УДК 519.711/.72

А.Я. Белецкий

Национальный авиационный университет, Киев

ОДНОСТОРОННЯЯ ФУНКЦИЯ НА ОСНОВЕ ОБОБЩЕННЫХ ПРИМИТИВНЫХ ПОЛИНОМОВ

Один из подходов к формированию односторонних функций на основе двоичных примитивных матриц $\mathbf{M}$ изложен в [1]. Суть протокола обмена данными по открытому каналу связи между двумя абонентами компьютерной сети (Алисой) А и (Бобом) В, в ходе которой образуется секретный ключ криптографической защиты информации $\mathbf{K}$, сводится к следующему. Пусть $\mathbf{V}$ и $\mathbf{M}$ – открытые n-битная вектор-строка (вектор инициализации) и примитивная матрица порядка n соответственно. Абонент А вырабатывает случайный показатель x, вычисляет вектор $\mathbf{V}_a = \mathbf{V} \cdot \mathbf{M}^x$ и посылает его абоненту В. В свою очередь абонент В вырабатывает случайный показатель y, вычисляет вектор $\mathbf{V}_b = \mathbf{V} \cdot \mathbf{M}^y$ и посылает его абоненту А. Затем Али-

са вычисляет ключ $\mathbf{K}_a = \mathbf{V}_b \cdot \mathbf{M}^x$, а Боб вычисляет ключ $\mathbf{K}_b = \mathbf{V}_a \cdot \mathbf{M}^y$. Вполне очевидно, что по завершении протокола оба абонента будут располагать одним и тем же секретным ключом $\mathbf{K}$, так как

$$\mathbf{K}_a = \mathbf{V} \cdot \mathbf{M}^y \cdot \mathbf{M}^x = \mathbf{K}_b = \mathbf{V} \cdot \mathbf{M}^x \cdot \mathbf{M}^y = \mathbf{K}. \qquad (1)$$

Появлению данного протокола обмена секретными ключами по открытому каналу связи предшествовал матричный алгоритм формирования ключей шифрования [2], основная идея которого состоит в следующем. Если **X, Y** – векторы, представляющие соответственно открытый и зашифрованный текст, а $\mathbf{M}$ – шифрующая матрица, то зашифрование задается уравнением $\mathbf{Y} = \mathbf{M} \cdot \mathbf{X}$, а расшифрование – уравнением $\mathbf{X} = \mathbf{M}^{-1} \cdot \mathbf{Y}$. Для обмена сеансовыми ключами в системе авторы (Ерош и Скуратов) предлагают использовать протокол Диффи – Хэллмана (DH) [3] в циклической группе матриц $\langle \mathbf{M} \rangle$, причем матрица считается общедоступной. Предполагается, что пользователь А вырабатывает случайный показатель x, вычисляет матрицу $\mathbf{M}^x$ и посылает ее пользователю В. В свою очередь пользователь В вырабатывает случайный показатель y, вычисляет матрицу $\mathbf{M}^y$ и посылает ее пользователю А. Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу (ключ шифрования) $\mathbf{M}^{xy} = \mathbf{M}^{yx}$. Поскольку мощность группы, образующим элементом которой являются невырожденные примитивные двоичные матрицы $\mathbf{M}$ (рекомендуемый порядок должен быть не менее чем 100), велико, то вычисление ключа, как утверждают авторы (кстати, без доказательства), имеет переборную сложность. Как показано в [4], изложенный выше алгоритм не обеспечивает заявленной стойкости шифрования, а ключ достаточно легко взламывается. Протокол формирования ключей шифрования (1) наследует некоторые черты алгоритма Ероша-Скуратова [2], поэтому вопрос его криптостойкости остается открытым.

Предлагаемый алгоритм формирования односторонней функции основан на применении так называемых *обобщенных примитивных полиномов* (ПрП). Понятие обобщенного ПрП корреспондируется с циклической группой $\langle \boldsymbol{\omega}_m \rangle$, образуемой степенями такого двоичного полинома $\omega_m(x)$ степени m по модулю двоичного неприводимого полинома (НП) $\varphi_n(x)$, который доставляет последовательности $\langle \boldsymbol{\omega}_m \rangle$ свойство m – последовательности. Назовем $\omega_m(x)$ образующим (примитивным) элементом (ОЭ) обобщенного ПрП. В качестве обобщенных ПрП могут быть приняты любые НП степени n, в том числе и не являющиеся (по классическому определению) изначально примитивными, при соблюдении условий:

$$[\omega_m(x)]^e \equiv 1 \bmod \varphi_n(x), \quad \min e = 2^n - 1, \quad 1 \le m < n.$$

Протокол формирования секретного ключа $\mathbf{K}$ организован следующим образом. В качестве открытых ключей принимаются двоичный n-разрядный вектор инициализации $\mathbf{V}$ и произвольный НП φ_n. Каждый из абонентов А и В вырабатывают по два секретных ключа, которые обозначим $(\omega_\alpha, x_\alpha)$ и (ω_β, x_β) соответственно. Оба параметра ω и x являются случайными n-битными числами. На основании НП φ_n и ОЭ ω Алиса и Боб вычисляют примитивные матрицы Галуа (алгоритм их формирования поясняется ниже), которые обозначим $\mathbf{G}_{\omega,\alpha}$ и $\mathbf{G}_{\omega,\beta}$ соответственно. Абонент А определяет вектор $\mathbf{V}_\alpha = \mathbf{V} \cdot \mathbf{G}_{\omega,\alpha}^{x_\alpha}$ и посылает его Бобу. В свою очередь Боб определяет вектор $\mathbf{V}_\beta = \mathbf{V} \cdot \mathbf{G}_{\omega,\beta}^{x_\beta}$ и посылает его Алисе. Затем Алиса вычисляет ключ $\mathbf{K}_\alpha = \mathbf{V}_\beta \cdot \mathbf{G}_{\omega,\alpha}^{x_\alpha}$, а Боб – ключ $\mathbf{K}_\beta = \mathbf{V}_\alpha \cdot \mathbf{G}_{\omega,\beta}^{x_\beta}$. В силу того, что произведение матриц Галуа коммутативное, у обоих абонентов появляется общий секретный ключ $\mathbf{K}$, так как $\mathbf{K}_\alpha = \mathbf{K}_\beta$.

Алгоритм синтеза матриц Галуа проиллюстрируем на конкретном примере, выбрав $\varphi_8 = 100101101$ и $\boldsymbol{\omega} = 111$. Процесс синтеза матрицы $\mathbf{G}$ разбивается на два этапа. На первом этапе составляется так называемая *стартовая таблица*, содержащая *стартовую матрицу* восьмого порядка $\mathbf{M}$, однозначно определяемую ее ОЭ $\boldsymbol{\omega}$ (табл. 1, в которой стартовая матрица выделена затенением).

Таблица 1

Стартовая таблица

$\boldsymbol{\varphi} \rightarrow$	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	$\mathbf{V}_1$						1	1	1

Вектор $\mathbf{V}_1$ порождает диагональное заполнение элементов стартовой матрицы $\mathbf{M}$. Предполагается, что в незаполненных ячейках матрицы $\mathbf{M}$ находятся нули. Для простоты восприятия эти ячейки оставлены пустыми. Для векторов $\mathbf{V}_k$ таких, что номер старшего разряда, в котором стоит 1, не превышает $n - m$, мы можем двумя способами вычислить вектор $\mathbf{V}_{k+1}$.

При первом способе (назовем его *аналитическим*) вектор $\mathbf{V}_{k+1}$ определяется соотношением $\mathbf{V}_{k+1} = (\mathbf{V}_k \otimes \boldsymbol{\omega}) \bmod \boldsymbol{\varphi}$. Полагая $\mathbf{V}_k = 1111111$ (т.е. выбрав вектор, заполняющий в колонке «Метки» единицами семь строк табл. 1), получим $\mathbf{V}_{k+1} =$ $= 01010000$.

Второй способ (назовем его *графическим*) определения вектора $\mathbf{V}_{k+1}$, обозначим его $\mathbf{V}^*_{k+1}$, сводится к поразрядному сложению элементов матрицы $\mathbf{M}$, помеченных в табл. 1 единицами вектора $\mathbf{V}_k$. Имеем $\mathbf{V}^*_{k+1}$ = 10111101. Невязка 11101101 векторов $\mathbf{V}_{k+1}$ и $\mathbf{V}^*_{k+1}$ как раз и определяет значение седьмой строки матрицы.

Выполнив аналогичную корректировку восьмой строки табл. 1, приходим к окончательной форме матрицы преобразования

$$\mathbf{G}_{\varphi}^{(111)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Примитивность и коммутативность $\mathbf{G}$ матриц Галуа как раз и составляют основу синтеза односторонней функции, относительно которой можно выдвинуть гипотезу, что единственной для нее атакой является лобовая атака прямого перебора. Криптостойкость функции может быть усилена за счет введения дополнительного секретного ключа – перестановочной матрицы $\mathbf{P}$ n-го порядка, посредством которой матрица $\mathbf{G}$ замещается подобной матрицей $\widetilde{\mathbf{G}} = \mathbf{P} \cdot \mathbf{G} \cdot \mathbf{P}^{-1}$, сохраняющей все свойства исходной матрицы $\mathbf{G}$.

Список литературы

1. Мегрелишвили Р.П. Однонаправленная матричная функция – быстродействующий аналог протокола Диффи-Хэллмана / Р.П. Мегрелишвили, М.А. Челидзе, Г.М. Бесиашвили // Інтернет-Освіта-Наука-2010: збірник матеріалів 7-й МК. – Вінниця: ВНТУ, 2010. – С. 341-344.

2. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / И.Л. Ерош, В.В. Скуратов // Проблемы информационной безопасности. Компьютерные системы. – 2004. – № 1. – С. 72-78.

3. Diffie W. New Directions in Cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – November 1976. – V. IT-22, no. 6. – P. 644-654.

4. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова) [Электронный ресурс] / А.Г. Ростовцев. – Режим доступа у ресурсу: http://www.ssl.stu. neva.ru/psw/crypto/rostovtsev/Erosh_Skuratov.pdf