Синтез криптографического метода посредством матриц над конечными полями

Р. П. Мегрелишвили, Д. З. Булавришвили, Т.В. Гнолидзе, М. Т. Махатадзе, В. А. Тогонидзе, Г. К. Хуцишвили
Проблемная лаборатория физической кибернетики,
Тбилисского Государственного Университета им. Ив. Джавахишвили

Абстракт
Исследуется отличный от метода Виженера матричный подход к построению симметричных криптографических систем защиты информации.

Введение

Криптографические методы, основанные на специальных матричных структурах, образуют отличную от методов Виженера систему, которая менее распространена и изучена [1,2]. Обычно, в обеих системах, слова, подлежащие шифрованию, представляются в виде векторов $a \in V_n$ - n-мерного векторного пространства над полем $GF(2)$ или многочленом $a(x)$ из алгебры классов вычетов многочленов A_n по модулю $f(x)$ над тем же конечным полем.

Криптограмма получается умножением вектора a на специальную матрицу A порядка n, а дешифрация зашифрованной информации b осуществляется умножением вектора b на A^{-1} - обратную для A матрицу, т.е.

$$aA=b; \qquad bA^{-1}=a\,. \tag{1}$$

При таком подходе, как и собственно для любых симметричных систем, основную проблему составляют вопросы формирования множества ключей – множества матриц (не поддающихся перебору в реальном масштабе времени, что определяет криптостойкость системы), а также – скорость осуществления шифрации-дешифрации и др.

Основная цель настоящей работы – синтез методов, осуществляющих алгоритмически несложное формирование и представление классов специальных невырожденных матриц порядка n (и обратных для них матриц), удовлетворяющих требованиям криптостойкости.

1. Общие методы формирования криптографических матричных ключей

Известны методы нахождения обратных для A матриц A^{-1} [3]. Построение обратной для $A=(a_{ij})_i^n$ (если она несингулярна) матрицы A^{-1} возможно, например в виде:

$$A^{-1} = \begin{bmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \dots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \dots & \frac{A_{n2}}{|A|} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \dots & \frac{A_{nn}}{|A|} \end{bmatrix}, \tag{2}$$

где A_{ij} - алгебраическое дополнение элемента a_{ij} матрицы A.

Несмотря на относительную простоту проведения операций над полями $GF(2)$, метод, связанный с реализацией (2), не может оказаться приемлемым для криптографического пользователя главным образом из-за невозможности представления обратных матриц в явном виде без выполнения достаточно сложных вычислений.

Необходимое решение не дается и посредством произведения матриц:

$$\begin{aligned} E_k\, E_{k-1} \;\dots\; E_1\, A &= I, \\ E_k\, E_{k-1} \;\dots\; E_1 &= A^{-1}, \end{aligned} \tag{3}$$

где A^{-1} - левая обратная матрица для матрицы A; $E_1,...,E_k$ - элементарные матрицы, с помощью которых матрицу A можно привести к каноническому виду и, следовательно, к единичному виду.

Для вычисления элементов x_1 , ... , x_n i-го столбца матрицы A^{-1}, исходя из равенства $A\,A^{-1} = I$, используют также решение системы уравнений:

$$a_{k1}x_1 + a_{k2}x_2 + ... + a_{kn}x_n = \begin{cases} 0, & \textit{если} \quad k \neq i; \\ 1, & \textit{если} \quad k = i; \end{cases} \tag{4}$$

где $k = 1, ... ,n$, и, как и прежде, $|A| \neq 0$.

Из алгебраической теории кодирования известно [4], что в алгебре A_n многочленов над полем $GF(q)$ по модулю многочлена $f(x)$ могут быть заданы классы базисных матриц G (размерности ($k \times n$)) и H (размерности ((n-k) $\times$ n)), которые удовлетворяют условию:

$$G\,H^T = 0, \tag{5}$$

где H^T - транспонированная матрица H.

Пространства строк матриц G и H являются идеалами в A_n. Для таких матриц задаются производящие многочлены соответственно $g(x)$ и $h(x)$ ($g(x)\cdot h(x)=f(x)$), которые формируют строки матриц G и H.

Аналогично вышесказанному, квадратные матрицы порядка n (и обратные для них) возможно записать в виде:

$$A^{-1} = \begin{bmatrix} a_1 & a_2 & a_3 & ... & a_{n-1} & a_n \\ 0 & a_1 & a_2 & ... & a_{n-2} & a_{n-1} \\ 0 & 0 & a_1 & ... & a_{n-3} & a_{n-2} \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & a_1 & a_2 \\ 0 & 0 & 0 & ... & 0 & a_1 \end{bmatrix}, \tag{6}$$

где строки матриц (6), аналогично идеалам многочленов, образуют компоненты некоторого вектора $a \in V_n$, т.е. предполагается, что матрица A преобразуется вектором $a=(a_1,...,a_n)$, а матрица A^{-1} составляется отличным от а определенным вектором $b=(b_1,...,b_n)$.

Для фиксированного вектора a и матрицы (6) с помощью известного (например (4)) метода нетрудно определить значения компонентов вектора b для произвольного значения n. Например, прибегая к математической индукции можно показать, что при произвольном n>1 матрица вида

$$A = \begin{bmatrix} 1 & 1 & 0 & ... & 0 & 0 \\ 0 & 1 & 1 & ... & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 & 1 \\ 0 & 0 & 0 & ... & 0 & 1 \end{bmatrix}, \tag{7}$$

с производящим вектором $a=(a_1,...,a_n)$ (где a_i=1, если $i \leq 2$ и a_i=1, если i>2) в качестве своей обратной имеет матрицу:

$$A^{-1} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \qquad (8)$$

где $b=(b_1,...,b_n)$, $b_i=1$ $(1 \le i \le n)$.

Аналогично для производящих векторов $a=(a_1,a_2,...,a_n)$ ($a_i=1$, $i\le 3$; $a_i=0$, $i>3$) и $b=(b_1,b_2,...,b_n)$ ($a_i=1$, $i=3k+1$, $i=3k+2$; $a_i=0$, $i=3k$), соответственно получаем:

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

$$A^{-1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & \Lambda & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & \Lambda & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & \Lambda & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & \Lambda & 1 & 1 & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & 0 & 0 & 0 & 0 & \Lambda & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \Lambda & 0 & 0 & 1 \end{bmatrix} \qquad (9)$$

(заметим, что в записи (9) $n=3k$, и $k \ge 0$ - целое число).

Главной задачей при построении матриц вида (8), (9) является не создание метода построения обратной матрицы, основанной на операциях вычисления, а выявление простого метода (или функции) соответствия для нахождения матрицы, обратной для матрицы (6).

Высокая криптостойкость требует построения множества ключей высокой мощности (например, $N=10^{30}$) из которого выбирается конкретный ключ, т.е. - конкретная матрица. Если в матрице (6) представить строки в определенном порядке, то и в обратной для нее матрице необходимо в том же порядке переставлять столбцы, т.е. из заданной матрицы можем получить $n!$ ключевых матриц. Аналогично можно в матрице A переставлять столбцы, что в целом для одной первичной матрицы (при фиксированных производящих a и b) составить множество ключей порядка $(n!)^2$.

Идеальные криптографические системы, к сожалению, построить невозможно. Выигрыш в криптостойкости чаще всего приводит к потере быстродействия или понижению значимости других характеристик, хотя известные различия в криптосистемах, несомненно, оправдываются неодинаковыми условиями их практического применения.

Преимущество матричных методов перед методами Виженера в принципе проявляется в том, что разовое вскрытие криптограммы не вызывает вскрытия самого ключа системы. Это достигается за счет понижения быстродействия. Однако именно потери в быстродействии окупаются качественно отличной и повышенной криптостойкостью данных систем.

2. Синтез криптографических матриц на основе алгебраических структур кодирования

Построение вышерассмотренных матриц принимает более целенаправленный характер с привлечением к решению задачи некоторых специальных структур алгебраической теории кодирования [4]. Как уже было указано, элементы $a=(a_1,...,a_n)\in V_n$ и

$$a(x)=\sum_{i=0}^{n} a_i x^i \in A_n$$

подразумеваются эквивалентными объектами. Известно также, что в алгебре A_n для любого идеала I существует единственный нормированный многочлен $g(x)$ наименьшей степени, такой, что класс вычетов $\{g(x)\}$ принадлежит идеалу I и, наоборот, каждый нормированный многочлен $g(x)$, который делит $f(x)$, образует определенный идеал I, в котором $g(x)$ есть нормированный многочлен минимальной степени такой, что класс вычетов $\{g(x)\}\in I$.

Известна следующая Теорема.

ТЕОРЕМА 1. *Пусть, $f(x)$ - многочлен степени n, $f(x)=g(x)h(x)$, а $h(x)$ - многочлен степени k. Тогда в алгебре многочленов по модулю $f(x)$ класс вычетов $\{g(x)\}$ имеет размерность k. Следовательно, степень многочлена $g(x)$ равна*

$$r=n-k. \tag{10}$$

Справедлива также следующая Теорема.

ТЕОРЕМА 2. *Предположим, что $f(x)$, $g(x)$ и $h(x)$ нормированные многочлены и $f(x)=g(x)h(x)$. Тогда класс вычетов $\{a(x)\}$ принадлежит нулевому пространству, порожденному $h(x)$ тогда и только тогда, когда он принадлежит идеалу, порожденному многочленом $g(x)$.*

Из вышеприведенного следует:

СЛЕДСТВИЕ 1. *Пусть, $f(x)=g(x)h(x)$, где $f(x)$ - степени n, а $g(x)$ - степени r многочлены, тогда*

$$G\,H^T = 0,$$

где G и H порождаются соответственно многочленами $g(x)$ и $h(x)$.

Циклический сдвиг компонентов вектора $g(x)$ на i позиций представляет собой вектор $g(i)=(g_i,...,g_{n-i})$, т.е. i-тый сдвиг многочлена $g(x)=1+xg_1+...+x^{n-1}g_{n-1}$ приводит к многочлену $g(x^{(i)})=x^i g(x) \bmod (x^n-1)$.

Предположим, что $g(x)h(x)=x^n-1$, а $g(x)$ и $h(x)$ порождают соответственно идеалы I и I'. Тогда

$$G=\begin{bmatrix} g_0 & g_1 & ... & g_r & 0 & ... & 0 & ... & 0 \\ 0 & g_0 & ... & g_{r-1} & g_r & ... & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & ... & g_0 & ... & g_r \end{bmatrix}, \tag{11}$$

$$H=\begin{bmatrix} h_0^* & h_1^* & ... & h_k^* & 0 & ... & 0 & ... & 0 \\ 0 & g_0 & ... & h_{k-1}^* & h_k^* & ... & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & ... & h_0^* & ... & h_k^* \end{bmatrix}, \tag{12}$$

и для произвольных $g(x^{(i)})$ и $h(x^{(i)})$ справедливо равенство:

$$g(x^{(i)})\,h(x^{(i)}) \equiv 0 \bmod (x^n-1), \tag{13}$$

где $i, j \in \{1,...,n\}$. С учетом того, что над полем $GF(2)$ произведения многочленов и векторов не совпадают, для любого $g\in I$

$$gH^{*T}=0, \tag{14}$$

где H^* матрица образуется вектором h^*, содержащим компоненты h, записанные в обратном порядке следования.

Следует подчеркнуть (что важно для последующих выводов) справедливость (13) и (14), исходящей из замкнутости идеалов I и I^* относительно векторных циклических сдвигов.

Рассмотрим соответствующие матрице (6) квадратные (порядка n) матрицы, которые порождаются многочленами $g(x)$ и $h(x)$ (т.е. многочленами, с помощью коэффициентов которых образуются матрицы (11) и (12)):

$$A_1 = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & g_0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} h_0 & h_1 & \dots & h_k & 0 & \dots & 0 \\ 0 & h_0 & \dots & h_{k-1} & h_k & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & h_0 \end{bmatrix}, \qquad (15)$$

где j-ый столбец матрицы A_2 представляет собой вектор $h'(j)$ в алгебре многочленов по модулю $x^n - 1$, i-тые компоненты которого суть компоненты вектора $h^*(x)\, x^{i+j-1}$, при $i \le j$ и $h'_i = 0$, если $i > j$.

Исходя из вышеизложенного (учитывая условие (10)) следует, что

$$g(i)h'(j)^T = \begin{cases} 0, & \textit{если} \quad i \ne j; \\ 1, & \textit{если} \quad i = j; \end{cases} \qquad (16)$$

где $h'^{\,T}$ - вектор-столбец, т.е. транспонированный вектор h'.

Следовательно доказана теорема:

<u>ТЕОРЕМА 3</u>. *Пусть $g(x)$ и $h(x)$ - многочлены соответственно степени r и k над полем $GF(2)$ в алгебре многочленов по модулю x^n-1 такие, что $g(x)h(x)=x^n-1$, а A_1 и A_2 - матрицы порядка n, которые порождаются многочленами $g(x)$ и $h(x)$ (15), тогда A_1 и A_2 взаимообратные, т.е.*

$$A_1A_2=I, \quad A_2A_1=I,$$

где I - единичная матрица.

Заметим, что разработаны и известны конструктивные методы построения многочленов $g(x)$ и $h(x)$ в алгебре многочленов по модулю x^n-1 с условием $g(x)h(x)=x^n-1$, которые создают необходимые предпосылки для конструктивной реализации метода, исходящего из теоремы 3.

ЛИТЕРАТУРА:

1. К Шеннон. *Работы по теории информации и кибернетике*. М.: ИЛ, 1963.
2. B. Schneier. *Applied cryptography. John Wiley and Sons*, Inc. New-York, 1996.
3. Ф. Р. Гантмахер. *Теория матриц*. М.: Наука, 1967.
4. Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки. *Теория кодирования*. М.: Мир, 1978.