ISSN 1512-1232

Семейство фракталов из ленточных матриц

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 построение матричного множества высокой мощности для имплементации быстродействующего асимметричного 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. В современной асимметричной криптографии характерно использование алгоритмов , предполагающих использование необходимых вычислительных средств. Известен ряд проверенных алгоритмов , которые при использовании ключа, достаточной длины,криптографически стойки и рационально реализованы, однако нет алгоритмов с впечатляющим и значительным свойством асимметричных систем и, одновременно, с быстродействием, подобным. как у симметричных методов шифрования. Целью настоящей работы является именно исследование вопросов генерации матричных множеств для решения, в целом, указанной задачи с применением оригинального алгоритма однонаправленной матричной функции.

Ключевые слова: *обмен ключами по открытому каналу, однонаправленная матричная функция, поле GF(2), фракталы.*

Введение

Впервые матричная однонаправленная функция была зафиксированна в работе [1], в которой она была представлена как операции 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, [3-9]. 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, исследующейся в данной работе.

Алгоритм обмена ключами по открытому каналу связи

ISSN 1512-1232

Для осуществления матричной функции задается n x n матрица A'. Для простаты изложения матрицы рассматриваются над полем GF(2). Матрица A' представляет собой секретный параметр, выбранный случайным образом из множества Â высокой мощности; т.е. A' Є Â, v Є V_n, где V_n векторное пространство над GF(2). Тогда, однонаправленная матричная функция имеет следующий вид:

$$vA = u , \quad (1)$$

где u Є V_n и u – открытый параметр.

Заметим, что если для алгоритма Диффи-Хеллмана однонаправленная функция

$$a^x = y \pmod p \quad (2)$$

основано на проблеме дискретного логарифма, то для функции (1) определенной проблемой является внутриматричная рекурсия. Этот вопрос был достаточно подробно исследован в работах [3-9]. Кроме того, относительно матричной функции (1) проблема может исходить из обычных методов линейной алгебры, в особенности когда множество Â рассматривается в виде конечномерной алгебры с мультипликативным базисом. Анализ этих вопросов был дан в работе [9], согласно которой в функции (1) вектор v представляет секретный параметр, т.е. v = k, где k – ключ, полученный в результате применения алгоритма Диффи-Хеллмана с тем, чтобы функция (1) функционировала, как однонаправленная функция в течение определенного периода времени (по аналогии с алгоритмом ЭльГамаля [10]).

Относительно быстродействия функций (1) и (2), можно судить, как было отмечено выше, по характеру операций данных функций. Функция (1) принципиально отличается от функции (2) тем, что для функции (1) используется операция умножения, в то время, как функция (2) – экспоненциальная функция.

Матричный алгоритм обмена ключами по открытому каналу осуществляется следующим образом:

- Алиса (случайно) выбирает n × n матрицу A_1 Є Â и посылает Бобу вектор

$$u_1 = vA_1 . \quad (3)$$

- Боб (случайно) выбирает n × n матрицу A_2 Є Âи посылает Алисе вектор

$$u_2 = vA_2 . \quad (4)$$

где α - n -размерный вектор (открытый), A_1 и A_2 суть (секретные) матричные ключи.

- Алиса вычисляет

$$k_1 = u_2A_1 , \quad (5)$$

- Боб вычисляет

ISSN 1512-1232

$$k_2 = u_1 A_2 \quad (6)$$

где k_1 и k_2 секретные ключи. $k_1 = k_2 = \mathrm{k}$ потому, что $k = vA_1A_2 = vA_2A_1$.

Фракталы

Фракталы — это прежде всего язык геометрии. Однако их главные элементы недоступны непосредственному наблюдению. В этом отношении они принципиально отличаются от привычных объектов евклидовой геометрии, таких, как прямая линия или окружность. Фракталы выражаются не в первичных геометрических формах, а в алгоритмах, наборах математических процедур. Эти алгоритмы трансформируются в геометрические формы с помощью компьютера. Репертуар алгоритмических элементов неисчерпаем. Овладев языком фракталов, можно описать форму облака так же чётко и просто, как архитектор описывает здание с помощью чертежей, в которых применяется язык традиционной геометрии.

Семейство фракталов

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 [3-9].

Во время исследования этой задачи мы обнаружили новое семейство фракталов из ленточных матриц (см. рис.)

ISSN 1512-1232

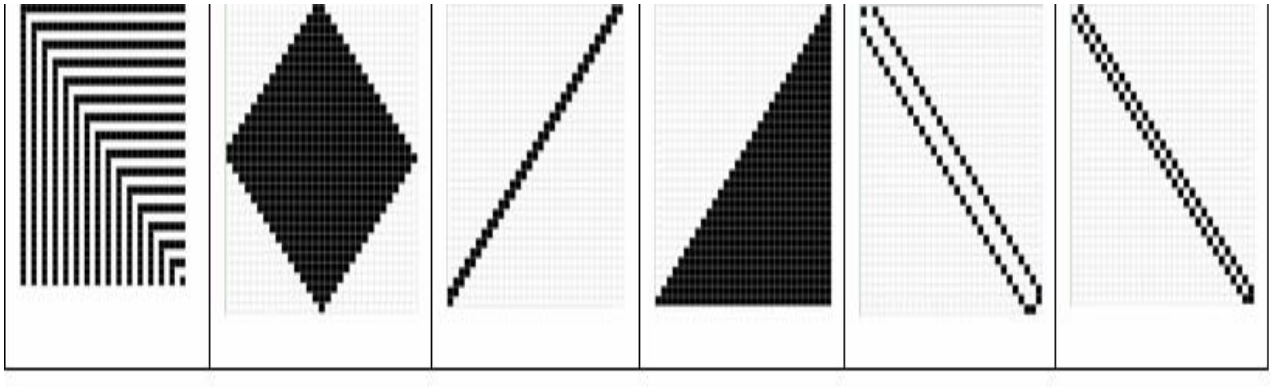
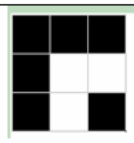
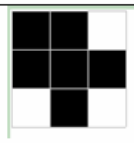
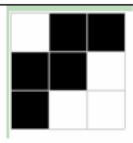
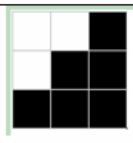
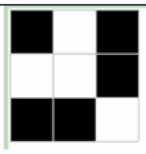
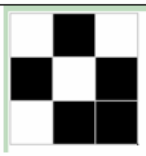


Рис. Семейство фракталов

Определение 1. 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, фрактальной структуры.

Пример 1. Выражением **(7)** представляются нормальные исходные матричные структуры размерности n = 3, полученные из нормальных фрактальных структур :

3x3						
A	$\begin{pmatrix}1&1&1\\1&0&0\\1&0&1\end{pmatrix}$	$\begin{pmatrix}1&1&0\\1&1&1\\0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&1\\1&1&0\\1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$	$\begin{pmatrix}1&0&1\\0&0&1\\1&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0\\1&0&1\\0&1&1\end{pmatrix}$

(7)

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

ISSN 1512-1232

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 e для исходных нормальных n x n матриц.

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

Во-первых, подтверждается оценка относительно порядка e_n матриц размерности n, заданная соотношением, равным числу Мерсена $e_n=2^m-1$, где $m \le n$ (имеются в выду оценки значения порядков e_n матриц размерности n, полученные в предшествующих работах; 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 Â , 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:

$$e_{2^r-1}=e_{2^r}=2^{r+1}-1 , \qquad (8)$$

где, $r \ge 2$.

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 [11], хотя хорошо известно, что в работе [11] исходными матрицами являются совершенно иные структуры, т.е. структуры, 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 e осуществлялось с использованием специальной программы.

ISSN 1512-1232

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. W.Diffie and M.E.Hellman, 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. R. Megrelishvili, G. Besiashvili, S.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. R. P. Megrelishvili, New direction in construction of matrix one-way function and tropical cryptography, Archil Eliashvili Institute of Control Systems of the Georgian Technical University Proceedings, No 16, 2012, pp, 244-248.
9. R.P.Megrelishvili, Analysis of the matrix one-way function and two variants of its implementation, International J. of Multidisciplinary Research And Advances In Engineering (IJMRAE), v. 5, n. IV (October 2013), pp. 99-105.
10. T.ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472
11. 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.

Статья получена: 2014-02-19