УДК 003.26:004.432:004(075.8)

Белецкий А.А., Белецкий А.Я.
Национальный авиационный университет, Киев

КОНВЕЙЕРНЫЙ АНАЛОГ МАТРИЧНОГО ПРОТОКОЛА ДИФФИ-ХЕЛЛМАНА

Предложен вариант построения матричного аналога протокола Диффи-Хеллмана, использующего процедуру конвейерного обновления секретного бинарного элемента, используемого для формирования секретного ключа шифрования легализованными абонентами открытой компьютерной сети. В отличие от классического протокола предлагаемый алгоритм свободен от атаки типа «человек посередине».

Ключевые слова: *неприводимые полиномы, поля Галуа, матрицы Галуа и Фибоначчи, криптостойкость протокола.*

Введение и постановка задачи

Классический протокол Диффи-Хеллмана ($DH-$протокол, алгоритм) предназначен для формирования секретных ключей шифрования информации легализованными абонентами компьютерной сети по открытым каналам связи [1]. В $DH-$алгоритме предполагается, что легализованным абонентам сети (Алисе и Бобу) известны открытые ключи p и q, причем p есть большое простое число, а $q-$ образующий элемент (ОЭ) мультипликативной группы кольца вычетов по модулю p такой, что $q<p$. Абонент Алиса генерирует случайное большое число $a<p$, вычисляет значение $A=q^a(\mathrm{mod}\,p)$ и пересылает его Бобу. В свою очередь Боб генерирует случайное большое число $b<p$, вычисляет значение $B=q^b(\mathrm{mod}\,p)$ и пересылает его Алисе. Далее, абонент Алиса возводит полученное от Боба число B в свою случайную степень a и вычисляет значение $K_a=B^a(\mathrm{mod}\,p)=q^{ba}(\mathrm{mod}\,p)$. Аналогично поступает Боб, вычисляя $K_b=A^b(\mathrm{mod}\,p)$ = $q^{ab}(\mathrm{mod}\,p)$. Очевидно, что оба абонента получают одно и то же число K, поскольку $K_a\equiv K_b$. Это число K Алиса и Боб могут использовать в качестве секретного ключа, например, для симметричного шифрования, поскольку противник (Ева), перехвативший числа A и B, не сможет воспроизвести ключ K, так как встретится с практически неразрешимой (за разумное время) проблемой вычисления K, если только значения p, a и b были выбраны достаточно большими. Основной недостаток $DH-$алгоритма состоит в том, что соответствующий протокол формирования секретных ключей подвержен атаке типа «человек посередине» [2].

В ряде работ [3]$-$[5] предложены матричные аналоги $DH-$протокола, которые также не являются свободными от атак упомянутого типа. Как показано в [6] матричный протокол Ероша-Скуратова [3] легко взламывается посредством китайской теоремы об остатках [7]. Проблема криптостойкости протокола Мегрелишвили [4] остается открытой. Процедура формирования ключа шифрования K в матричном аналоге $DH-$протокола, предлагаемого в [5], состоит в следующем. Абонент Алиса выбирает секретный примитивный элемент ω_a поля $GF(2^n)$, порождаемого неприводимым полиномом (НП) f_n степени n, формирует примитивную матрицу Галуа $G_{f_n}^{(\omega_a)}$, вычисляет вектор $V_a=V\cdot G_{f_n}^{(\omega_a)}$ и посылает его Бобу. Невырожденная квадратная матрица G является *примитивной*, если последовательность степеней этой матрицы в поле $GF(p)$ образует последовательность максимальной длины ($m-$последовательность), равной p^n-1. В свою очередь Боб выбирает

примитивный элемент ω_b, формирует примитивную матрицу $G_{f_n}^{(\omega_b)}$, вычисляет вектор $V_b = V \cdot G_{f_n}^{(\omega_b)}$ и посылает его Алисе. После этого оба абонента умножают векторы, полученные от партнера, на свои секретные матрицы Галуа. Тем самым будет сформирован общий секретный ключ K, поскольку произведение примитивных матриц Галуа над одним и тем же НП f_n коммутативно. Следовательно,

$$K_a = V_b \cdot G_{f_n}^{(\omega_a)} = V \cdot G_{f_n}^{(\omega_b)} \cdot G_{f_n}^{(\omega_a)} \quad \equiv \quad K_b = V_a \cdot G_{f_n}^{(\omega_b)} = V \cdot G_{f_n}^{(\omega_a)} \cdot G_{f_n}^{(\omega_b)}. \qquad (1)$$

Необходимые и достаточные условия примитивности и коммутативности матриц Галуа уточняются в следующем разделе работы.

Вместо базовых (как и сопряженных) матриц Галуа, с равным успехом в матричном аналоге [5] могут быть использованы обобщенные двоичные матрицы Фибоначчи, обладающие теми же свойствами (примитивности и коммутативности), что и матрицы Галуа. Существенный недостаток анализируемого протокола, как будет показано ниже, состоит в том, что для данного алгоритма характерна низкая криптостойкость.

Основная задача исследования, поставленная в статье, состоит в разработке *модифицированного* варианта матричного аналога протокола [5], которым, во-первых, достигается существенное повышение криптостойкости алгоритма и, во-вторых, устраняются атаки на протокол типа «человек посередине».

Анализ криптостойкости матричного аналога DH – протокола [5]

В процессе формирования секретных ключей шифрования абоненты Алиса и Боб обмениваются по открытым каналам связи, как отмечено выше, бинарными векторами $n-$го порядка V_a и V_b, образуемыми произведением открытого вектора инициализации V и индивидуальных для каждого абонента секретных примитивных матриц Галуа $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$ соответственно. Синтез матриц Галуа осуществляется в соответствии с методом, названным методом *диагонального заполнения* [8]. Суть этого метода состоит в следующем. Образующий элемент ω, являющийся примитивным элементом поля $GF(2^n)$, порождаемого НП f_n, размещается в правом углу нижней (первой) строки матрицы $n-$го порядка G. Элементы этой строки, расположенные левее ω, заполняются нулями. Последующие строки матрицы G (по направлению снизу вверх) образуются простым сдвигом на один разряд справа налево предыдущих строк матрицы, причем старшие разряды строк, содержащие нули, теряются, а в правые освобождающиеся элементы записываются нули. Такая процедура формирования строк носит название *круговой прокрутки* (циклического сдвига) на один разряд по часовой стрелке. Если при этом левый элемент сдвигаемой строки равен 1, то выполняется обычный сдвиг строки на один разряд влево. Разрядность подобных строк становится на единицу больше порядка матрицы. Векторы, отвечающие таким строкам, приводятся к остатку по модулю НП f_n. Тем самым длина вектора также приводится к величине, равной n битам.

Пример матрицы Галуа восьмого порядка с параметрами $\omega = 101101$ и $f_8 = 101001101$, полученной на основании метода диагонального заполнения, представлен выражением

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \qquad (2)$$

Если ω_a и ω_b – примитивные элементы расширенного поля Галуа $GF(p^n)$, порождаемого НП f_n, то матрицам $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$ становятся присущи как свойства примитивности, так и коммутативности. На простых числовых примерах легко убедиться в том, что мультипликативные группы, порождаемые матрицами n – го порядка $G_{f_n}^{(\omega)}$, изоморфны группам, порождаемыми образующими элементами ω этих матриц. В самом деле, пусть, для примера, $n=3$ и $\omega=11$ – примитивный элемент поля $GF(2^3)$, порождающий полином которого есть НП $f_3=1011$. Последовательность степеней s матрицы $G_{1011}^{(11)}$ над полем $GF(2)$ сведена в табл. 1.

Таблица 1.

Мультипликативная группа матриц Галуа

s	G^s	s	G^s	s	G^s	s	G^s
0	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	1	$\begin{pmatrix}1&1&1\\1&1&0\\0&1&1\end{pmatrix}$	2	$\begin{pmatrix}0&1&0\\0&0&1\\1&0&1\end{pmatrix}$	3	$\begin{pmatrix}1&1&0\\0&1&1\\1&0&0\end{pmatrix}$
4	$\begin{pmatrix}0&0&1\\1&0&1\\1&1&1\end{pmatrix}$	5	$\begin{pmatrix}0&1&1\\1&0&0\\0&1&0\end{pmatrix}$	6	$\begin{pmatrix}1&0&1\\1&1&1\\1&1&0\end{pmatrix}$	7	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$

Из анализа матриц, представленных в табл. 1, приходим к следующим выводам. Во-первых, последовательность степеней матриц G образует последовательность максимальной длины (m – последовательность). А это означает, что матрицы G, порождаемые примитивными элементами ω, являются примитивными матрицами. И, во-вторых, каждая степень s матрицы G может быть получена методом диагонального заполнения, причем образующий элемент матрицы G^s, обозначим его ω_s, определяется соотношением $\omega_s=\omega^s \pmod{f_n}$. И, как следствие второго вывода: мультипликативная группа, порождаемая матрицей G изоморфна мультипликативной группе, порождаемой образующим элементом этой матрицы.

Очевидно также, что если m – последовательность формируется примитивной матрицей $G_{f_n}^{(\omega_a)}$, то найдется такая степень k этой матрицы, которая приводит к равенству $G_{f_n}^{(\omega_b)}=\left[G_{f_n}^{(\omega_a)}\right]^k$. Следовательно, матрицы $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$ принадлежат одной и той же *абелевой* группе максимального порядка по умножению независимо от того, какой примитивной матрицей порождается эта группа. Из того, что произведение элементов любой абелевой группы коммутативно [9], приходим к заключению, что произведение матриц $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$ также коммутативно.

Таким образом, приходим к заключению, что примитивность образующих элементов ω_a и ω_b поля $GF(p^n)$, порождаемого НП f_n, является необходимым и достаточным условиями примитивности и коммутативности матриц Галуа $G_{f_n}^{(\omega_a)}$ и $G_{f_n}^{(\omega_b)}$.

Существенный недостаток рассмотренного алгоритма формирования секретных ключей шифрования легализованными абонентами сети по открытым каналам связи состоит в том, что предлагаемый способ синтеза матриц Галуа (по методу диагонального заполнения

строк этих матриц) содержит в себе угрозу достаточно простого взлома протокола. Для подтверждения высказанного предположения рассмотрим вектор

$$V_a = V \cdot G_{f_n}^{(\omega_a)}, \tag{3}$$

формируемый абонентом Алиса.

Из теории многочленов (полиномов) одной переменной, которую обозначим x, известно [10], что умножение произвольного полинома $\omega_n(x)$ степени n на x эквивалентно простому сдвигу полинома на один разряд влево и, соответственно, увеличению на 1 степен полинома, т.е.

$$x \cdot \omega_n(x) \to \omega_{n+1}(x). \tag{4}$$

Воспользовавшись выражением (4), представим матрицу Галуа $G_{f_n}^{(\omega_a)}$ порядка n соотношением

$$G_{f_n}^{(\omega)} = \begin{pmatrix} x^{n-1} \cdot \omega \\ x^{n-2} \cdot \omega \\ \dots \\ x \cdot \omega \\ \omega \end{pmatrix} = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \dots \\ x \\ 1 \end{pmatrix} = \omega \cdot \varphi_{\text{n-1}}^{\text{T}}(x) (\text{mod } f_n), \tag{5}$$

в котором $\varphi_{\text{n-1}}^{\text{T}}(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 -$ полином степени $n-1$.

На основании соотношений (3) и (5) получим

$$V_a(x) = \omega_a \cdot \varphi_v(x), \tag{6}$$

где

$$\varphi_v(x) = V \cdot \varphi_{n-1}(x) \equiv V,$$

поскольку вектор-столбец, соответствующий полиному $\varphi_{n-1}(x)$, состоит из n чисел 1. Тем самым уравнение (6) может быть представлено равенством

$$V_a = \omega_a \cdot V, \tag{7}$$

в котором все компоненты известны за исключением компонента ω_a. Разрешая равенство (7) относительно ω_a, находим

$$\omega_a = V_a \cdot V^{-1} (\text{mod } f_n). \tag{8}$$

Рассмотрим числовой пример. Воспользуемся матрицей $G_{f_n}^{(\omega_a)}$, заданной выражением (2), согласно которому $n = 8$, $\omega_a = 101101$, а НП $f_8 = 101001101$, причем $f_8 -$ открытый, а $\omega_a -$ секретный ключ протокола. В качестве вектора инициализации выберем вектор $V = 11010010$, которому отвечает обратный по модулю f_8 вектор $V^{-1} = 110010$. На основании преобразования (3) получим $V_a = 10111111$. Подставив значения векторов V_a и V^{-1} в правую часть выражения (8) и приводя произведение векторов к остатку по модулю f_8, приходим к искомому (секретному) ключу ω_a абонента Алисы ω_a. Аналогичным образом Ева находит секретный ключ ω_b абонента Боба. После определения ключей ω_a и ω_b проблема вычисления секретного ключа K становится тривиальной.

Конвейерный метод формирования ключей

Стойкость рассмотренных альтернативных протоколов можно довести до уровня стойкости алгоритмов, основанных на проблеме факторизации модульных произведений больших чисел, если допустить возможность существования секретного параметра θ, известного как Алисе, так и Бобу.

Модификация протокола [5] состоит в следующем. Предположим, что легализованные абоненты сети располагают секретным параметром θ, представляющим собой двоичный вектор $n-$го порядка. Параметр θ может быть передан от Алисы к Бобу (или наоборот) тем или иным способом, например, с помощью протокола RSA [11]. Алиса генерирует случайное $n-$битное число ω_a, вычисляет образующий элемент

$$\theta_a = \omega_a \cdot \theta \left(\mathrm{mod}\ f_n\right), \tag{9}$$

с помощью которого формирует матрицу Галуа $G_{f_n}^{(\theta_a)}$, определяет вектор $V_a = V \cdot G_{f_n}^{(\theta_a)}$ и отправляет его Бобу. Аналогично поступает Боб, направляя Алисе вектор $V_b = V \cdot G_{f_n}^{(\theta_b)}$, в котором $\theta_b = \omega_b \cdot \theta \left(\mathrm{mod}\ f_n\right)$.

Как показано выше, образующие элементы θ_a и θ_b легко вычисляются и, следовательно, абоненты Алиса и Боб (но не противник Ева) могут без проблем определить секретный параметр ω партнера. Так, например, на основании (9) абонент Боб находит $\omega_a = \theta_a \cdot \theta^{-1} \left(\mathrm{mod}\ f_n\right)$, что предоставляет ему возможность (аналогично и Алисе) вычислить общий секретный ключ $K = \omega_a \cdot \omega_b \left(\mathrm{mod}\ f_n\right)$. Ключ K (или некоторая функция от него) может быть принят в качестве секретного параметра $\theta^+ = K$ для очередного сеанса формирования секретного ключа шифрования по открытым каналам связи.

Такой способ формирования ключей шифрования назван нами *конвейерным*. Конвейерный алгоритм может быть задействован в обоих рассмотренных выше вариантах альтернативных протоколов. Преимущество конвейерного алгоритма формирования секретного ключа шифрования легализованными абонентами открытой компьютерной сети состоит в том, что предлагаемый протокол свободен от атаки типа «человек посередине». Данное свойство протокола приобретается за счет включения в образующие элементы матриц Галуа секретного элемента θ, известного только Алисе и Бобу. Любая попытка замены противником Евой на свой элемент θ_e приводит к тому, что Ева оказывается не в состоянии вычислить параметры ω_a и ω_b. А это означает, что Ева оказывается также не в состоянии определить общий ключ шифрования K.

Выводы

В статье проведен анализ известных матричных алгоритмов обмена ключами шифрования между абонентами компьютерной сети по открытым каналам связи. В основу алгоритмов положен модифицированный асимметричный протокол Диффи-Хэллмана (DH). Суть модификации сводится к замене больших простых чисел алгоритма DH гарантированно невырожденными примитивными двоичными матрицами высокого порядка. Предлагаются методы синтеза таких матриц, как на основе обобщенных кодов Грея, так и неприводимых полиномов. Разработаны новые матричные протоколы обмена ключами, превосходящие по криптостойкости протоколы Ероша-Скуратова и Мегрелишвили, описанные в данной работе.

Предлагаемые варианты векторно-матричных протоколов обмена криптографическими ключами по открытым каналам связи имеют хорошую перспективу применения в системах компьютерного симметричного шифрования в компьютерных сетях, защищенных от подмены данных, обеспечивая необходимый уровень защиты секретных ключей от несанкционированного доступа и атаки типа «человек посередине».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Diffe W. New Directions in Cryptography / Diffe W., Hellman V.E. // IEEE Transact. On Information Theory, v. IT-22, no. 6, Nov, 1976, p. 644-654.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ, 2003. – 816 с.

3. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / Ерош И.Л., Скуратов В.В. // Проблемы информационной безопасности. Компьютерные системы. – 2004. – №1. – С. 72-78.
4. Мегрелишвили Р.П. Однонаправленная матричная функция – быстродействующий аналог протокола Диффи-Хэллмана / Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М. – Збірник матеріалів 7-й МК «Інтернет-Освіта-Наука-2010». – Вінниця: ВНТУ, 2010. – С. 341-344.
5. Білецький А.Я. Матричні аналоги протоколу Діффі-Хеллмана / Білецький А.Я., Білецький А.А., Кандиба Р.Ю. – Матеріали І-ої МНТК «Захист інформації і безпека інформаційних систем». – Львів: Нац. ун-т «Львівська політехніка», 2012. – С. 68-69.
6. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова). Ел. ресурс: www. ssl.stu.neva.ru/psw/crypto/rostovtsev/Erosh_Skuratov.pdf
7. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
8. Белецкий А.Я. Синтез примитивных матриц над конечними полями Галуа и их приложения / Белецкий А.Я., Белецкий О.А. // Інформаційни технології в освіті: Збірник наукових праць, Вип. 13. – Херсон: ХДУ, 2012. – С. 23-43.
9. Александров П.С. Введение в теорию групп. – М.: Наука, 1980. – 144 с.
10. Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. Т 1. – М.: Мир, 1988. – 430 с.
11. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – New York, NY, USA: ACM, 1978. – Т. 21. – № 2, Feb. 1978. – С. 120-126.

Стаття надійшла до редакції 24.01.2013.

Beletsky A.J., Beletsky A.A.
National Aviation University, Kyiv

CONVEYOR ANALOG OF MATRIX DIFFIE-HELLMAN PROOTOKOL

A variant of the construction of the matrix analog of Diffie-Hellman based on pipelined binary update secret element used to generate the secret key encryption legalized subscribers open network. In contrast to the classical protocol proposed algorithm is free from the attacks of the "man in the middle."

Keywords: irreducible polynomials, Galois fields, Galois and Fibonacci matrix, cryptographic protocol.

Білецький А.Я., Білецький О.А.
Національний авіаційний університет, Київ

КОНВЕЄРНИЙ АНАЛОГ МАТРИЧНОГО ПРОТОКОЛУ ДІФФІ-ХЕЛЛМАНА

Запропоновано варіант побудови матричного аналога протоколу Діффі-Хеллмана на основі конвеєрного поновлення секретного бінарного елемента, що використовується для формування секретного ключа шифрування легалізованими абонентами відкритої комп'ютерної мережі. На відміну від класичного протоколу алгоритм, що запропоновано, вільний від атаки типу «людина посередині».

Ключові слова: незвідні поліноми, поля Галуа, матриці Галуа і Фібоначчі, криптостійкість протоколу.