ОБЗОР КРИПТОГРАФИЧЕСКИХ СИСТЕМ В ГРУППАХ КОС

Паршина Д.А., Горбенко И.Д.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Безопасности Информационных Технологий,
тел. (057) 702-14-25, E-mail: dashaparshina@mail.ru

The past several years have seen an explosion of interest in the cryptographic applications of non-commutative braid groups in particular are especially desirable, as they provide difficult computational problems and can be implemented quite efficiently. Several different groups of researches have proposed numerous cryptographic protocols that make use of braid groups. This expository paper discusses the specifications and responses of both the M.Anshel,I.Anshel, and Goldfeld Commutator and the Co et al. Diffie-Hellman Conjugacy key exchange protocols.

На протяжении нескольких последних лет заметно вырос интерес к криптографическим приложениям, основанным на преобразованиях в некоммутативных группах. Группы кос в частности представляют особый интерес в силу своей эффективности при обеспечении трудоёмких вычислительных процессов. Различными группами исследователей были предложены протоколы с преобразованиями в группе кос. Данная работа посвящена описанию основных криптографических преобразований в кос-группах, обзору некоторых протоколов, использующих данные преобразования, а также рассмотрению самых распространённых вопросов в этой области[1].

Коса из n-ломаных нитей – объект который состоит из двух параллельных плоскостей P_0 и P_1 в трёх мерном пространстве R^3, который состоит из упорядоченног множества точек a1,a2,… an ϵ P0 , b1,b2,… bn ϵ P1 и из n – простых ломаных $l_1,l_2,\dots l_n$, которые не пересекаются между собой, пересекая каждую плоскость P_t между P_0 и P_1 и соединяют точки $\{a_i\}$ с точками $\{b_i\}$.

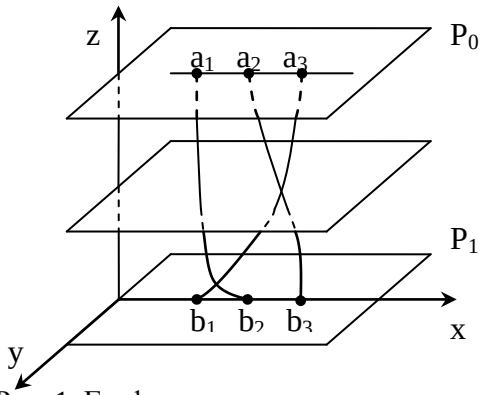

Рис. 1. Графическое представление косы

Косы из n-нитей, аналогично перестановкам владеют природной структурой групп. Пусть есть две косы A и B. Операция умножения кос определяется как: вертикальное сжимание и расположение одна над одной (рис. 2а). Нейтральным элементом в группе кос является коса с вертикально расположенными нитями (рис. 2б). Обратный элемент в группе кос задаётся вертикальным отображением (рис. 2в).

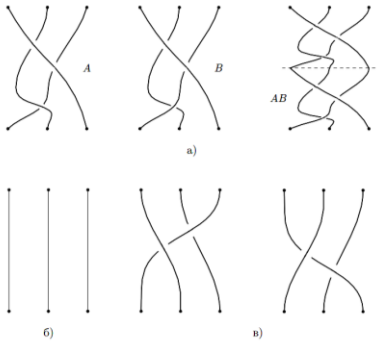

Рис. 2. Операции в группе кос: а)умножение б)нейтральный элемент в)обратный элемент

Фундаментальная коса - $\Delta_n \in B_n$, это коса алгебраическое представление которой имеет вид: $\Delta_n = (\sigma_1 \ldots \sigma_{n-1})(\sigma_1 \ldots \sigma_{n-2}) \ldots \sigma_1$, где σ_i – образующий элемент.

Основные соотношения в группе кос направлены на изменение формы записи, при этом не изменяя изоморфного класса косы.

Дальняя коммутативность – если существует два пересечения, которые находятся на большом расстоянии друг от друга по горизонтали, но близко по вертикали (не существует ни одного пересечения, которое находится выше одного из них, но ниже другого), порядок существующих элементов σ_i и σ_j изменится на σ_j и σ_i:

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \text{ при условии } |i-j| \geq 2 \quad (1)$$

Второе движение Рейдемейстра – пусть две нити косы находятся на близком расстоянии друг от друга и не пересекаются, тогда одну из этих нитей можно «накласть» на другую, то есть провести сверху другой, что можно описать соотношением:

$$\sigma_i^{-1}\sigma_i = \sigma_i\sigma_i^{-1} = e, \text{ где } e \text{ – нейтральный элемент.} \quad (2)$$

Третье движение Рейдемейстра – движение, которое в теории узлов описывается формулой:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \text{ при условии } 1 \leq i \leq n-2 \quad (3)$$

Если для некоторой косы существуют три точки попарных пересечений трёх разных нитей косы, которые находятся рядом, при этом одна из нитей проходит выше (ниже) других двух, тогда используя соотношение (3) можно протянуть над (под) двумя другими (рис. 3).

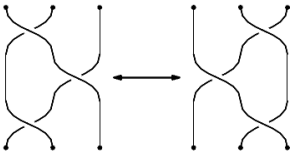

Рис. 3. Третье движение Рейдемейстра

Фундаментальной в теории кос является теорема Артина: группа кос B_n, изоморфна абстрактной группе, порождённой образующими $b_1, b_2, \ldots b_{n-1}$, которые удовлетворяют соотношениям (1), (2), (3). В алгебраическом виде это можно записать так:

$$\left\langle \sigma_1,\ldots,\sigma_{n-1} \middle| \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \text{для} \, |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{для} \, |i-j| = 1 \end{array} \right\rangle \quad (4)$$

Приступим к рассмотрению криптографических алгоритмов, базирующихся на группах кос, предварительно разбив их на четыре класса: системы обмена ключами, системы шифрования – расшифрования, системы аутентификации и системы подписи [2].

Среди ***систем обмена ключами*** выделяют две основных – это схема Аншеля-Аншеля –Гольдфельда и схема, аналогичная алгоритму Диффи-Хеллмана. Итак, в криптоалгоритме Аншеля-Аншеля-Гольдфельда в качестве открытого ключа принимается два набора кос $\{\{p1, \ldots, pn\}, \{q1, \ldots, qm\}\} \in Bn$. Секретный ключ U, принадлежащий A, состоит из l нитей и их инверсий. Аналогично секретный ключ V, принадлежащий B, состоит из m нитей и их инверсий. Обмен происходит следующим образом:

• A генерирует косу $s = u(p_1, \ldots, p_l)$, и использует её, чтобы сгенерировать сопряжённые $q_1' = sq_1s^{-1}, \ldots, q_m' = sq_ms^{-1}$; пересылает $q_1' \ldots q_m'$.

• B генерирует косу $r = v(q_1, \ldots, q_m)$, и использует её, чтобы сгенерировать сопряжённые $p_1' = rp_1r^{-1}, \ldots, p_m' = sq_ms^{-1}$; пересылает $p_1' \ldots q_l'$.

• A вычисляет $t_A = su(p_1, \ldots, p_l)^{-1}$.

• B вычисляет $t_B = v(q_1, \ldots, q_m)r^{-1}$.

• Искомый ключ $t_A = t_B$[3].

Далее рассмотрим протокол, предложенный К.Н. Ко, основой которого является протокол Диффи-Хеллмана. Здесь, открытый ключ p это определённая коса в группе B_n. Секретный ключ принадлежащий A представляет собой косу s из подгруппы L B_n, а секретный ключ B – косу r из подгруппы U B_n. Обмен ключами происходит таким образом:

• A генерирует сопряжение $p' = sps^{-1}$ и пересылает его B;

• B генерирует сопряжение $p'' = rpr^{-1}$ и пересылает его A;

• A вычисляет $t_A = sp''s^{-1}$;

• B вычисляет $t_B = rp'r^{-1}$;

Искомый ключ $t_A = t_B$.

Схема шифрования - расшифрования. Данная схема была предложена К.Н.Ко. Пусть есть группа кос B_n, и её подгруппа L B_n (соответственно U B_n), порождённая элементами $\sigma_1, \ldots, \sigma_{m-1}$ (соответственно $\sigma_{m+1}, \ldots, \sigma_{n-1}$) из m=n/2. Каждая коса из L B_n будет коммутативна каждой косе из U B_n. h – безколизийная однонаправленная хеш-функция. $(h(b_1) \neq h(b_2))$, $B_n \rightarrow \{0, 1\}^N$.

Алгоритм генерации ключевой пары:

Выбирается открытая коса p∈ Bn;

Выбирается персональный ключ s ∈ LBn;

• Вычисляется открытый ключ p` = sps^{-1};

• В качестве персонального ключа используется s, в качестве открытого ключа используется (p, p`).

Алгоритм зашифрования:

Вход: открытый ключ (p, p`), сообщение m из пространства $\{0, 1\}^N$, h – хеш- функция.

Выход: криптограмма e.

• Абонент выбирает случайную косу r из U B_n, и вычисляет $p'' = rpr^{-1}$

• Зашифровывает сообщение: $e = m \oplus h(rp'r^{-1})$

• В качестве криптограммы на выход подаётся (e, p″).

Алгоритм расшифрования:

Вход: персональный ключ s, криптограмма (e, p″), h – хеш- функция.

Выход: сообщение m.

• Абонент используя персональный ключ s вычисляет $m = e \oplus h(sp''s^{-1})$[4].

Системы аутентификации.. Как и в предыдущих системах, открытый ключ – это пара сопряжённых кос (p, p'), причём $p' = sps^{-1}$, принадлежащих группе B_n, сопряжённая коса s является секретным ключём A. В отличие от предыдущих систем и p и s принадлежат группе B_n, т.е мы не можем предположить, что s принадлежит какой-нибудь из подгрупп L B_n или же U B_n. Однако по прежнему предположим, что h-это односторонняя хэш-функция, в которой не происходит коллизий, заданная в группе B_n как $\{0,1\}^N$. Процедура аутентификация заключается в повторении *k* раз следующих трёх шагов:

• A выбирает случайную косу r, принадлежащую B_n и пересылает запрос $x = h(rp'r^{-1})$;

• B выбирает случайный бит c и пересылает его A;

• Для c=0, A пересылает $y=r$, и B проверяет $x = h(yp'y^{-1})$;

• Для c=1, A пересылает $y=rs$, и B проверяет $x= h(yp'y^{-1})$.

Электронная цифровая подпись. Две системы электронной подписи были предложны К.Н.Ко: применение второй схемы рекомендовано автором, однако на примере первой легче разобраться в самом алгоритме подписи, он является более наглядным и легко читаемым. Как и ранее открытый ключ представляет собой пару кос (p, p'), $p' = sps^{-1}$, принадлежащих группе B_n, а сопряжённая им коса s, принадлежащая B_n, является персональным ключом A. Будем использовать однонаправленную хэш-функцию H из {0,1}* в B_n.

На первом шаге выполняются следующие действия:

• A подписывает сообщение m при помощи $q' = sqs^{-1}$, где $q=H(m)$;

• B проверяет $q' \sim q$ и $p'q' \sim pq$.

Если A использует секретный ключ s, то получаем $q' = sqs^{-1}$ и $p'q' = spqs^{-1}$, то есть подпись принята. Возможная слабость данной системы может быть обусловлена тем, что возможно возникающие повторения могут раскрыть достаточно большое кол-во сопряжённых пар (q_i, q_i'), связанных с начальным сопряжением s, что делает возможным осуществление атаки на такую систему. Чтобы избежать этого, автор впоследствии несколько изменил общую схему путём включения дополнительных случайных кос.

Анализ рассмотренных криптографических систем показывает, что разработка алгоритмов, использующих группы кос является перспективным направлением в развитии современной криптографии[4]. Основные характеристики подобных систем приведены в таблице 1.

Таблица 1. Основные характеристики криптографических систем, базирующихся на группах кос

Входящее сообщение, бит	pnlog(n)
Зашифрованное сообщение, бит	4pnlog(n)
Скорость зашифрования, операций	$O(p^{2n}\log(n))$
Скорость расшифрования, операций	$O(p^{2n}\log(n))$
Длина персонального ключа, бит	0.5pnlog(n)
Длина открытого ключа, бит	3pnlog(n)
Сложность атаки «грубая сила»	$((n/2)!)^p = \exp(0.5pn\log(n))$

Литература:

1. D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, Length-based conjugacy search in the braid group, Contemp. Math. 418 (2006), 75–87.

2. E. Artin, Theory of Braids, Ann. of Math. 48 (1947) 101–126.

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

4. J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, J.H. Cheon, An efficient implementation of braid groups, AsiaCrypt 2001, Springer Lect. Notes in Comput. Sci., 2048 (2001) 144–156.