ISSN 1512-1232

ОРИГИНАЛЬНАЯ МАТРИЧНАЯ ОДНОНАПРАВЛЕННАЯ ФУНКЦИЯ И ГЕНЕРАЦИЯ НОВОЙ МУЛЬТИПЛИКАТИВНОЙ ЦИКЛИЧЕСКОЙ МАТРИЧНОЙ ГРУППЫ ВЫСОКОГО ПОРЯДКА

Ричард Мегрелишвили[1], София Шенгелия[2].

[1] Тбилисский государственный университет им. И.Джавахишвили, ул. Университетская, 13. Тбилиси, 0186, Грузия, тел. (+995 595) 55 91 59. E-mail: richard.megrelishvili@tsu.ge
[2] Сухумский государственный университет, ул. Джикия 9. Тбилиси, 0186, Грузия, тел. (+995 599) 29 22 46.E-mail: sofia_shengelia@mail.ru

Аннотация

Целью настоящей работы является обоснование нового оригинального быстродействующего матричного алгоритма обмена ключами по открытому каналу. По замыслу, быстродействие нового алгоритма должно быть примерно таким, как у известных криптографических алгоритмов шифрации и дешифрации симметричных систем. Достижение заданной цели, очевидно, связанно с существующими глобальными проблемами, так как в настоящее время нет действующих ассиметричных систем, обладающих быстродействием, подобным быстродействию симметричных систем. Иначе говоря, в настоящее время нет криптогрофических систем, которые одновременно выполняли бы обе задачи – осуществляли обмен ключами по открытому каналу (без применения закрытого канала) и – обладали бы таким же высоким быстродействием, как у симметричных систем. Причина полностью кроется в самых однонаправленных функциях, которые служат основой реализации существующих ассиметричных систем. Из вышесказанного следует вся сложность и важность построения и обоснования новой оригинальной однонаправленной матричной функции и алгоритмов, исследуемых в настоящей работе.

Ключевые слова : *Открытый канал, обмен ключами, однонаправленная функция, поле GF(2)*

Введение

Впервые матричная однонаправленная функция была зафиксированна в работе [1], в которой она была представлена как операция умножения вектора на матрицу. На основе этой матричной однонаправленной функции в той же работе [1] впервые был также описан алгоритм обмена ключами по открытому каналу (алгоритм – альтернативный протоколу Диффи-Хеллмана [2]). Дальнейшие результаты были опубликованы в последующих работах, например, [3-7]. Ответ на вопрос о быстродействии матричной однонаправленной функции, вынесенный в раздел Аннотации настоящей работы, непосредственно следует из ответа на вопрос о том, - из каких операций состоит сама матричная однонаправленная функция? По мнению авторов, после ознакомления с последующим разделом не должно быть сомнений как о высоком быстродействии самой матричной однонаправленной функции, так о быстродействии алгоритма обмена ключами по открытому каналу, исследующихся в данной работе.

Построение циклических мультипликативных групп из исходных n x n матриц

В предшествующем разделе показано, что для осуществления алгоритма обмена ключами обязательным фактором является наличие множества n x n матриц высокой мощности, которые в тоже время коммутативны. Коммутативность чисел в алгоритме Диффи-Хеллмана выполняется, можно сказать, естественно, в соответствии с (2), в то время,

как для нашего алгоритма, т.е. в соответствии с (1), построение коммутативных множеств Â для каждого значения размерности n является не простой задачей.
В данной работе предлагается эффективное и конструктивное решение. Свойства эффективности и конструктивности метода построения матриц заключается в следующем:

- Для каждой размерности n>1 исходная n x n матрица должна генерировать либо максимальное число матриц (2^n-1), либо это число должно быть числом Мерсена, т.е. 2^j-1, где j <n;
- Метод синтеза исходной n x n матрицы для любой размерности должен быть одинаковым (где n возможно реализуемая максимальная размерность исходных матриц, т.е. технология построения исходных матриц должна быть реализуемой и одинаковой для любой заданной размерности n.

Кроме вышесказанного, необходимо учитывать, что структура матриц не должна содержать внутриматричной рекурсии [3-7].

В начале изложения метода генерации матриц скажем, что к построению излагаемого метода авторы пришли во время исследования совершенно иной задачи. Предположим, что рассматривается задача определения примитивности элементов (1+α) в поле GF (2^n) по модулю циклического многочлена $p(x)=1+x^2+...+x^n$, где $p(\alpha)=0$.

Предположим теперь, что рассматриваются значения j-тых степеней элемента (1+α), при условии, что j<n. Тогда, получим следующую последовательность степеней элемента (1+α), с соответствующими элементами поля и векторами из V_n над полем GF(2):

$$
\begin{array}{ll}
(1+\alpha)^0 = 1 & (1000000...0) \\
(1+\alpha)^1 = 1+\alpha & (1100000...0) \\
(1+\alpha)^2 = 1+\alpha^2 & (1010000...0) \\
(1+\alpha)^3 = 1+\alpha+\alpha^2+\alpha^3 & (1111000...0) \\
(1+\alpha)^4 = 1+ \quad +\alpha^4 & (1000100...0) \\
(1+\alpha)^5 = 1+\alpha+ \quad +\alpha^4+\alpha^5 & (1100110...0) \\
\ldots & \ldots
\end{array} \tag{1}
$$

Структура, обозначенная формулой (1), не что иное как треугольник Серпинского , со всеми свойствами фрактальной структуры.

Определение 1. Предположим, что данной структуре (1) добавляется единичная строка в качестве первой строки, тогда получается полная фрактальная структура (рис.)

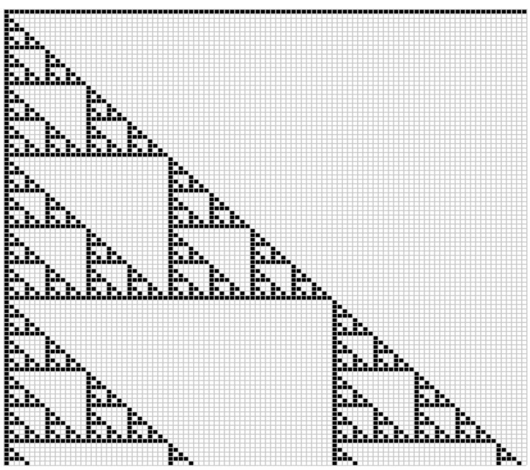

Рис. Полная фрактальная структура.

ISSN 1512-1232

Определение 2. Нормальной n x n матричной структурой называется матрица, образованная из первых n x n элементов, т.е. из первых n строк и первых n столбцов, полной фрактальной структуры.

Пример 1. Выражением (2) представляются нормальные матричные структуры размерности n = 2, 3, 4 полученные из полной фрактальной структуры:

$$A_1=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\ A_2=\begin{pmatrix}1 & 1 & 1\\ 1 & 0 & 0\\ 1 & 1 & 0\end{pmatrix},\ A_3=\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0\end{pmatrix} \qquad (2)$$

С помощью программного обеспечения были вычислены порядки е для исходных нормальных n x n матричных структур и полученные результаты представлены в таблице .

n	e	n	e	n	e	n	e	n	e	n	e
1	2^1-1	18	87381	35	2^{35}-1	52	2^{12}-1	69	2^{69}-1	86	2^{86}-1
2	2^2-1	19	2^{12}-1	36	2^9-1	53	2^{53}-1	70	2^{46}-1	87	2^{81}-1
3	2^3-1	20	2^{10}-1	37	2^{20}-1	54	2^{18}-1	71	2^{60}-1	88	2^{29}-1
4	2^3-1	21	2^7-1	38	2^{30}-1	55	2^{36}-1	72	2^{14}-1	89	2^{89}-1
5	2^5-1	22	2^{12}-1	39	2^{39}-1	56	2^{14}-1	73	2^{42}-1	90	2^{90}-1
6	2^6-1	23	2^{23}-1	40	2^{27}-1	57	2^{44}-1	74	2^{74}-1	91	2^{60}-1
7	2^4-1	24	2^{21}-1	41	2^{41}-1	58	2^{12}-1	75	2^{15}-1	92	2^{18}-1
8	2^4-1	25	2^8-1	42	2^8-1	59	2^{24}-1	76	2^{24}-1	93	2^{40}-1
9	2^9-1	26	2^{26}-1	43	2^{28}-1	60	2^{55}-1	77	2^{20}-1	94	2^{18}-1
10	2^6-1	27	2^{20}-1	44	2^{11}-1	61	2^{20}-1	78	2^{26}-1	95	2^{95}-1
11	2^{11}-1	28	2^9-1	45	2^{12}-1	62	2^{50}-1	79	2^{52}-1	96	2^{48}-1
12	2^{10}-1	29	2^{29}-1	46	2^{10}-1	63	2^7-1	80	2^{33}-1	97	2^{12}-1
13	2^9-1	30	2^{30}-1	47	2^{36}-1	64	2^7-1	81	2^{81}-1	98	2^{98}-1
14	2^{14}-1	31	2^6-1	48	2^{24}-1	65	2^{65}-1	82	2^{20}-1	99	2^{99}-1
15	2^5-1	32	2^6-1	49	2^{15}-1	66	2^{18}-1	83	2^{83}-1	100	2^{33}-1
16	2^5-1	33	2^{33}-1	50	2^{50}-1	67	2^{36}-1	84	2^{78}-1	101	2^{84}-1
17	2^{12}-1	34	2^{22}-1	51	2^{51}-1	68	2^{34}-1	85	2^9-1	102	2^{10}-1

Таблица . Результаты вычисления порядков е для исходных нормальных n x n матриц.

Из анализа данных, представленных в таблице, приходим к таким выводам.

Во-первых, подтверждается оценка относительно порядка матрицы *e* , заданная соотношением, равным числу Мерсена $e_n=2^m-1$, где $m\leq n$ (исключение проявляется лишь в точке $n = 18$, в которой $e_{18}=87381$).

Во-вторых, существуют такие значения размерности *n* (в табл. они выделены затенением), для которых элементы групп, порождаемые степенями матриц $\hat{A}$, составляют последовательность максимальной длины, равной 2^n-1.

В-третьих, для каждой смежной пары значений (n, $n+1$) , расположенных на границе изменения разрядности r (т. е. на границе перехода от r к ($r+1$) числам), оценки e_n и e_{n+1} совпадают. Такими парами в табл. являются смежные числа (3, 4),(7, 8), (15, 16),(31, 32) и (63,64). Аналитически порядок циклических групп, указанных пар смежных значений *n,* можно представить выражением:

$$e_{2^r-1}=e_{2^r}=2^{r+1}-1 , \qquad (3)$$

где, $r\geq 2$.

И, наконец, в- четвертых, следует заметить, что, не принимая во внимание указанных замечаний, полученные результаты полностью совпадают (для матриц любой размерности) с результатами, полученными в работе [8], хотя хорошо известно, что в работе [8] исходными матрицами являются совершенно иные структуры, т.е. структуры,

ISSN 1512-1232

которые получены из обобщенных кодов Грея . Отметим также, что порядок матриц в таблице установлен с помощью последовательного вычисления всех степеней до размерности n = 63 исходной матрицы; для размерности же n>63 вычисление порядка е осуществлялось с использованием специальной программы.

Литература:

1. R.Megrelishvili, M. Chelidze, K. Chelidze, On the construction of secret and public-key cryptosystems, Iv. Javakhishvili Tbilisi State University I.Vekua Institute of Applied Mathematics, Applied Mathematics, Informatics and Mechanics, AMIM, v.11, N2, 2006, pp. 29-36.
2. Diffie W. and Hellman M. E. New Directions in Cryptography . IEEE Transactions on Information Theory. V. IT-22, n.6, Nov, 1976, pp. 644-654
3. R . Megrelishvili, A . Sikharulidze , New matrix-set generation and the cryptosystems, Proceedings of the European Computing conference and 3rd International Conference on Computational Intelligence, Tbilisi, Georgia, June 26-28, 2009, pp. 253-256
4. R. Megrelishvili, M.Chelidze , G. Besiashvili , Investigation of new matrix-key function for the public cryptosystems, The Third International Conference "Problems of Cybernetics and Information", September 6-8, 2010, Baku, Azerbaijan, Section N1, "Information and Communication Technologies", 2010, pp. 75-78.
5. Р. Мегрелишвили, М. Челидзе, Г. Бесиашвили, Однонаправленная матричная функция - быстродействующий аналог протокола Диффи-Хеллмана, Седмая международная научно-практическая конференция," Интернет – Образование – Наука -2010" Винница, Украина, 28 сентября - 3 октября, 2010, стр. 341-344.
6. R . Megrelishvili, G . Besiashivli, S . Shengelia, New one-way matrix function and public key-exchange, Proceedings of International Conference SAIT 2011, System Analysis and Information Technologies, Kyiv, Ukraine, May 23-28, 2011, p. 407.
7. Richard Megrelishvili, Gela Besiashvili, Sofia Shengelia, Original one-way cryptography function using n x n matrices, Proceedings of the 11th International Conference, Pattern Recognition and Information Processing, PRIP 2011, (18-20 May 2011), Minsk, Belarus, 2011, pp. 355-357.
8. А. Я. Белецкий, Д. А. Стеценко, Порядок абелевых циклических групп, порождаемых обобщенными преобразования Грея, Электроника и системы управления сигналов, N1(23), 2010,сс. 5-11.

_

Article received: 2012-12-10