С. А. Теньшова
(ГрГУ им. Я. Купалы, Гродно)

ПРОТОКОЛЫ ОБМЕНА КЛЮЧАМИ, ОСНОВАННЫЕ НА ЗАДАЧЕ КРАТНОГО СОПРЯЖЕНИЯ В ГРУППЕ КОС B_4

Обозначим через B_n группу кос, заданную с помощью образующих и определяющих соотношений:

$$\left\langle \sigma_1,...,\sigma_{n-1} \left| \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i для |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} для |i-j| = 1 \end{array} \right. \right\rangle.$$

Элементы группы будем называть n-косами.

С группами кос связаны две трудноразрешимые задачи, на основе которых строятся криптосистемы с открытым ключом.

1) Задача сопряжения: для двух данных сопряженных элементов $u, w \in B_n$ требуется найти элемент $v \in B_n$ такой, что $w = v^{-1}uv$.

2) Задача кратного сопряжения: для m данных пар сопряженных элементов $(u_1, w_1),...,(u_m, w_m) \in B_n$, о которых известно, что они сопряженных с помощью одного и того же элемента, найти $v \in B_n$ такой, что $w_i = v^{-1}u_iv$, для всех $i \in \{1,...,m\}$.

Приведем протокол обмена ключами, предложенный в [1,2]:

Открытые ключи: $\{g_1,...,g_m\} \subset B_n$.

Секретные ключи: Алиса: a; Боб: b.

Алиса: Посылает Бобу в открытом доступе сопряженные элементы $ag_1a^{-1},...,ag_ma^{-1}$.

Боб: Посылает Алисе в открытом доступе сопряженные элементы $bg_1b^{-1},...,bg_mb^{-1}$.

Секретный ключ: $K = aba^{-1}b^{-1}$.

В докладе изучаются атаки на криптосистему, основанную на задаче кратного сопряжения в группе кос B_4. В частности приводится построение графов $SSS(\sigma)$ - множеств и ориентированных графов $USS(x)$ – множеств в группе B_4.

Литература

1 Anshel, I. Anshel, M. Fisher, B. and Goldfeld, D. *New key agreement protocols in braid group cryptography*, CT-RSA 2001 (San Francisco), Springer Lect. Notes in Comp. Sci. 2020 (2001), 1–15.

2 I. Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Research Letters 6 (1999), 287–291.