Р.П. МЕГРЕЛИШВИЛИ [1], М.А. ЧЕЛИДЗЕ [2], Г.М. БЕСИАШВИЛИ [1], М.В. ДЖИНЖИХАДЗЕ[3]

ПОСТРОЕНИЕ НОВОЙ ОДНОНАПРАВЛЕННОЙ МАТРИЧНОЙ ФУНКЦИЙ И ЕЁ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

[1]Им. Ив. Джавахишвили Тбилисский государственный университет,
ул. Университетская, 3, Тбилиси, 0143, Грузия, тел.: (995-95) 55-91-59,
E-Mail: richard.megrelishvili@tsu.ge

[2]Сухумский государственный университет,
ул. Джикия, 9, Тбилиси, 0143, Грузия, тел.: (995-99) 11-55-42,
E-Mail: makho111@hotmail.com

[3]Им. Ак. Церетели Кутаисский государственный университет,
ул. Царицы Тамары, 59, Кутаиси, Грузия, тел.: (995-93) 19-85-62,
E-Mail: mjinji@yahoo.com

Аннотация. Рассматривается новый подход для построения однонаправленной криптографической функции на $n \times n$ матрицах, заданных над полем Галуа $GF(p)$ (для простоты изложения рассматривается поле $GF(2)$). Полученная функция может быть применена как быстродействующий аналог протокола Диффи-Хэллмана, а также для осуществления процесса шифрации-дешифрации по открытому каналу.

Abstract. In this article is investigate new cryptography matrix-one-way function on $n \times n$ matrices over the Galois field $GF(2)$. The idea is that these construction must perform the same functions as in the well-known algorithms operating via an open channel. Here, in the first place we mean the Diffie-Hellman protocol and, also, the algorithms of message encryption-decryption etc.

Ключевые слова: криптография, открытый канал, матричный ключ, атака с открытым текстом, матричные преобразования, поля Галуа $GF(q)$.

ВВЕДЕНИЕ

Известно, что асимметричные криптографические системы, имея существенные преимущества перед симметричными системами, в тоже время, значительно уступают им в быстродействии. В данной работе рассматривается новый подход построения криптосистем для открытого канала с более скоростными свойствами функционирования.

Основная цель работы состоит в исследовании возможности построения новой однонаправленной функции на матрицах и исследовании новых матричных структур для построения соответствующих конструктивных криптографических методов и алгоритмов. По идее эти построения должны выполнять те задачи, которые выполняются в известных алгоритмах, действующих по открытому каналу. Здесь, в первую очередь, имеются в виду протокол Диффи-Хэллмана, и – намерение того, что на матрицах получить функциональные схемы шифраций-дешифраций. Идея эта не новая, хотя она была применена в ином исполнении еще в работе [8], и по имеющимся данным вновь вызывает интерес в научных кругах [5,6]. Оправдание предпринимаемых усилий, видимо, надо видеть в быстродействии схемных и программных решений матричных структур [7].

Ниже исследуется отличный от [4-6] подход построения однонаправленной функции на коммутативных матрицах. При этом построении рассматриваются также две проблемы: проблема о внутри-матричной рекуррентной зависимости и проблема конструктивного построения исходных матриц, необходимых для генерации матричной коммутативной мультипликативной группы $\mathcal{A}$ высокого порядка, при заданной $n \times n$ размерности над $GF(p)$.

ОДНОНАПРАВЛЕННАЯ МАТРИЧНАЯ ФУНКЦИЯ И АЛГОРИТМ, АНАЛОГИЧНЫЙ ПРОТОКОЛУ ДИФФИ-ХЭЛЛМАНА

Для осуществления однонаправленной функции и алгоритма обмена ключами по открытому каналу задается исходная $n \times n$ матрица A (матрица A открыта), которая генерирует мультипликативную группу коммутативных матриц высокой мощности $\mathcal{A}$ (см. Разделы 3 и 4).

Матричный алгоритм обмена ключами по открытому каналу осуществляется следующим образом:

• Алиса (случайно) выбирает $n \times n$ матрицу $A_1 \in \mathbb{A}$ и посылает Бобу вектор $b = aA_1$;

• Боб(случайно) выбирает $n \times n$ матрицу $A_2 \in \mathbb{A}$ и посылает Алисе вектор $c = aA_2$, где a - n-мерный вектор (открытый), A_1 и A_2 суть (секретные) матричные ключи.

• Алиса вычисляет $k_1 = cA_1$.

• Боб вычисляет $k_2 = bA_2$,

где $k_1 = k_2 = k$ (k - общий секретный ключ) потому, что $k = aA_1A_2 = aA_2A_1$.

Из последних соотношений явствует важность коммутативности множества $\mathbb{A}$ при его генерации. Однако, из следующего раздела явствует, также, что такое внутри-матричная рекуррентная зависимость и какую опасность может она представлять для взлома генерируемых матриц.

МАТРИЦЫ С ВНУТРИ-МАТРИЧНОЙ РЕКУРРЕНТНОЙ ЗАВИСИМОСТЬЮ

Мы хотим обратить внимание на тот факт, что некоторые невырожденные матрицы имеют внутри-матричную рекуррентную зависимость. Эта зависимость имеется между строками или столбцами матриц. В тоже время она не является обычной линейной зависимостью. Потому-то подобные матрицы остаются невырожденными.

Матрицы таково вида легко вскрыть, если они используется в криптографических целях. Возможно, осуществить построение специальных классов с внутри-матричной рекуррентной зависимостью. Однако, в ряде случаев (в особенности при больших размерах матриц) обнаружение внутри-матричной рекуррентной зависимости остается непростой задачей.

Матрицы с внутри-матричной рекуррентной зависимостью можно построить с помощью поля Галуа $GF(p^n)$. Для простоты изложения это построение будем рассматривать как поле многочленов $GF(2^n)$ по модулю неприводимого многочлена $p(x)$. Например, мультипликативная группа поля $GF(2^3)$, образованная с помощью α, корня примитивного $p(x) = 1 + x + x^3$, имеет вид [3]:

$$\begin{aligned}
&\alpha^0 = 1 && -(100)\\
&\alpha^1 = \quad \alpha && -(010)\\
&\alpha^2 = \qquad \alpha^2 && -(001)\\
&\alpha^3 = 1 + \alpha && -(110)\\
&\alpha^4 = \quad \alpha + \alpha^2 && -(011)\\
&\alpha^5 = 1 + \alpha + \alpha^2 && -(111)\\
&\alpha^6 = 1 + \qquad \alpha^2 && -(101)\\
&\alpha^7 = 1
\end{aligned} \tag{1}$$

Мультипликативная группа (1) записана в виде степеней α, но при этом, также указываются соответствующие записи в виде многочленов от α и соответствующие им векторы, которые вместе с нулевым вектором составляют векторное пространство $V_{n=3}$ над полем $GF(2)$.

В соответствии с (1) можно записать, например, мультипликативную группу матриц A, A^2, $A^3, \ldots, A^7 = I$ (I единичная матрица):

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \ldots, \quad A^7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{2}$$

которая образована примитивной матрицей A, соответствующей элементу α (при этом (1) и (2)

изоморфны). Очевидно, что порядок каждой матрицы A^i совпадает с порядком элемента α^i (1).

Все матрицы A^i (2) имеют внутри-матричную рекуррентную зависимость, предопределенную многочленом $p(x)$. Покажем эту зависимость на примере $p(x) = 1 + x + x^3$. Любая матрица из (2) состоит из $n^2 = 9$ неизвестных:

$$A^i = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}. \tag{3}$$

Однако, с учетом внутри-рекуррентной зависимости, из (3) легко можно получить матрицу A_1^i с числом неизвестных, равным $n = 3$:

$$A_1^i = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{13} & x_{11} + x_{13} & x_{12} \\ x_{12} & x_{13} + x_{12} & x_{11} + x_{13} \end{pmatrix}. \tag{4}$$

Эту матрицу легко вскрыть даже при одноразовом криптографическом применении, например, при использовании её для осуществления операции умножения вектора на матрицу (имеется в виду, скажем, осуществление протокола Диффи-Хэллмана на матрицах; см. раздел 2). Например, матрица A (4) легко вскрывается, так как уравнение

$$aA = b \tag{5}$$

(при известных a и $b \in V_{n=3}$ над полем $GF(2)$ предоставляет возможность составить три линейных уравнения и найти x_{11}, x_{12}, x_{13} неизвестные).

Очевидно, что число матриц с внутри-рекуррентной зависимостью связано с числом неприводимых многочленов, используемых для построения $GF(2^n)$, а может быть и заметно больше. На наш взгляд вопрос этот существенен и поэтому рассматривается в следующем примере.

Для примера приведем отличное от (2) построение мультипликативной группы из матриц с периодом $e = 3$:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad A^3 = I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{6}$$

В матрицах A, A^2 и A^3 (6) наблюдаемая нами рекуррентная зависимость проявляется в ином виде. Она, также, связана с определенной последовательностью элементов из (1). Например, строки в матрице A (6) суть векторы, соответствующие элементам α^3, α^5, $\alpha^7 = \alpha^0$ (учитывая $\mathrm{mod}(e = 2^3 - 1 = 7)$) (1); в матрице A^2 (6) они являются векторами, соответствующими элементам α^2, α^6, $\alpha^{10} = \alpha^3$ (1); а в матрице A^3 (6) соответствуют элементам α^0, α^1, α^2 (1).

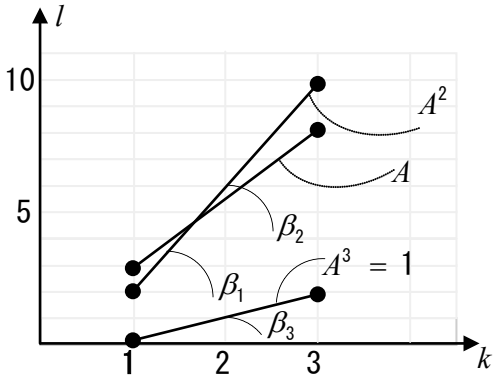

Рис. 1. $l = f(k)$ линейная зависимость для мультипликативной группы (6)

Следует заметить, что таких видоизмененных зависимостей, имеющих закономерный характер, видимо, не просто выявить и пересчитать. Однако, если рассмотренная зависимость $l = f(k)$ линейная, как в данном примере (6) (где l-показатель степени элемента поля α^l (1), а k-номер строки матрицы $k = 1,2,...,n$), то обнаружение подобной зависимости может оказаться относительно несложной задачей. Изображенная на рис.1 $l = f(k)$ зависимость для матриц группы (6) является линейной. Очевидно, что $l = f(k)$ зависимость для всех вышерассмотренных матриц, с внутри-матричной рекуррентной зависимостью, также линейная. Однако, в отличие от матриц (6) (см. рис.1.), для всех матриц вида (2) линейность одинаковая (т.е. β-постоянная величина) и легко обнаруживается. Поэтому внутри-матричная рекуррентная зависимость в них – тривиальная.

Резюмируя и обобщая вышерассмотренные результаты можно выделить три вида матриц с в внутри-матричными зависимостями:

- Множества матриц (например, (2)) с тривиальными внутри-матричнными зависимостями;
- Множества матриц (например, (5)) с линейными внутри-матричными зависимостями $l = f(k)$;
- Множества матриц (например, (7)), в которых внутри-матричнные зависимости не обнаруживаются.

В действительности не все матричные множества (группы) будут иметь $l = f(k)$ линейную зависимость. Например, матрицы мультипликативной группы, образованной исходной матрицей $A_{n=5}$ (7) (разд. 4), с периодом $e = 31$, не содержат вышерассмотренных внутри-матричных рекуррентных зависимостей.

ПОСТРОЕНИЕ МУЛЬТИПЛИКАТИВНЫХ ГРУПП ИЗ $n \times n$ МАТРИЦ

Наша цель – построить мультипликативную группу матриц, которая будет свободна от внутри-матричной рекуррентной зависимости. Кроме этого, каждая $n \times n$ исходная матрица должна быть примитивной, т.е. должна иметь максимальный порядок, равный $e = 2^n - 1$ и следовательно образовывать мультипликативную группу с максимальным периодом. Рассматриваемые матричные группы коммутативны. Для примера можно привести исходные матрицы (7). Основой для построения структур исходных матриц является определенная симметричность элементов и, в тоже время, асимметричность структур относительно диагоналей.

$$A_{n=5} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \; A_{n=7} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & & & & & & 0 \\ 0 & & & & & & 1 \\ 1 & & & A_{n=5} & & & 0 \\ 0 & & & & & & 1 \\ 1 & & & & & & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}, ..., \; A_n = \begin{pmatrix} 1 & 0 & 1 & 0 & . & . & 1 \\ 1 & & & & & & 0 \\ 0 & & & & & & 1 \\ . & & & A_{n-2} & & & . \\ . & & & & & & . \\ 1 & & & & & & 0 \\ 0 & 1 & 0 & 1 & .. & . & 0 \end{pmatrix}. \quad (7)$$

Исходная 5×5 матрица $A_{n=5}$, построена на базе матрицы $A_{n=3}$, которая окаймляется с помощью двоичной последовательности при соблюдении определенной закономерности. Следующая исходная матрица $A_{n=7}$ построена на базе матрицы $A_{n=5}$, т.е. для получения матрицы $A_{n=7}$ матрица $A_{n=5}$ также окаймляется последовательностью единиц и нулей по установленному порядку. Порядок этот остается в силе для получения исходной матрицы $A_{n=9}$ на базе матрицы $A_{n=7}$ и т.д. до $n\times n$ матрицы, где $n=2k-1$, $k>1$ целое число. Каждая $n\times n$ исходная матрица $A\in\mathbb{A}$ должна генерировать мультипликативную группу $A, A^2, A^3, \ldots, A^{2^n-1}=I$ (I единичная матрица), которая, при достаточно высокой размерности n ($n\approx150$), образует множество коммутативных матриц $\mathbb{A}$ (высокой мощности) для использования их в криптографических целях.

ВЫВОДЫ

В работе получены следующие основные результаты:

– Разработан новый метод построения однонаправленной функции на матрицах.

– С целью получения матриц с заданными свойствами исследован вопрос о внутри-матричных рекуррентных зависимостях. По проведенным исследованиям можно заключить, что возможно построение группы, генерируемых матриц, не содержащих внутри-рекурентных зависимостей.

– Разработаны алгоритмы построения специальных классов матричных множеств высокой мощности. В построении $n\times n$ матриц исходные матицы примитивны, с максимальным периодом, равным $e=2^n-1$. Мультипликативная группа генерируемых матриц коммутативна.

– С помощью полученного метода построения однонаправленной функции и исследования матричных структур, возможно построение криптосистем обмена ключами и шифрации-дешифрации, работающих исключительно только на матричных структурах.

СПИСОК ЛИТЕРАТУРЫ

1. Megrelishvili R., Sikharulidze A. New matrix-sets generation and the cryptosystems. Proceedings of the European Computing Conference and Proceedings of the 3rd International Conference on Computational Intelligence, Tbilisi, Georgia, June 26-28, 2009, pp. 253-253.
2. Megrelishvili R., Chelidze M., Besiashvili G. Investigation of new matrix-key function for the public cryptosystems. The Third International Conference “Problems of cybernetics and Information”, Volume 1, September 6-8, Baku, Azerbaijan, Section N1, “Information and Communication Technologies”, 2010, pp. 75-78.
3. Megrelishvili R., Chelidze M., Besiashvili G. Proceedings of the Seventh International Conference, INTERNET-EDUCATION-SCIENCE, IES-2010, 28 September-3 October, Vinnytsia, Ukraine, 2010, pp.341-344.
4. 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.
5. Белецкий А.Я., Стеценко Д.А. Порядок абелевых циклических групп, порождаемых обобщенными преобразованиями Грея. Електроніка на систем и управління, Теорія на методу оброблення сигналів. 2010, N1 (23), с. 5-11.
6. Ерош И.Л., Сергеев Н.Б. Скоростное шифрование разнородных сообщений. Сб. Трудов: Вопросы передачи и защиты информации. Санкт-Петербург, 2006, с. 133-155.
7. Schneier B. Applied cryptography. John Wiley and Sons. Inc. New York, 1996.
8. Hill. L.S. Cryptography in an Algebraic Alphabet. American Mathematical Monthly, v. 36, Jun-Jull 1929, pp. 306-312.

Надійшла до редакції 21.11.2010р.

МЕГРЕЛИШВИЛИ Р.П. – д.т.н., профессор, ассоциированный профессор Тбилисского государственного университета, направление компьютерных наук, Тбилиси, Грузия.

ЧЕЛИДЗЕ М.А. – д.а.н., ассоциированный профессор Сухумского государственного университета, направление компьютерных наук, Сухуми, Грузия.

БЕСИАШВИЛИ Г.М. – к.т.н., ассистент, профессор Тбилисского государственного университета, направление компьютерных наук, Тбилиси, Грузия

ДЖИНДЖИХАДЗЕ М.В. – докторант Тбилисского государственного университета, направление компьютерных наук, Тбилиси, Грузия.