УДК 512.54 + 003.26 + 004.056.55 Вестник УрФО № 4(14)/2014. Стр. 40–44

Сурина А. А., Зюляркина Н. Д.

РЮКЗАЧНАЯ КРИПТОСИСТЕМА НА ОСНОВЕ ПРЯМОГО ПРОИЗВЕДЕНИЯ ДИЭДРАЛЬНЫХ ГРУПП

В статье рассматривается задача о мультипликативном рюкзаке с использованием диэдральных групп. Предложена математическая модель рюкзачной системы на основе прямого произведения диэдральных групп, которая оказалась криптостойкой к атаке методом полного перебора. Приведен пример выполнения шифрования/дешифровки сообщения с использованием предложенной математической модели.

Ключевые слова: *криптосистема, рюкзачная схема, группа, порождающий элемент, мультипликативный рюкзак.*

Surina A. A., Ziuliarkina N. D.

KNAPSACK PUBLIC KEY CRYPTOSYSTEM ON THE BASIS OF DIRECT PRODUCT OF DIHEDRAL GROUPS

The article deals with the problem of multiplicative knapsack with dihedral groups. A mathematical model of knapsack system based on direct product of dihedral groups is proposed; it was proved to be cryptographically resistant to the full enumeration method attack. The authors give examples of the encryption/decryption of key message with the use of proposed mathematical model.

Keywords: *cryptosystem, knapsack system, group, generating element, multiplicative knapsack.*

Усовершенствование технических средств требует постоянных изменений параметров системы, отвечающей за конфиденциальность информации. В связи с этим часто стали использоваться криптосистемы с открытым ключом: криптосистемы, основанные на задаче факторизации (RSA) и задаче нахождения дискретного логарифма (схема Эль-Гамаля). Но возникающие сложности при их использовании вынуждают искать задачи достаточно гибкие и позволяющие вводить новые варианты для преодоления криптографических слабостей.

Рюкзачные схемы очень удобны для иллюстрации основных идей криптографии с открытым ключом. Задача об укладке рюкзака является NP-полной, следовательно, созданная на ее основе система будет лучше и

быстрее, чем системы на основе целочисленной факторизации и дискретного логарифмирования.

Идея мультипликативного рюкзака была предложена в 1988 Масакацу Мории (Masakatu Morii) и Масао Касахара (Masao Kasahara). Мультипликативный рюкзак использует точно такую же функцию шифрования, как и у аддитивной рюкзачной схемы Меркля – Хеллмана.

Алгоритм построения открытого ключа

1. Выбирается n взаимно простых чисел ($p_1, p_2, \ldots, p_n$).

2. Выбирается некоторое простое число q, такое, что q-1 раскладывается на маленькие простые множители так, что

$$q > \prod_{i=1}^{n} p_i \qquad (1)$$

3. Выбирается некоторый примитивный корень $b(\mathrm{mod}\ q)$.

4. Затем находятся такие a_i $(1 < a_i < q-1)$, что: $p_i = b^{a_i} \pmod q$. a_i – дискретный логарифм от p_i по основанию $b(\mathrm{mod}\ q)$.

Зашифрованное сообщение будет выглядеть так:

$$S = \sum_{i=1}^{n} x_i \cdot a_i,$$

где x_i – n-битный вектор исходного сообщения.

Дешифрование происходит по следующей формуле:

$$S' = b^S \bmod q,$$

так как $b^S = b^{\sum x_i a_i} = \prod b^{x_i a_i} = \prod b_i^{x_i} \bmod q.$

Последнее равенство – результат условия (1).

Закрытым ключом является (b, q), открытый ключ – a_i. Затем можно легко найти соответствующий x, начинающийся с S', используя тот факт, что числа p_i взаимно простые [6]. Это очень важно, так как в общем случае задача о произведении подмножеств NP-полная.

Для рюкзака Мории – Касахара в настоящее время неизвестно эффективного способа взлома.

Задачу о мультипликативном рюкзаке можно модифицировать, взяв в качестве элементов рюкзака элементы прямого произведения диэдральных групп.

Пусть D_{2n} – *диэдральная группа порядка* $2n$, такая, что $D_{2n} = a, b$, где $a^2 = e$, $b^n = e$, и выполняется соотношение

$$a^{-1}ba = aba = b^{-1}. \qquad (2)$$

Если $d = a^x b^y$ – элемент диэдральной группы D_{2n}, существует алгоритм нахождения показателей x и y.

Математическая модель рюкзачной системы на основе прямого произведения диэдральных групп

Пусть $G = a, b = D_{2n}$ – диэдральная группа.

Тогда можно рассмотреть следующую рюкзачную систему, основанную на вычисления в диэдральной группе.

Генерация ключей

1. Сообщение шифруется двоичной последовательностью (можно использовать двоичные ASCII-коды символов латинского алфавита). Затем последовательность разбивается на блоки, длина которых равна количеству элементов в рюкзаке.

2. Секретный ключ задается следующим образом:

2.1. для группы $D_{2(q-1)}$

$$g_1' = \begin{pmatrix} \alpha_1 & 0 & \ldots & \ldots \\ 0 & \alpha_1^{-1} & \ldots & \ldots \\ \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & 0 & 1 \end{pmatrix}, \quad g_1'' = \begin{pmatrix} 0 & 1 & \ldots & \ldots \\ 1 & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & 0 & 1 \end{pmatrix}, \ldots, g_n' = \begin{pmatrix} 1 & 0 & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \alpha_n & 0 \\ \ldots & \ldots & 0 & \alpha_n^{-1} \end{pmatrix}, g_n'' = \begin{pmatrix} 1 & 0 & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots \\ \ldots & \ldots & 0 & 1 \\ \ldots & \ldots & 1 & 0 \end{pmatrix}$$

где: $b_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1^{-1} \end{pmatrix}$, $b_2 = \begin{pmatrix} \alpha_2 & 0 \\ 0 & \alpha_2^{-1} \end{pmatrix}$, $a_1 = a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и так далее.

Для удобства вычислений можно выбрать $\alpha_1 = \alpha_2 = \ldots = \alpha_n$.

2.2. для группы $D_{2(q+1)}$

$$g_1^{'}=\begin{pmatrix} a & b & \dots & \dots \\ \alpha b & a & \dots & \dots \\ \dots & \dots & \dots & 0 \\ \dots & \dots & 0 & 1 \end{pmatrix},\ g_1^{''}=\begin{pmatrix} 0 & 1 & \dots & \dots \\ 1 & 0 & \dots & \dots \\ \dots & \dots & \dots & 0 \\ \dots & \dots & 0 & 1 \end{pmatrix},\dots,g_n^{'}=\begin{pmatrix} 1 & 0 & \dots & \dots \\ 0 & \dots & \dots & \dots \\ \dots & \dots & c & d \\ \dots & \dots & \alpha d & c \end{pmatrix},g_n^{''}=\begin{pmatrix} 1 & 0 & \dots & \dots \\ 0 & \dots & \dots & \dots \\ \dots & \dots & 0 & 1 \\ \dots & \dots & 1 & 0 \end{pmatrix}$$

Таких матриц получается столько, сколько элементов в рюкзаке.

3. Формируется рюкзак-ловушка $(\delta_1^{'},\delta_1^{''},\delta_2^{'},\delta_2^{''},\dots)$, который и является открытым ключом.

При этом $\delta_i^{'},\delta_i^{''}$ формируются следующим образом: $\delta_i^{'}=\left(g_i^{'}\right)^x$, $\delta_i^{''}=\left(g_i^{''}\right)^x$, где $x\in GL_{2n}(q)$. При этом x подбирается такой, что матрица будет иметь не диагональный вид, а общий.

Алгоритм шифрования

1. Блоки открытого текста, которые представлены в виде матрицы, возводятся в соответствующую степень (0 – получаем единичную матрицу, или 1 – получаем саму матрицу).

2. Перемножаем те матрицы, которые возводили в степень 1:

$$S=\prod_{i=1}\delta_i^{k_i}$$

Алгоритм дешифровки

1. Вычисляем $\gamma_i=\left(\delta_i^{k_i}\right)^{x^{-1}}$. Получим матрицу, которая будет иметь диагональный вид.

2. Разбиваем матрицу на блоки 2×2. Каждый блок будет элементом диаэдральной группы.

3. Относительно каждого блока применяем алгоритм нахождения показателей в диэдральной группе, при этом учитывая четность n. Таким образом, находится матрица исходного текста.

Пример 1. Рассмотрим группу $G=GL_2(5)$ и выберем в ней элементы

$$b=\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix},\ a=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

где α – примитивный элемент поля F_5, $\alpha=2$, $\alpha^{-1}=3$.

Тогда элементы секретного ключа задаются следующим образом:

$$g_1^{'}=\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ g_1^{''}=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ g_2^{'}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},\ g_2^{''}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Заметим, что $\left\langle g_1^{'},g_1^{''},g_2^{'},g_2^{''}\right\rangle$ является прямым произведением подгрупп $G'=\left\langle g_1^{'},g_1^{''},g_2^{'},g_2^{''}\right\rangle=\left\langle g_1^{'},g_1^{''}\right\rangle\left\langle g_2^{'},g_2^{''}\right\rangle$

Выберем в качестве маскирующего изоморфизма сопряжение посредством $x\in GL_4(5)$:

$$x=\begin{pmatrix} 2 & 0 & 0 & 2 \\ 4 & 3 & 2 & 4 \\ 3 & 1 & 3 & 3 \\ 3 & 4 & 3 & 4 \end{pmatrix}.\ \text{Заметим, что } x^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 0 \\ 0 & 2 & 4 & 0 \\ 2 & 3 & 2 & 1 \end{pmatrix}.$$

Вычислим набор $((g_1^{'})^x,(g_1^{''})^x,(g_2^{'})^x,(g_2^{''})^x)$, который будет являться открытым ключом:

$$(g_1^{'})^x=\begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 0 & 1 & 4 \\ 1 & 2 & 4 & 1 \\ 3 & 3 & 2 & 4 \end{pmatrix},\ (g_1^{''})^x=\begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix},\ (g_2^{'})^x=\begin{pmatrix} 4 & 0 & 3 & 1 \\ 2 & 0 & 2 & 2 \\ 2 & 4 & 3 & 2 \\ 2 & 0 & 2 & 0 \end{pmatrix},(g_2^{''})^x=\begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 3 & 0 & 4 \\ 0 & 2 & 1 & 4 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

Зашифруем в данной системе сообщение OK (0100111101001011).

Так как у нас рюкзак размером 4 x 4, то делим двоичный код сообщения на блоки по 4 символов: (0100), (1111), (0100), (1011). Далее следуем алгоритму шифрования, указанному выше.

В итоге получим зашифрованные блоки S_i:

$$S_1 = (g_1')^0 (g_1'')^1 (g_2')^0 (g_2'')^0 = \begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix} \qquad S_2 = (g_1')^1 (g_1'')^1 (g_2')^1 (g_2'')^1 = \begin{pmatrix} 4 & 2 & 3 & 0 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix}$$

$$S_3 = (g_1')^0 (g_1'')^1 (g_2')^0 (g_2'')^0 = \begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix} \qquad S_4 = (g_1')^1 (g_1'')^0 (g_2')^1 (g_2'')^1 = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 3 & 3 & 4 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 4 & 4 \end{pmatrix}$$

Для дешифровки сообщения S найдем элемент γ:

$$\gamma_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ \gamma_2 = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}, \ \gamma_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}, \ \gamma_4 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

Получили блочно-диагональные матрицы.

Применяя соответствующие алгоритмы, описанные выше, находим показатели элементов диэдральной группы:

$$b' = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}, \quad (b^2)' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$x = 1, b' = ab^y \Rightarrow (b')^{-1} = a^{-1}b' = b^y$$

$$a^{-1}b' = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}^y$$, откуда $y=1$.

Тогда элемент сообщение, соответствующее элементу γ_1, дешифруется как (0100).

Аналогично дешифруем сообщения, соответствующие γ_2, γ_3, γ_3, и получаем сообщения (1111), (0100), (1011). Выписываем сообщения в строчку и по таблице двоичных кодов символов латинского алфавита находим соответствующие буквы. При этом учитываем, что в таблице 1 символ представлен восьмиразрядной двоичной записью:

$$(0100111101001011) \rightarrow (01001111 \,|\, 01001011) \rightarrow \text{OK}.$$

References

1. Diffie W., Hellman M.E. New Directions in Cryptography. // IEEE Transactions on Information Theory, V. TI-22, 1977, pp. 644–654.

2. Salomaa A. Kriptografiya s otkrytym klyuchom [Public Key Cryptography]// Moscow: Mir Publ., 1995. p. 318.

3. Hellman M.E. The Mathematics of Public-Key Cryptography // Scientific American, V.241, No. 8, Aug 1982, pp.146–157.

4. Merkle R.C., Hellman M.E. Hiding information and signatures in Trapdoor Knapsack // IEEE Transactions on Information Theory, V.24, No. 5, Sep 1978, pp. 525–530.

5. Kharin Yu.S., Bernik V.I., Matveev G.V. Matematicheskie osnovy kriptologii: uchebnoe posobie [Mathematical Fundamentals of Cryptology: Reference Book] // Minsk: Belorussian State University, 1999,p. 319.

6. Henk C.A. van Tilborg. Encyclopedia of Cryptography and Security // Science, 2005, 697 p.

7. Harris M.E. Finite groups containing an intrinsic 2-component of Chevalley type over field of odd order // Transactions of the American math.soc. V.272, No. 1, 1982, pp. 1 – 65.

Сурина Альфия Адгамовна, аспирант ЮУрГУ. E-mail: dallila87@mail.ru

Зюляркина Наталья Дмитриевна, к. ф.-м. н., доцент ЮУрГУ.

Alfiya Adgamovna Surina, PhD student of South Ural State University. E-mail: dallila87@mail.ru

Natalia Dmitrievna Ziuliarkina, Cand. Sc. Physics and Mathematics, associate professor of South Ural State University.