ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 2
2015

А. А. Сурина (Челябинск, ЮУрГУ). **Рюкзачная криптосистема на основе прямого произведения циклических групп.**

Для обеспечения информационной безопасности в настоящее время широко применяются ассиметричные алгоритмы. Наиболее распространенными являются алгоритмы шифрования, основанные на задаче факторизации. К достоинствам этих алгоритмов следует отнести наличие элементов большого порядка и сложность нахождения дискретного логарифма. Однако системы, использующие подобные алгоритмы шифрования, с усовершенствованием технических средств требуют постоянного изменения. Для преодоления криптографических слабостей вводятся новые варианты, например, рюкзачные схемы, которые являются достаточно гибкими.

Определение 1. Пусть даны группа G и две ее подгруппы G_1 и G_2, причем выполнены следующие условия:

1) G_1 и G_2 являются нормальными подгруппами группы G,

2) пересечение $G_1 \bigcap G_2$ состоит только из единицы e,

3) каждый элемент группы G может быть представлен в виде произведения a_1a_2, где $a_1 \in G_1$, $a_2 \in G_2$.

Тогда группа G называется прямым произведением своих подгрупп G_1 и G_2 и записывается как $G = G_1 \times G_2$.

Определение 2. Группа, порожденная одним элементом, называется *циклической*.

Пример 1. Группы Z, Z_n являются циклическими группами. Этими группами исчерпываются — с точностью до изоморфизма — все циклические группы.

Циклическая группа порядка mn, где m и n взаимно простые, разлагается в прямое произведение подгрупп порядков m, n.

Пусть $G = G_1 \times G_2 \times \cdots \times G_n$. Тогда любой элемент $g \in G$ однозначно представляется в виде $g = g_1 \cdot g_2 \cdot \ldots \cdot g_n$, где $g_i \in G_i$.

Заметим, что G_i — циклическая группа и $G_i = \langle g_i \rangle$ $|g_i| = m_i$, то любой элемент $g \in G = G_1 \times G_2 \times ... \times G_n$ однозначно представляется в виде $g = g_1^{k_1} \times g_2^{k_2} \times \cdots \times g_n^{k_n}$, где $k_i \in Z_{m_i}$.

Рассмотрим следующую рюкзачную криптосистему, основанную на вычислениях в прямом произведении циклических подгрупп группы G.

Пусть $G = GL_n(q)$. Рассмотрим в G систему элементов:

$$g_1 = \begin{pmatrix} \alpha_1 & 0 & \ldots & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & .. & 0 & 1 & 0 \\ 0 & \ldots & \ldots & 0 & 1 \end{pmatrix}, \; g_2 = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 \\ 0 & \alpha_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & .. & 0 & 1 & 0 \\ 0 & \ldots & \ldots & 0 & 1 \end{pmatrix}, \ldots, \; g_n = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & .. & 0 & 1 & 0 \\ 0 & \ldots & \ldots & 0 & \alpha_n \end{pmatrix}.$$

Порядок элемента α_1 в поле $F_q : |\alpha_1| = k_1$, элемента α_2 в поле $F_q : |\alpha_2| = k_2, \ldots, \alpha_n$ в поле $F_q : |\alpha_n| = k_n$.

Для удобства вычислений можно выбрать $k_1 = k_2 = \cdots = k_n$.

Тогда подгруппа, порожденная элементами $\langle g_1, g_2, \ldots, g_n \rangle$, будет являться прямым произведением подгрупп $\langle g_1, g_2, \ldots, g_n \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle$. Заметим, что

для любого элемента $g \in \langle g_1,\ g_2, \ldots,\ g_n\rangle$ существует простой алгоритм нахождения таких $a_1,\ a_2, \ldots, a_n$, где $a_i \in Z_{k_i}$, что $g = g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n}$ (при условии, что задача о нахождении дискретного логарифма в поле F_q легко разрешима).

Таким образом, система элементов $g_1, g_2, \ldots, g_n$ удовлетворяет условиям, описанным в модификации, рассмотренной в параграфе 2.1, и является рюкзачной системой.

В качестве маскирующего изоморфизма можно рассмотреть сопряжение с помощью специально подобранного элемента $x \in GL_n(q)$ такого, что g_i^x — не диагональная матрица.

П р и м е р 2. Рассмотрим циклическую группу в Z_5 и выберем в ней элементы g_1, g_2, g_3 и g_4:

$$g_1 = \begin{pmatrix} 2&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1&0&0&0\\ 0&3&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&4&0\\ 0&0&0&3 \end{pmatrix}, \quad g_4 = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&2 \end{pmatrix}.$$

Заметим, что $\langle g_1,\ g_2, g_3,\ g_4\rangle$ является прямым произведением подгрупп $\langle g_1\rangle$, $\langle g_2\rangle$, $\langle g_3\rangle$ и $\langle g_4\rangle$, каждая из которых имеет порядок 4.

В качестве маскирующего изоморфизма рассмотрим сопряжение посредством элемента x. Элемент x нужно выбирать так, чтобы элементы g_i^x не имели блочно-диагональный вид:

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

Вычислим набор $(g_1^x, g_2^x, g_3^x, g_4^x)$, который будет являться открытым ключом:

$$g_1^x = \begin{pmatrix} 3&4&4&0\\ 3&2&1&0\\ 4&3&4&0\\ 4&3&3&1 \end{pmatrix}, \quad g_2^x = \begin{pmatrix} 4&1&0&4\\ 1&3&0&3\\ 0&0&1&0\\ 4&3&0&3 \end{pmatrix}, \quad g_3^x = \begin{pmatrix} 3&0&3&1\\ 1&0&2&2\\ 3&1&0&0\\ 2&4&1&1 \end{pmatrix}, \quad g_4^x = \begin{pmatrix} 4&4&0&3\\ 1&4&0&1\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}.$$

Зашифруем в данной системе сообщение (3, 1, 4, 2):

$$(3,\ 1,\ 4,\ 2) \to S = (g_1^x)^3 (g_2^x)^1 (g_3^x)^4 (g_4^x)^2 = \begin{pmatrix} 2&1&3&3\\ 0&4&2&1\\ 3&1&2&0\\ 2&4&1&3 \end{pmatrix}.$$

Для дешифровки сообщения S найдем элемент γ:

$$\gamma = xgx^{-1} = \begin{pmatrix} 3&0&0&0\\ 0&3&0&0\\ 0&0&1&0\\ 0&0&0&4 \end{pmatrix}$$

$$\begin{cases} 2^k = 3,\\ 3^s = 3,\\ 4^t = 1,\\ 3^t 2^l = 4; \end{cases} \quad \begin{cases} k = 3,\\ s = 1,\\ 4^t = 1\\ 3^t 2^l = 4; \end{cases} \quad \begin{cases} k = 3,\\ s = 1,\\ t = 4\\ l = 2. \end{cases}$$

Поэтому, $g = a^2 b^1 c^4$ и открытый текст имеет вид (2, 1, 4).

СПИСОК ЛИТЕРАТУРЫ

1. *Diffie W.*, *Hellman M. E.* New Directions in Cryptography. — IEEE Transactions on Information Theory, 1977, v. IT-22, is. 6, p. 644–654.
2. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995, 318 с.