УДК 681.3.06

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СИСТЕМ В ГРУППАХ КОС

Д.А. ПАРШИНА, И.А. МИТЯЕВА, И.Д. ГОРБЕНКО

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.

Ключевые слова: преобразования в группах КОС, механизмы обмена ключами, схемы шифрования, механизмы аутентификации, электронная цифровая подпись, задача поиска сопряжений.

ВВЕДЕНИЕ

В последние годы проявляется интерес к криптографическим преобразованиях в некоммутативных группах КОС[1]. Их особенностью является эффективность при обеспечении трудоёмких вычислительных процессов. Рядом исследователей предложены криптографические протоколы, которые базируются на преобразованиях в группе КОС. В тоже время возможности практического применение преобразований в группах КОС ограничены из-за недостаточного их анализа, как раз в криптографических приложениях. Целью настоящей статьи является рассмотрение и первичный анализ основных криптографических преобразований и криптографических протоколов в КОС-группах, а также рассмотрению проблемных вопросов[1].

1. ОСНОВНЫЕ ПОНЯТИЯ О ГРУППАХ КОС

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 упорядоченного множества точек $a_1, a_2, ..., a_n \in P_0$, $b_1, b_2, ..., b_n \in P_1$, и из n – простых ломаных l_1, l_2, ... 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 $\{b_i\}$.

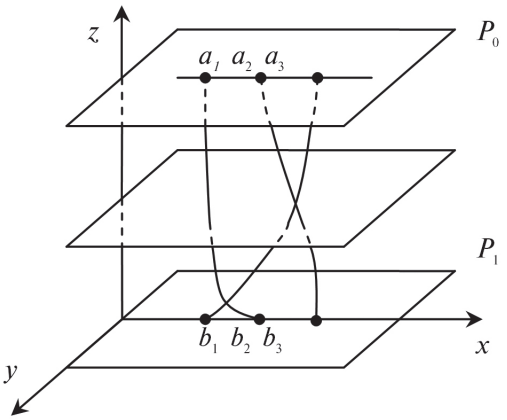

Рис. 1. Графическое представление косы

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. 2*а*). Нейтральным элементом в группе КОС является коса с вертикально расположенными нитями (рис. 2*б*). Обратный элемент в группе КОС задаётся вертикальным отображением (рис. 2*в*).

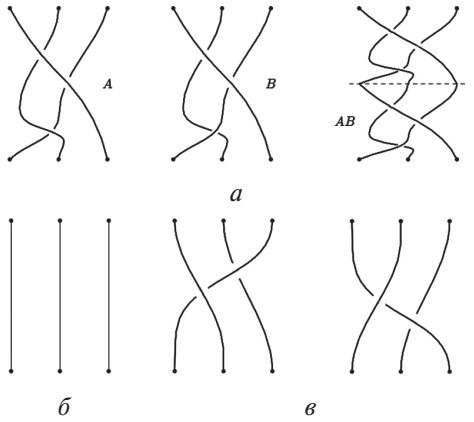

Рис. 2. Операции в группе кос:
а – умножение; *б* – нейтральный элемент;
в – обратный элемент

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

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

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:

$$\sigma_i^{-1}\sigma_i = \sigma_i\sigma_i^{-1} = e, \quad (2)$$

где e – нейтральный элемент.

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

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad (3)$$

при условии $1 \le i \le n-2$.

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, то её можно протянуть над (под) двумя другими (рис. 3).

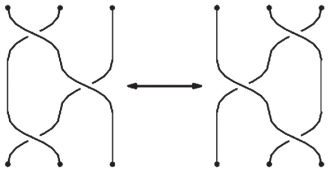

Рис. 3. Третье движение Рейдемейстра

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

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

2. КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ В ГРУППАХ КОС

К основным криптографическим преобразования в группах КОС относятся: механизмы обмена ключами, системы шифрования, аутентификации и цифровой подписи[2].

2.1. Механизмы обмена ключами

Среди *механизмов обмена ключами* можно выделить два основных – это протокол Аншеля-Аншеля-Гольдфельда и протокол, аналогичный алгоритму Диффи-Хеллмана. В протоколе Аншеля-Аншеля-Гольдфельда в качестве открытого ключа принимается два набора кос $\{\{p_1, ..., p_n\}, \{q_1, ..., q_m\}\} \in B_n$. 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 :

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

2. В генерирует косу $r = v(q_1, \ldots, q_m)$, и использует её, чтобы сгенерировать сопряжённые $p_1' = rp_1r^{-1}, ..., p_l' = rp_lr^{-1}$; пересылает $p_1'...p_l'$.

3. А вычисляет $t_A = su(p_1, ..., p_l)^{-1}$.

4. В вычисляет $t_B = v(q_1, ..., q_m)r^{-1}$.

Искомый ключ $t_A = t_B$[3].

Протокол, который предложен К.Н. Ко, базируется на классическом протоколе Диффи — Хеллмана. Здесь, открытый ключ p это определённая коса в группе B_n. Секретный ключ принадлежащий A представляет собой косу s из подгруппы LB_n, а секретный ключ B – косу r из подгруппы UB_n. Обмен ключами происходит таким образом:

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

2. В генерирует сопряжение $p'' = rpr^{-1}$ и пересылает его A;

3. А вычисляет $t_A = sp''s^{-1}$;

4. В вычисляет $t_B = rp'r^{-1}$;

Искомый ключ $t_A = t_B$.

2.2. Схема (метод) шифрования

Данная схема была предложена К.Н. Ко. Пусть есть группа кос B_n, и её подгруппа LB_n (соответственно UB_n), порождённая элементами σ_1, ..., σ_{m-1} (соответственно σ_{m+1}, ..., σ_{n-1}) из $m = n/2$. Каждая коса из LB_n будет коммутативна каждой косе из UB_n. h – безколизийная однонаправленная хеш-функция.

$$(h(b_1) \ne h(b_2)),\ B_n \to \{0, 1\}^N.$$

Алгоритм генерации ключевой пары:

1. Выбирается открытая коса $p \in B_n$;
2. Выбирается персональный ключ $s \in LB_n$;
3. Вычисляется открытый ключ $p' = sps^{-1}$;
4. В качестве персонального ключа используется s, в качестве открытого ключа пара (p, p')

Алгоритм зашифрования:

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

Выход: криптограмма e.

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

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

3. 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].

2.3. Механизмы 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 ключом 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 LB_n или же UB_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 аутентификации заключается в повторении k раз следующих трёх шагов:

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

2. В выбирает случайный бит c и пересылает его A;

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

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

2.4. Электронная цифровая подпись

Две системы электронной подписи были предложны K.H.Ko: 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:

1. A подписывает сообщение m при помощи $q_1' = sq_1s^{-1}$, где $q=H(m)$;

2. В проверяет $q' \approx q, p'q' \approx pq$.

Если A использует секретный ключ s, то получаем $q_1' = sq_1s^{-1}$, 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 $\left(q_i, q_i'\right)$, 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.

3. ОЦЕНКА КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ

Описанные выше преобразования в немалой степени завися от решения следующих задач.

3.1. Задача поиска корня

Пусть $(x,y) \in B_n \times B_n$ такие, что $y = x^c$, $c \in N$, $c \geq 2$, N – множество натуральных чисел. Задача нахождения корня состоит в нахождении такой косы $b \in B_n$, чтобы $y = b^c$, $c \geq 2$.

3.2. Задача декомпозиции кос

Пусть $(x,y) \in B_n \times B_n$ и $y = a_1xa_2$ для некоторых $(a_1, a_2) \in B_n \times B_n$. Задача декомпозиции кос состоит в нахождении такой пары $(b_1, b_2) \in B_n \times B_n$, чтобы $y = b_1xb_2$.

3.3. Криптографическое допущение

В данной схеме мы рассматриваем группу кос B_n, порожденную $\{\sigma_1,\sigma_2,...,\sigma_n\}$ и ее подгруппами

$$LB_n = \{\sigma_1,\sigma_2,...,\sigma_{n/2-1}\}$$

$$RB_n = \{\sigma_{n/2+1},\sigma_{n/2+2},...,\sigma_{n-1}\}$$

Связь этих групп определяется как:

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \ |i-j| > 1$$

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, \ |i-j| = 1$$

Т.е. мы имеем коммутативное свойство $\alpha\beta = \beta\alpha$ для любых $\alpha \in LB_n$ и $\beta \in RB_n$.

Пусть H_1: $B_n \rightarrow \{0,1\}^k$ – идеальная функция нахождения $\{0,1\}^k$ из косы.

Пусть H_2: $\{0,1\}^k \rightarrow B_n$ – идеальная функция нахождения косы из $\{0,1\}^k$.

Пусть c: $\{0,1\}^k \rightarrow B_n$.

Стойкость криптосистем с использованием кос-групп основывается на следующих проблемах:

1. Задача поиска сопряжений (CSP):

Пусть $(x, y) \in B_n \times B_n$ такие, что $y = a^{-1}xa$, где $a \in B_n$ или одной из подгрупп B_n. Задача – найти такое b, что $y = b^{-1}xb$.

2. Задача одновременного поиска множества сопряжений (MSCSP):

Пусть $(x_1,a^{-1}x_1a)...(x_r,a^{-1}x_ra) \in B_n \times B_n$ такие, что $y = a^{-1}xa$, где $a \in B_n$ или одной из подгрупп B_n. Задача – найти такое b, что $y = b^{-1}x_1b = a^{-1}x_1a$, ..., $b^{-1}x_rb = a^{-1}x_ra$.

3. Задача декомпозиции (*BDP*):

Пусть $(x, y) \in B_n \times B_n$ такие, что $y = a_1xa_2$ для $(a_1,a_2) \in LB_n \times LB_n$. Задача – найти пару $(b_1,b_2) \in LB_n \times LB_n$ такую, что $y = b_1xb_2$.

4. Задача одновременной множественной декомпозиции (MSBDP):

Пусть $(x_1,a_1x_1a_2)$ ... $(x_r,a_1x_ra_2) \in B_n \times B_n$ для $(a_1,a_2) \in LB_n \times LB_n$. Задача – найти пару $(b_1,b_2) \in LB_n \times LB_n$ такую, что $y = b_1x_1b_2 = a_1x_1a_2$, ..., $b_1x_rb_2 = a_1x_ra_2$.

5. Задача поиска корня (RP):

Пусть x = a^p, где a, $x \in B_n$ и $p \in N$. Задача поиска для экспоненты p – найти такую косу $b \in B_n$, чтобы $b^p = x$.

6. Задача выбора сопряженных элементов (*CDP*):

Пусть $(x, y) \in B_n \times B_n$. Задача – установить, являются ли x и y сопряженными, т.е. установить, существует ли такое $a \in B_n$ или одной из подгрупп B_n, что $y = a^{-1}xa$.

Исходя из вышеприведенного, рассмотрим три основные разновидности атак на криптосистемы, основанные на преобразованиях в группах кос:

1) использование решения задачи поиска сопряжений;

2) использование вероятностного подхода в B_n;

3) использование вспомогательной группы, как правило, в представлении Бурау[1].

3.4. Решение задачи поиска сопряжений

Наиболее очевидный способ атаки на кос-криптосистемы – решение задачи поиска сопряжений в B_n, который стал известен благодаря основополагающей работе Гарсайда. Последующие уточнения метода значительно улучшили его алгоритмическую эффективность.

Метод Гарсайда для решения задачи поиска сопряжений в B_n состоит в привязке к каждой косе b характерного конечного набора сопряжений b, называемого высшим множеством. Эль-Рифай и Мортон предложили заменить высшее множество его подмножеством – супер высшим множеством(*SSS*). Супер высшее множество меньше, следовательно, его легче определить. Под *SSS* подразумевается множество всех сопряжений b минимально возможной запутанности.

Для каждой косы b супер высшее множество конечно и алгоритмически вычислимо.

Две косы b и b' сопряжены тогда и только тогда, когда их *SSS*. Таким образом, предполагаем разрешимость задачи поиска сопряжений в B_n. В действительности, известны и более точные результаты. Введем следующее определение: фундаментальная коса – $\Delta_n \in B_n$, это коса, алгебраическая запись которой имеет вид:

$$\Delta_n = (\sigma_1 ... \sigma_{n-1})\,(\sigma_1 ... \sigma_{n-2}) ... \sigma_1.$$

Геометрический пример приведен для косы Δ_4, где любые две нити пересекаются положительно, кроме одной (рис. 1).

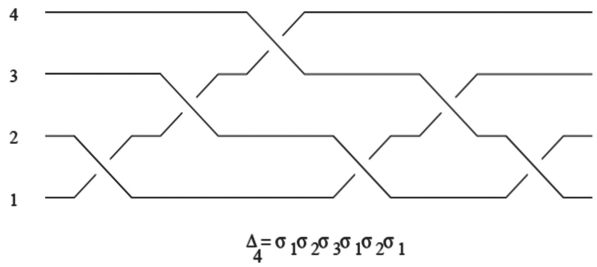

Рис. 4. Фундаментальная коса для Δ_4

Предположим, что b – коса в B_n и $(k; b_1 ..., b_r)$ – её нормальная форма. Если косы $\partial_+(b)$ и $\partial_-(b)$ определяются как

$$\partial_+(b) = \Delta_n^k b_2 ... b_r \varphi_n^k(b_1),$$

$$\partial_-(b) = \Delta_n^k \varphi_n^k(b_r) b_1 ... b_{r-1}, \qquad (5)$$

где φ_n – флип-автоморфизм, отображающий σ_i в σ_{n-i} для каждого i; считается что $\partial_+(b)$ (соответственно $\partial_-(b)$) получена циклированием (дециклированием) из b.

Косы $\partial_+(b)$ и $\partial_-(b)$ – сопряжения b. Дело в том, что если b – коса в B_n, не принадлежащая супер высшему множеству b, т.е. не имеет минимальной запутанности в этом классе сопряжений, тогда циклированием или дециклированием максимум $n(n-1)/2$ раз можно найти сопряжение b точно меньшей запутанности. Таким образом, повторяя эти действия, после конечного числа шагов мы получим сопряжение b^* для b, лежащее в супер высшем множестве b.

Приведем полную процедуру принятия решения о сопряженности кос b и b', проиллюстрированную на рис. 5:

1) Используя циклирование (cycling) и дециклирование (decycling), найти b^* для b, лежащую в супер высшем множестве (*SSS*) b;

2) Используя циклирование и дециклирование, найти b^* для b', лежащую в $SSS(b')$;

3) Определить $SSS(b)$, насыщая $\{b^*\}$ простыми сопряжениями;

4) b и b' будут сопряженными, если b'^* принадлежит

Отслеживая сопряжение кос на каждом шагу, можно не только определить, являются ли b и b' сопряженными, но также получить сопряжение, если оно существует, т.е. если b и b' сопряжены. Таким образом, решаются две задачи: задача сопряжения и задача поиска сопряжений в B_n[2].

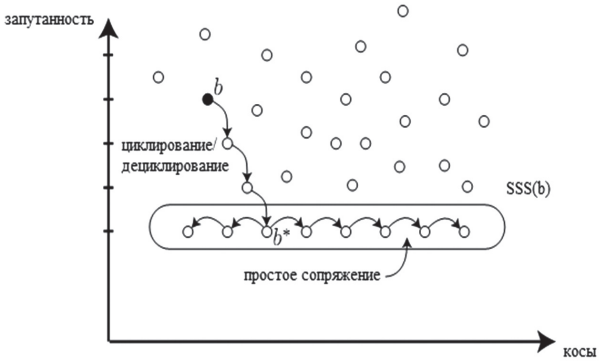

Рис. 5. Решение задачи сопряжения: определение SSS и его перечисление (точки показывают сопряжения b)

Что касается сложности, так как циклирование и дециклирование постоянное количество раз гарантирует, что нормальная длина будет уменьшаться, если это возможно, нахождение сопряжения в *SSS* имеет линейную сложность по сравнению со сложностью для исходной косы. Потом остается только сложность перечисления $SSS(b)$.

Совсем недавно В. Гебхардт предложил новое совершенствование. Это совершенствование состоит в замене *SSS* еще меньшим множеством, называемым ультра высшим множеством (*USS*). Рассмотрим действие циклирования на *USS*: начиная с косы b в ее *SSS*, не обязательно возвращаться к исходной b в циклировании *SSS*, но, безусловно, циклирование, в конечном счете, становится периодичным. Таким образом, можно разделить *SSS* на несколько орбит, состоящих из цикличных частей и остатков (рис. 6).

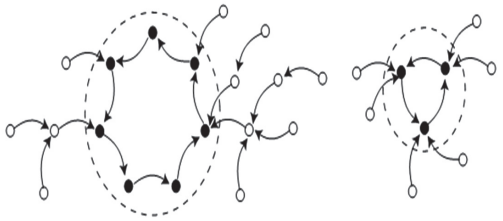

Рис. 6. Действие циклирования в *SSS*; черным показаны элементы *USS*

Гебхардт определяет ультра высшее множество как объединение цикличных частей орбиты. По определению *USS* является подмножеством *SSS*, и Гебхардт показывает, что *USS* может быть использовано вместо *SSS*: как и для *SSS*, элементы *USS* легко определить, а потом подсчитать и все *USS*, используя минимальные простые элементы. Дело в том, что размер *USS* обычно гораздо меньше *SSS*, типично его размер линеен относительно длины исходной косы, тогда как размер *SSS* экспоненциален. В таких случаях *USS* можно определить быстро и проблема сопряжения будет решена. На данный момент это не доказано, но сложность метода может быть сведена к полиномиальной.

3.5. Атаки, основанные на длине

Помимо использования конкретного решения задачи поиска сопряжений, также кос-криптосистемы можно атаковать, используя вероятностный эвристический подход: всякий раз, когда вероятность успеха более чем незначительна, этого может быть достаточно для того, чтоб поставить под угрозу кос-криптосистему. Основанные на длине атаки относятся к этому семейству. Общий принцип таких атак состоит в попытке получить сопряжение для пары (p, p'), начиная с p', которая должна быть получена из p и многократно сопрягающаяся с p' в новую косу $tp't^{-1}$ так, что длина или запутанность $tp't^{-1}$ будет минимальной.

При осуществлении атаки проверяется, случается ли, что новое сопряжение $tp't^{-1}$ равно p. Атака особо применима к протоколам обмена ключами, основанным на задаче одновременного поиска множества сопряжений, потому что, в данном случае, злоумышленник знает несколько пар сопряженных кос, связанных с одной и той же сопряженной косой. Атака, описанная Хофхайнцем и Штайнвандтом, аналогична, но она включает в себя еще один шаг, и поэтому является более мощной. Вместо проверки, является ли $tp't^{-1}$ равным p, злоумышленник проверяет, чтобы «расстояние перестановки» между $tp't^{-1}$ и p не превышало 1, т.е. пытается найти такую перестановку f, что $tp't^{-1}$ равно простому сопряжению fpf^{-1}. Нахождение возможных перестановок является очень легким, так как оно сводится к решению задачи поиска сопряжений в симметричной группе S_n. При этом улучшении вероятность успешного осуществления атаки достигает 99% для протокола согласования ключей Аншеля-Аншеля-Гольдфельда в B_{80} при $l = m = 20$ и исходными косами p_i и q_j длины 5 или 10[3].

3.6. Атаки, основанные на линейных представлениях

Третий способ атаки кос-криптосистем – использование линейного представления кос-групп, т.е. отображение кос-групп в группы матриц. Так как задача сопряжения в линейной группе легка, так что можно думать о решении задачи сопряженности таким способом.

Наиболее известным представлением кос-групп B_n является представление Бурау, линейное представление со значениями $GL_n(Z[t, t^{-1}])$. Представление Бурау для B_n, как известно, неточно для $n \geq 5$, но ядро очень мало, потому вероятность того что различные косы примут один и тот же образ Бурау незначительна [3].

Рассмотрим также результаты, полученные в результате анализа безопасности подобных систем.

Только уполномоченная сторона может проверить подпись (R_1, R_2, S_1, S_2, S_3, δ): *Только уполномоченная сторона владеет секретным ключом b, используя который вычисляет:*

$$R_3 = bR_1b^{-1}, m = H_1(R_3) \oplus S_3$$

$$R_4 = bR_2b^{-1}, S_4 = H_2\left[H_1(R_4) \oplus m\right]$$

$$\theta = b^{-1}S_1b.$$

Затем проверяет равенство $\delta = \left[S_4\theta\right]^c$. Если неуполномоченная сторона хочет проверить (R_1, R_2, S_1, S_2, S_3, δ), что она должна вычислить R_3, R_4, θ, что невозможно сделать без секретного ключа b.

Любой злоумышленник не может атаковать подпись

Любой злоумышленник не может получить секретный ключ (u_i, v_i), без знания которого невозможно вычислить R_1, R_2, R_3, R_4, S_1, S_2, поскольку вычисления основываются на задачах поиска сопряжений и декомпозиции кос. Предположим, злоумышленник подделал $\delta = \left[S_4d\right]^c$, но он не может определить S_4d из-за сложности задачи поиска корня. Таким образом, любой противник не может ни вычислить сообщение, ни выполнять проверки.

Никто не может снять подпись за исключением авторизованной группы T.

Не зная секретные ключи u_i, a, никто не может вычислить сертификат авторизации y_i и проверить равенство $S_4^c = \delta\theta^{'-1}$. Авторизованная группа T, имея секретный ключ a, может вычислить сертификат авторизации y_i и θ' и проверить равентво $S_4^c = \delta\theta^{'-1}$. Если равенство имеет место, авторизованная группа объявляет, что подпись осуществляется P_i (i=1,2,3,...,k).

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 табл. 1.

Таблица1

Основные характеристики криптографических систем, базирующихся на группах кос

Входящее сообщение, бит	$pn\log(n)$
Зашифрованное сообщение, бит	$4pn\log(n)$
Скорость зашифрования, операций	$O(p^{2n}\log(n))$
Скорость расшифрования, операций	$O(p^{2n}\log(n))$
Длина персонального ключа, бит	$0{,}5pn\log(n)$
Длина открытого ключа, бит	$3pn\log(n)$
Сложность атаки «грубая сила»	$((n/2)!)^p = \exp(0{,}5pn\log(n))$

ВЫВОДЫ

В целом важным фактором, влияющим на возможности осуществления атаки является способ генерации ключей. Так, например, атака Гебхардта возможна лишь при достаточно малом USS, что не всегда соответствует действительности. Из вышеизложенного следует, что вычисление $p' = sps^{-1}$ с исходной косой p не является лучшим способом генерации пары сопряженных кос. Действительно, установление ряда ограничений на ключи – довольно распространенная

ситуация, существует всего несколько криптосистем, в которых ключи могут быть выбраны в случайном порядке. Поэтому даже если некоторые авторы утверждают, что существующие атаки полностью нивелируют криптографию в группах кос, на данный момент, более разумным кажется заключить, что необходимо приложить больше усилий для построения доказуемо стойких крипо алгоритмов или же предоставлении доказательств того, что построение подобных крипто алгоритмов невозможно.

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.

Поступила в редколлегию 14.03.2012

Паршина Дарья Андреевна, студентка кафедры БИТ. Область научных интересов: криптографические протоколы в группах кос.

Митяева Ирина Андреевна, студентка кафедры БИТ. Область научных интересов: анализ криптографических протоколов в группах кос.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на с. 190.

УДК 681.3.06

Аналіз криптографічних систем в групах КОС/ Д.А. Паршина, І.А. Мітяєва, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 210–215.

Протягом кількох останніх років помітно зростає інтерес до криптографічних додатків, заснованих на перетвореннях у некомутативних групах. Групи КОС зокрема представляють особливий інтерес завдяки своїй ефективності при забезпеченні трудомістких обчислювальних процесів. Різними групами дослідників були запропоновані протоколи з перетвореннями в групах КОС. Дана робота присвячена опису основних криптографічних перетворень в кос-групах, огляду деяких протоколів, що використовують дані перетворення, а також розгляду найпоширеніших питань у цій галузі.

Ключові слова: перетворення в групах КОС, механізми обміну ключами, схеми шифрування, механізми автентифікації, електронний цифровий підпис, завдання пошуку сполучень

Табл. 1. Іл. 6. Бібліогр.: 4 найм.

UDC 681.3.06

Analysis of cryptographic system in braid groups / D.A. Parshina, I.A. Mityaeva, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 210–215.

The past several years have seen an explosion of interest in cryptographic applications based on transformations in non-communicative groups. Braid groups are of particular interest due to their efficiency in providing labour-consuming computational processes. Different groups of researchers have proposed protocols with transformations in the braid groups. The paper is devoted to describing the main cryptographic transformations in the braid groups, reviewing some protocols using the given transformations as well as considering the most common questions in this field.

Keywords: transformations in braid groups, key exchange mechanisms, encryption schemes, authentication mechanisms, digital signature, conjugation search problem.

Tab. 1. Fig. 6. Ref.: 4 items.