АНАЛИЗ УЯЗВИМОСТИ КРИПТОАЛГОРИТМОВ В ГРУППАХ КОС

Митяева И.А., Горбенко И.Д
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. Безопасности информационных технологий,
тел. (057) 702-14-25, E-mail: miaskad@gmail.com

In the last decade, a number of public key cryptosystems based on combinatorial group theoretic problems in braid groups have been proposed. These cryptosystems and some known attacks on them are represented in the given work.

Алгоритмы, основанные на преобразованиях в группах кос, являются одной из альтернативных ветвей криптографии. Криптосистема, основанная на косах – частный случай более общего подхода, впервые предложенного Аншелем, Аншелем и Гольфельдом. Позднее, на конференции CRYPTO'2000 была полностью описана идея создания данной криптосистемы. Ее ключевым моментом является задача эквивалентности. Существует алгоритм решения этой задачи за полиномиальное
время. Результатом его является каноническая форма n -косы, которая соответствует уникальной группе косы. Если мы преобразуем имеющееся произведение кос sps^{-1} в его каноническую форму, то нахождение исходных кос (множителей) будет иметь достаточно высокую сложность. Именно нахождение исходных кос является основной задачей криптоанализа рассматриваемых криптосистем.

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

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 $(x_1,a_1x_1a_2)\ldots(x_r,a_1x_ra_2) \in B_n \times B_n$ 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 $y = b_1x_1b_2 = a_1x_1a_2,\ldots, b_1x_rb_2 = a_1x_ra_2$.

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].

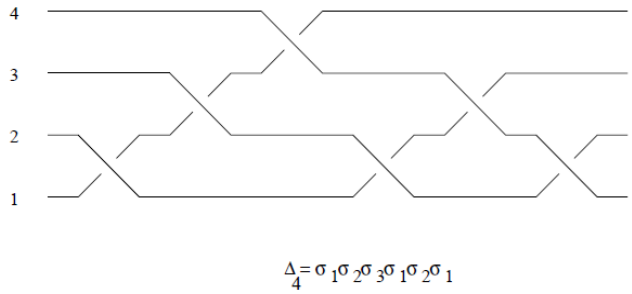
Решение задачи поиска сопряжений. Наиболее очевидный способ атаки на кос-криптосистемы – решение задачи поиска сопряжений в B_n, который стал известен благодаря основополагающей работе Гарсайда. Последующие уточнения метода значительно улучшили его алгоритмическую эффективность.

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 Bn. В действительности, известны и более точные результаты. Введем следующее определение: фундаментальная коса – $\Delta_n \in$ Bn, это коса, алгебраическая запись которой имеет вид:

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

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



$\Delta_4 = \sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1$

Рис. 1. Фундаментальная коса для Δ_4

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

$$\partial_+(b) = \Delta_n^k b_2 \ldots b_r \varphi_n^k(b_1),\ \partial_-(b) = \Delta_n^k \varphi_n^k(b_r) b_1 \ldots b_{r-1}, \qquad (1)$$

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.2:

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 SSS(b).

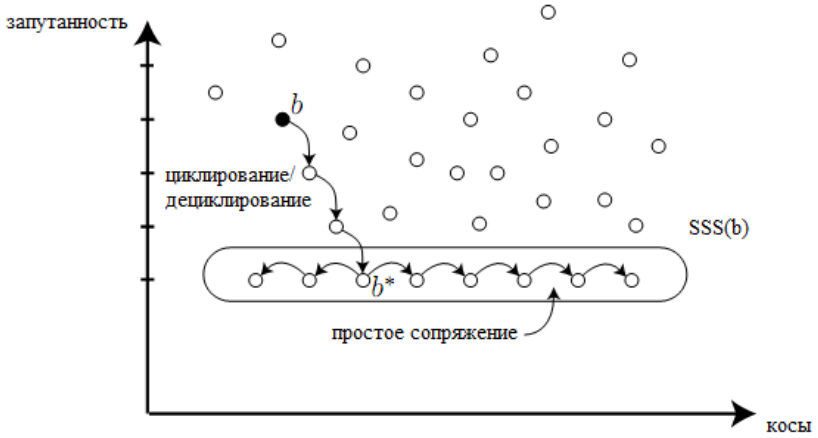


Рис. 3.Решение задачи сопряжения: определение SSS и его перечисление (точки показывают сопряжения b)

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].

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.4).

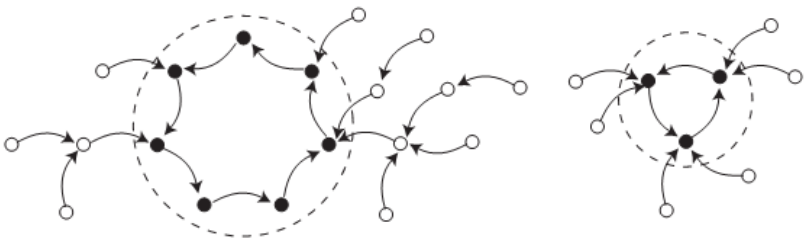


Рис. 4. Действие циклирования в SSS; черным показаны элементы USS

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.

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 $\hat{f}p\hat{f}^{-1}$. 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].

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].

В заключение, можно сделать вывод, что важным фактором 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. И это неудивительно, так как установление ряда ограничений на ключи – довольно распространенная ситуация, существует всего несколько криптосистем, где 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 крипоалгоритмов или же предоставлении доказательств того, что построение подобных криптоалгоритмов 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. J.S. Birman and T.E. Brendle, Braids: a survey, in: Handbook of knot theory, Elsevier, B.V., Amsterdam, 2005, pp. 19–103.

3. S.J. Lee & E.K. Lee, Potential weakness of the commutator key agreement protocol based on braid groups, Eurocrypt 2002, Springer Lect. Notes in Comput. Sci. 2332 (2002) 14–28.