связана с открытыми ключами (по сравнению с протоколами Ероша-Скуратова и Мегрелишвили).

На основании проведенного анализа можно выдвинуть гипотезу о том, что предлагаемый протокол формирования ключей шифрования обладает криптостойкостью, достаточно близкой к экспоненциальной.

Выводы

Основной результат данной работы состоит в том, что в ней введена новая алгебраическая структура, названная *обобщенным примитивным полиномом*, расширяющая представление о классических примитивных полиномах. Понятие обобщенного ПрП корреспондируется с циклической группой $\langle\omega_m\rangle$, образуемой степенями такого двоичного полинома $\omega_m(x)$ степени m по модулю двоичного неприводимого полинома $\varphi_n(x)$, который доставляет последовательности $\langle\omega_m\rangle$ свойство m-последовательности. 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 $L_n = 2^n - 1$.

Кроме того, получен 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. И, наконец, на основании обобщенных ПрП предложена простая в программной и аппаратной реализации криптостойкая односторонняя функция.

Список литературы

1. csrc.nist.gov/publications/fips/fips197/fips-197.pdf
2. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля / Под ред. М.А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.
3. 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.
4. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / Ерош И.Л., Скуратов В.В. // Проблемы информационной безопасности. Компьютерные системы. 2004, №1, с. 72-78.

5. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова)/http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/ Erosh_Skuratov.pdf

Рецензент: Шелест М.Є
Надійшла 12.09.2011

УДК: 004.056.5 **Карпінець В. В., Яремчук Ю. Є.**

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ

Вступ

На сьогодні графічні цифрові зображення векторного формату дуже широко використовуються для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв'язку з цим актуальною стає задача захисту векторних зображень. При цьому особливий інтерес викликає таке забезпечення захисту, для якого не потрібно наявності оригіналу для підтвердження авторства.

Ця задача вирішується методами вбудовування цифрових водяних знаків (ЦВЗ) у зображення [1]. Серед них найбільшого поширення отримали методи, які базуються на частотних перетвореннях. До таких методів відносяться методи Базіна-Барса-Маделана, Хе-Жу-Ванга, Солачідіса-Ніколаїдіса-Пітаса [2], а також метод Войта-Янга-Буша [3], який забезпечує зменшення впливу ЦВЗ при його вбудовуванні на якість зображення, однак сумарна похибка відхилення координат точок відносно оригіналу в деяких випадках є досить суттєвою.

В роботі [4] запропоновано метод, який забезпечує зменшення сумарної похибки відхилення координат точок від оригіналу. Однак, в деяких випадках максимальне відхилення точок досягає великих значень, яке може призвести до помітних спотворень окремих точок [5]. В зв'язку з цим, певний інтерес викликає метод, представлений в роботі [6], в якому для забезпеченням зменшення впливу його вбудовування на відхилення точок зображення вбудовування бітів ЦВЗ здійснюється лише у ті матриці коефіцієнтів дискретного косинусного перетворення (ДКП), зміна яких не призводить до таких відхилень. Для визначення придатних для вбудовування матриць запропоновано умови відбору, з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Це дало можливість зменшити рівень спотворення векторних зображень до 20 разів порівняно з відомим методом Войта-Янга-Буша. Однак, при цьому залишається питання як змінилася обчислювальна складність запропонованого методу.

Тому актуальним є аналіз обчислювальної складності запропонованого методу методу та порівняння з відомим методом.

Аналіз обчислювальної складності методу вбудовування ЦВЗ у векторні зображення на основі двовимірного ДКП

Проведемо дослідження обчислювальної складності запропонованого методу. Обчислювальна складність буде визначатися як O :

$$O = O_{вбуд.} + O_{вит.}, \tag{1}$$

де $O_{вбуд.}$ та $O_{вит.}$ – обчислювальна складність вбудовування та витягування ЦВЗ відповідно.