Математика и Математическое моделирование
Сетевое научное издание
http://mathmelpub.ru ISSN 2412-5911

Ссылка на статью:
// Математика и математическое моделирование. 2018. №6. С. 88–111.
DOI: **10.24108/mathm.0618.0000151**
Представлена в редакцию: 04.11.2018

УДК 519.40

Асимметричная схема передачи секретного ключа по открытому каналу в k-детерминированных группах с условиями $C(3)$–$T(6)$

Безверхний Н. В.[1,*], **Никитина М. В.**[2] *nbezv@mail.ru

[1]МГТУ им. Н.Э. Баумана, Москва, Россия;
[2]Российская корпорация средств связи, Москва, Россия

Статья посвящена построению односторонней функции в группах с условиями малого сокращения $C(3)$–$T(6)$ и разработке схемы формирования секретного ключа при обмене информацией по открытому каналу связи. Описаны алгоритмы непосредственного построения ключей и несанкционированного восстановления секретной информации по открытым данным. Оценивается сложность решения обеих задач. Доказано, что прямая задача имеет линейную, а обратная — экспоненциальную сложность. Сложность алгоритмов оценивается в терминах числа областей групповых диаграмм. В статье используются геометрические методы комбинаторной теории групп и, в частности, теории групп с условиями малого сокращения $C(3)$–$T(6)$.

Ключевые слова: группа; копредставление; групповая диаграмма; проблема равенства

Введение

В комбинаторной теории групп для задания группы G используют так называемые копредставления: $G = (X; R)$. Здесь X — конечный алфавит, соответствующий множеству образующих группы G и содержащий вместе с каждым символом x его инверсию x^{-1}, а R — конечное множество слов в указанном алфавите — определяющие соотношения. Множество R содержит все циклические перестановки и инверсии своих элементов: вместе со словом $xy \dots z$ множество R содержит слово $z^{-1} \dots y^{-1}x^{-1}$. Множество слов, замкнутое относительно инверсий и циклических перестановок элементов называют симметризованным.

При таком задании группы ее элементам соответствуют классы эквивалентных слов. В каждом таком классе слов бесконечно много. Ниже определяется понятие несократимого представителя класса эквивалентных слов и приводится алгоритм построения несократимого представителя, дается оценка его сложности.

В статье используются геометрические методы комбинаторной теории групп, а именно, метод диаграмм над группами, базирующийся на лемме Ван Кампена [1, 2, 3], в соответствии

с которой слово представляет нейтральный элемент группы тогда и только тогда, когда существует односвязная диаграмма с граничной меткой, равной этому слову.

С точки зрения приложений решенная здесь задача представляет интерес при построении односторонних функций, использующихся в криптографии при обмене информацией по открытому каналу связи. А именно, предлагается схема передачи информации по открытому каналу, с помощью которой строится секретный ключ. Приводятся оценки сложности как прямого алгоритма построения ключа, так и обратного, то есть несанкционированного восстановления секретного ключа по известной открытой информации.

Большой интерес представляют такие алгоритмы, для которых сложность последней операции превышает полиномиальную. Построенный в данной работе алгоритм обладает указанным свойством.

В дальнейшем мы будем использовать следующие обозначения: $u \equiv v$ — слово u графически равно слову v; $u = v$ — слово u эквивалентно слову v, т.е. равно ему в группе G; $|u|$ — длина слова u.

1. Диаграммы над группами

Допустим, что группа G имеет копредставление $G = (X; R)$.

Пусть E^2 — евклидова плоскость. Для $S \subseteq E^2$ через ∂S обозначена граница множества S, через $\bar{S}$ — его топологическое замыкание. Вершина — это некоторая точка из E^2. Ребро — ограниченное подмножество из E^2, гомеоморфное открытому единичному интервалу. Область — ограниченное множество, гомеоморфное открытому единичному кругу. Карта M — конечный набор попарно непересекающихся вершин, ребер и областей, удовлетворяющих следующим условиям:

1) если e — ребро из M, то имеются вершины a и b (не обязательно различные), такие, что $\bar{e} = e \cup \{a\} \cup \{b\}$;

2) граница ∂D каждой области D из M связна, причем для некоторых ребер $e_1, \ldots, e_n$ из M имеем $\partial D = \bar{e_1} \cup \ldots \cup \bar{e_n}$.

Буква M будет использоваться также для обозначения теоретико-множественного объединения вершин, ребер и областей соответствующей диаграммы. Если $\bar{e} = e \cup \{a\} \cup \{b\}$, то говорят, что a и b — концы ребра e. Замкнутое ребро — это ребро e вместе с его концами.

Если e — ориентированное ребро, v_1 — начальная вершина этого ребра, а v_2 — конечная вершина, то ребро, обратное к ребру e, обозначается через e^{-1} и направлено от v_2 к v_1.

Путь — это последовательность ориентированных замкнутых ребер $e_1, \ldots, e_n$, такая, что начальная вершина ребра e_{i+1} — это конечная вершина ребра e_i, $1 \leq i \leq n-1$. Концы пути — это начальная вершина ребра e_1 и конечная вершина ребра e_n.

Замкнутый путь, или цикл, — это такой путь, в котором начальная вершина ребра e_1 является конечной вершиной ребра e_n.

Путь называется приведенным, если он не содержит последовательной пары ребер вида ee^{-1}. Приведенный путь $e_1 \ldots e_n$ называется простым, если при $i \neq j$ начальные вершины ребер e_i и e_j различны.

Если D — область в карте M, то любой цикл минимальной длины, включающий в себя все ребра из ∂D, в котором все ребра ориентированы в соответствии с ориентацией границы области D, то есть по часовой стрелке, и при обходе всех этих ребер область остается справа, называется граничным циклом этой области.

Если карта M связна и односвязна, то граничный цикл для M — это ориентированный против часовой стрелки цикл α минимальной длины, содержащий все ребра границы ∂M и не имеющий самопересечений в том смысле, что если e_i и e_{i+1} — последовательные ребра цикла α, такие, что e_i оканчивается вершиной v, то e_i^{-1} и e_{i+1} — соседние ребра в циклически упорядоченном множестве ребер карты M с началом v. Такое правило обхода карты гарантирует, что если M имеет вид восьмерки, то есть предтавляет собой пару касающихся внешним образом кругов, то при обходе границы карта всегда будет оставаться слева.

Диаграммой над группой $G = (X; R)$, или R-диаграммой, называется ориентированная карта M вместе с функцией метки φ, сопоставляющей каждому ориентированному ребру e карты M метку $\varphi(e)$ — слово из образующих таким образом, что если e — ориентированное ребро из M, а e^{-1} — противоположным образом ориентированное ребро, то $\varphi(e^{-1}) \equiv \varphi(e)^{-1}$. При этом метка граничного цикла любой области D из M графически равна некоторому определяющему соотношению из R: $\varphi(\partial D) \equiv r \in R$.

2. Группы с условиями малого сокращения

Рассмотрим группу с копредставлением $G = (X; R)$. Ниже всегда считаем множество R симметризованным. Предположим, что r_1 и r_2 — различные элементы из R, такие, что $r_1 \equiv bc_1$ и $r_2 \equiv bc_2$. В этом случае элемент b называется куском относительно множества R. Таким образом, кусок — это общее начало двух различных определяющих соотношений.

Предположения о малом сокращении состоят в том, что куски — относительно малые части элементов из R. Метрическое условие $C'(\lambda)$, где λ — действительное число из интервала $(0;\ 1)$, означает следующее: если $r \in R$, $r \equiv bc$, где b — кусок, то $|b| < \lambda|r|$.

Тесно связанным с приведенным является неметрическое условие $C(p)$, где p — некоторое натуральное число. Условие $C(p)$ состоит в том, что никакой элемент из R не является произведением менее чем p кусков.

Сформулируем условие $T(q)$. Пусть $3 \le h < q$. Предположим, что $r_1, \ldots, r_h$ — элементы из R, такие, что последовательные элементы r_i, r_{i+1} не являются взаимно обратными. Тогда по крайней мере одно из произведений $r_1r_2, \ldots, r_{h-1}r_h, r_hr_1$ приведено.

Пусть M — произвольная диаграмма над F. Допустим, что D_1 и D_2 — области из M с общим ребром $e \subseteq \partial D_1 \cap \partial D_2$. Пусть $e\delta_1$ и $\delta_2 e^{-1}$ — граничные циклы областей D_1 и D_2 соответственно. Положим $\varphi(\delta_1) = f_1$ и $\varphi(\delta_2) = f_2$. Пара областей (D_1, D_2) называется сократимой, если $f_2 \equiv f_1^{-1}$. Диаграмма M называется приведенной, если она не содержит сократимых пар областей.

Пусть M — некоторая карта. Граничной вершиной в M, соответственно, граничным ребром в M мы будем называть вершину, ребро из ∂M. Граничной областью карты M называется такая область D из M, что $\partial D \cap \partial M \neq \varnothing$. Таким образом, если D — граничная область карты M, то $\partial D \cap \partial M$ не обязано содержать некоторое ребро, но может состоять из одной и более вершин. Вершина, ребро или область карты M, не являющиеся граничными, называются внутренними.

Если v — вершина карты M, то $d(v)$ — степень вершины v, равная числу ребер инцидентных вершине v. Если оба конца некоторого ребра e совпадают с v, мы считаем e дважды. Если D — область из M, то $d(D)$ — степень области D определяется как число ребер в граничном цикле для D. Символ $i(D)$ обозначает число внутренних ребер из ∂D, причем ребро, встречающееся в граничном цикле для D дважды, считается два раза.

Плодотворным оказывается использование геометрической интерпретации условий $C(p)$ и $T(q)$, сформулированной в следующей теореме.

Теорема 1 ([2]). Пусть R — симметризованное множество слов, M — приведенная R-диаграмма.

Если множество R удовлетворяет условию $C(k)$, то каждая область D из M, такая, что $\partial D \cap \partial M$ не содержит ребер, имеет степень $d(D) \geq k$. При этом метка любого внутреннего ребра является куском.

Если множество R удовлетворяет условию $T(m)$, то каждая внутренняя вершина v карты M имеет степень $d(v) \geq m$.

Класс групп с условиями $C(3)$–$T(6)$ обладает замечательным свойством, отличающим его от других классов типа $C(p)$–$T(q)$: в группах с условиями $T(q)$ при $q > 4$ все куски имеют единичную длину [4].

Далее приведем два важных понятия: R-и $\bar{R}$-сокращения. С их помощью будет определен несократимый представитель класса эквивалентных слов, о котором говорилось во введении.

Будем говорить, что в слове w есть R-сокращение [5, 6, 7], если существует элемент $r \in R$ такой, что:

1) $r \equiv r_1 r_2$;

2) $w \equiv w_1 w_2 w_3$;

3) $r_1 \equiv w_2$;

4) слово r_2 либо пусто, либо является куском;

5) слова $w_1 r_2^{-1}$, $r_2^{-1} w_3$ несократимы в свободной группе.

При замене слова w равным ему в группе G словом $w_1 r_2^{-1} w_3$ будем говорить, что в w выполнено R-сокращение. R-сокращение в слове w, являющемся степенью некоторого слова v: $w = v^s$, является длинным, если $|w_2| \geq |v|$. Если же $|w_2| < |v|$, то R-сокращение называется коротким.

Пример. Рассмотрим группу $G = (X; R)$, где $X = \{a, b, c\}$, а $R = \{abc, acb\}$. Пусть имеется также слово $w = abb$. Используя определяющее соотношение $r_1 = abc$, заменяем в

слове w подслово ab куском c^{-1}. Получаем $w = c^{-1}b$. Таким образом, мы выполнили в слове w короткое R-сокращение.

Пусть теперь у нас есть слово $w = v^2$, где $v = acb$, т.е. $w = acbacb$. Используя определяющее соотношение $r_2 = acb$, заменяем первое вхождение acb в w пустым словом. В данном случае мы выполнили длинное R-сокращение в слове w, так как $|acb| = |v|$. Если в любой циклической перестановке слова w нет R-сокращений, то слово w называется циклически R-несократимым.

Понятие $\bar{R}$-сокращения определим с помощью диаграмм. Также дадим геометрическое определение R-сокращения. Для этого нам понадобятся понятия полосы и дэновской области.

Рассмотрим диаграмму M. Область $D \subset M$ называется дэновской [8], если $\partial D \cap \partial M$ — последовательная часть границы ∂M, т.е. $\partial D \cap \partial M = p$ — подпуть в граничных циклах области D и диаграммы M; $i(D) \in \{0, 1\}$.

Полосой [8] в диаграмме M называется поддиаграмма $\Pi = \bigcup\limits_{i=1}^{k} D_i$ со следующими свойствами:

• $\partial D_i \cap \partial M = p_i$ — последовательная часть границы ∂M при всех $i = 1, \ldots, k$;

• $\partial\Pi \cap \partial M = p$ — последовательная часть границы ∂M;

• если $k = 3$, то $i(D_1) = i(D_2) = i(D_3) = 2$, причем соседние области имеют общее ребро, а все три области полосы имеют общую вершину;

• если $k > 3$, $k = 2l + 1$, то $i(D_1) = i(D_2) = i(D_{2l}) = i(D_{2l+1}) = 2$, $i(D_3) = i(D_5) = \ldots$ $\ldots = i(D_{2l-3}) = i(D_{2l-1}) = 3$, $i(D_4) = i(D_6) = \ldots = i(D_{2l-4}) = i(D_{2l-2}) = 2$;

• $\partial D_i \cap \partial D_{i+1}$ — ребро ($i = 1, \ldots, k - 1$).

Пусть Π — полоса в диаграмме M. Граничным словом области $D_i \subset \Pi$ называется метка пути $\partial D_i \cap \partial M$, прочитанная в соответствии с ориентацией области D_i. Граничным словом полосы Π называется метка пути $\partial\Pi \cap \partial M$, прочитанная в направлении, противоположном ориентации границы ∂M. Аналогично определяется граничное слово дэновской области.

Будем говорить, что в слове v есть R-сокращение, если существует связная односвязная диаграмма M над группой $G = (X; R)$, в которой существует дэновская область, граничное слово которой является подсловом в v. В слове v есть $\bar{R}$-сокращение, если существует связная односвязная диаграмма M над копредставлением $G = (X; R)$, в которой существует полоса Π, граничное слово которой является подсловом в v.

Для любого циклически несократимого в свободной группе слова w, не равного единице в группе G, существует циклически $R, \bar{R}$-несократимое слово w_0, сопряженное с w в G.

Действительно, из определений следует, что в результате $R, \bar{R}$-сокращения длина слова строго уменьшается. Поэтому, записав произвольное слово w на окружности C и выполнив в его циклических перестановках все возможные $R, \bar{R}$-сокращения, получим непустое слово w_0, в циклических перестановках которого нет $R, \bar{R}$-сокращений. Пустым слово w_0 быть не может, поскольку исходное слово w представляло в группе G элемент, не равный единице.

3. Схема открытого распределения ключей в группах с условием $C(3)$–$T(6)$

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ. Таким образом, необходимым условием использования симметричных криптосистем является получение пользователями общего секретного ключа. При этом доступ к ключу потенциального злоумышленника должен быть исключен.

Целью данной работы является разработка асимметричной схемы передачи секретного ключа по открытому каналу, основанной на проблеме слов в группах, копредставление которых удовлетворяет условиям $C(3)$–$T(6)$.

Был разработан следующий протокол получения секретного ключа.

Участники процесса: 1) абонент A, 2) абонент B, 3) противник E.

Открытая информация:

1) группа $G = (X; R)$, копредставление которой удовлетворяет условиям $C(3)$–$T(6)$;

2) слово w в алфавите X, представляющее некоторый элемент группы G.

Алгоритм получения секретного ключа абонентом A.

1) Абонент A выбирает произвольное целое число k, отличное от нуля, (закрытый ключ 1) и произвольное слово v_A в алфавите X (закрытый ключ 2). Далее абонент A вычисляет открытый ключ $K_1 = w^k v_A$ и отправляет его абоненту B.

2) Абонент B умножает K_1 на w^l слева и на w^{-l} справа и передает A полученный открытый ключ $K_1' = w^{k+l} v_A w^{-l}$.

3) Абонент A умножает K_1' на w^{-k} слева и на w^k справа и получает секретный ключ $K_1'' = w^l v_A w^{k-l}$.

Алгоритм получения секретного ключа абонентом B.

1) Абонент B выбирает произвольное целое число l, отличное от нуля, (закрытый ключ 3) и произвольное слово v_B в алфавите X (закрытый ключ 4). Далее абонент B вычисляет открытый ключ $K_2 = w^l v_B$ и отправляет его абоненту A.

2) Абонент A умножает K_2 на $v_A w^k$ слева и передает B полученный открытый ключ $K_2' = v_A w^{k+l} v_B$.

3) Абонент B умножает K_2' на $v_B^{-1} w^{-2l}$ справа и на w^l слева и получает секретный ключ $K_2'' = w^l v_A w^{k-l} = K_1''$.

При этом к слову w предъявляются следующие требования:

1) $w \neq 1$ в группе G;

2) слово w должно представлять в группе G элемент бесконечного порядка.

Необходимость выполнения первого требования очевидна, так как если $w = 1$ в группе G, то все его степени $w^n = 1$ в G, и тогда в качестве открытого ключа будут использоваться закрытые ключи (v_A и v_B), что недопустимо.

Второе требование также является необходимым, поскольку если w представляет элемент конечного порядка, то противнику нужно будет найти не k и l, а остатки от деления k и l

на порядок p слова w, что является гораздо более простой задачей. Заметим, что алгоритм нахождения порядка слова w описан в статьях [9], [10]. Ниже будет предложен алгоритм построения слова w, в соответствии с которым требование 2) бесконечности порядка будет выполняться автоматически.

От группы G, используемой для шифрования, требуется только выполнение условий $C(3)$–$T(6)$.

Следует отметить, что если информация о группе G и слове w не является общеизвестной, а выбирается, например, абонентом A, то абонент A отправляет абоненту B в качестве открытого ключа K_1, G, w.

4. Односторонняя функция для получения открытого ключа

Структура слов, используемых в качестве пересылаемых открытых ключей такова, что позволяет идентифицировать входящие в их состав структурные элементы, в том числе и секретные, основываясь только на знании общего вида слова.

Например, для нахождения подслова v_A и степени k в составе слова $v_A w^k$ противнику достаточно знать, что данное слово состоит из случайного слова, к которому справа присоединена степень некоторого известного всем слова. Согласно общепринятым допущениям, используемым при построении криптосистем, подобные сведения у противника E имеются. В результате возникает необходимость сокрытия структурных элементов слов, используемых в качестве открытых ключей.

В настоящей работе используется схема получения открытого ключа с помощью односторонних функций. Протокол получения открытого ключа включает преобразования, обратные к R- и $\bar{R}_3$-сокращениям. Данные преобразования определяются следующим образом.

Будем говорить, что в слове w есть R-удлинение, если существует элемент $r \in R$, такой, что:

1) $r \equiv r_1 r_2$;

2) $w \equiv w_1 w_2 w_3$;

3) $r_1 \equiv w_2$;

4) слово r_1 является куском.

В случае замены слова w равным ему в группе G словом $w_1 r_2^{-1} w_3$ будем говорить, что в w выполнено R-удлинение.

Будем говорить, что в слове w есть $\bar{R}_3$-удлинение, если существуют элементы r_1, r_2, $r_3 \in R$, такие, что:

1) $r_1 \equiv r_{11} r_{12} r_{13}$;

2) $r_2 \equiv r_{21} r_{22} r_{23}$;

3) $r_3 \equiv r_{31} r_{32} r_{33}$;

4) $w \equiv w_1 w_2 w_3 w_4$;

5) $r_{13} \equiv w_2^{-1}$;

6) $r_{32} \equiv w_3^{-1}$;

7) $r_{23} \equiv r_2^{-1}$;

8) $r_{22} \equiv r_{33}^{-1}$;

9) слова $r_{11}, r_{12}, r_{13}, r_{21}, r_{22}, r_{23}, w_2, w_3$ являются кусками.

В случае замены слова w равным ему в группе G словом $w_1 r_{11} r_{21} r_{31} w_4$ будем говорить, что в w выполнено $\bar{R}_3$-удлинение.

Перед тем, как перейти к подробному описанию процедуры получения открытого ключа, отметим следующую ее особенность, связанную с вхождением в его состав случайного слова. Указанное случайное слово может оказаться таким, что в открытом ключе можно будет провести такое количество свободных, R- и $\bar{R}$-сокращений, что длина открытого ключа существенно уменьшиться. Это приведет к упрощению задачи противника за счет снижения верхней границы числа вариантов при подборе открытого ключа.

Действительно, если открытый ключ, представляющий собой переработанное описанным ниже способом слово K, имеет большую длину, то это может означать, что либо степень слова w велика при малой длине слова v, либо наоборот, степень слова w мала, но слово v имеет большую длину. А возможен и третий вариант, когда и степень большая, и длина слова v. Если же открытый ключ имеет маленькую длину, то и вариантов для перебора различный комбинаций типа (n, v), где n — неизвестный показатель степени, а v — неизвестное слово, становится значительно меньше.

Для того чтобы предотвратить нежелательные сокращения в слове w^n, в качестве него выбираем внешнюю граничную метку однослойной кольцевой диаграммы M, с границей $\partial M = \sigma \cup \tau$. При этом все области в M имеют в точности по два внутренних ребра, одну вершину либо на σ, либо на τ, а области с единственной вершиной на σ чередуются с областями, имеющими единственную вершину на τ. Такую кольцевую диаграмму будем называть $(2,2)$-слоем, или 1-слойной кольцевой диаграммой типа $(2,2)$. Легко проверить, что граничные метки такой диаграммы $\bar{R}, R$-несократимы.

Заметим, что в соответствии со сказанным в пункте 3, необходимо гарантировать бесконечность порядка слова w. Это требование выполняется, поскольку конечность порядка w означала бы, в соответствии с леммой Ван Кампена [2], существование односвязной диаграммы с меткой w^p, на границу которой можно наклеить $(2,2)$-слой, что невозможно, так как метка $(2,2)$-слоя $\bar{R}, R$-несократима, а приведенная односвязная диаграмма над ($C(3)$–$T(6)$)-группой должна содержать полосы или дэновские области [8], т.е. ее граничная метка должна быть $\bar{R}$- или R-сократимой.

Итак, процедура получения открытого ключа на основе некоторого слова включает два последовательных этапа.

Этап 1. Генерация однослойной кольцевой диаграммы с $(2,2)$-слоем, на внешней границе которого читается слово $\delta = w^n$. Следующая лемма гарантирует возможность построения периодического $(2,2)$-слоя.

Лемма 1. Для любого копредставления $G = (X; R)$ с условиями $C(3)$–$T(6)$ существует кольцевая периодическая 1-слойная диаграмма типа $(2, 2)$.

Доказательство. Будем считать, что уже построена 1-слойная дисковая диаграмма M, имеющая форму прямоугольника, в котором две противоположные стороны обозначены σ и τ, а все области имеют по одной вершине на σ или τ и по ребру на τ или σ, соответственно, или наоборот. При этом области первого и второго типов строго чередуются при движении вдоль сторон σ, τ. Две оставшиеся стороны прямоугольника имеют метки $a,\ b \in X$.

Для периодичности необходима возможность склейки такого прямоугольника в 1-слойную кольцевую диаграмму. Последнее можно сделать, добавив соотношений abc, bac к множеству R и образующий c к X. Полученное таким образом новое соотношение определяет область, замыкающую $(2, 2)$-слой в кольцо. Может оказаться, что такая область уже существует, и тогда описанные преобразования копредставления $(X; R)$ не понадобятся.

Важно, что описанное преобразование не меняет свойство копредставления $C(3)$, так как слово ab не становится куском после преобразования, иначе в R слово, необходимое для зацикливания слоя, существовало и до преобразовния.

Что касается условия $T(6)$, то построение диаграммы с вершиной, имеющей внутреннюю степень меньше 6, из областей с метками abc, bac невозможно: проверка тривиальная.

Тем не менее, сохранить условие $T(6)$ удается не всегда. Представим себе, что 6 определяющих соотношений $r_1,\ \ldots,\ r_6$ позволяют построить односвязную диаграмму M_6, в которой 6 областей с граничными метками $r_1, \ldots, r_6$ имеют единственную общую вершину A: $d_{M_6}(A) = 6$. При этом области занумерованы в порядке следования при обходе вершины A против часовой стрелки: $D_1, \ldots, D_6$.

Возможна следующая ситуация: $\varphi(\partial D_1) \equiv axy$, $\varphi(\partial D_2) \equiv x^{-1}bz$. После введения в множество R нового соотношения $r \equiv abc$, можно вырезать из M_6 области D_1, D_2 и вклеить на их место область $D : \varphi(\partial D) \equiv abc$. В результате получим приведенную диаграмму M_5, в которой $d(A) = 5$, что противоречит условию $T(6)$.

Таким образом, введение в множество R нового соотношения не решает задачу зацикливания $(2, 2)$-слоя.

Покажем, что при построении $(2, 2)$-слоя можно устроить его зацикливание. Представим его в виде двух отрезков σ и τ на параллельных прямых, между которыми вклеиваются треугольные области, причем, первая слева область D_1 имеет на верхнем отрезке σ ребро, а на нижнем τ — только вершину, а вторая область D_2 наоборот: на σ только вершину, а на τ — ребро, и так далее при движении вдоль отрезков σ и τ области с ребром на τ и вершиной на σ чередуются с областями с ребром на σ и вершиной на τ.

Обозначим метки областей с нечетными номерами через $\varphi(\partial D_{2k+1}) \equiv a_{2k+1}b_{2k+1}a_{2k+2}^{-1}$. Тогда метки областей с четными номерами равны $\varphi(\partial D_{2k+2}) \equiv a_{2k+2}a_{2k+3}^{-1}c_{2k+2}$. Уточним, что метки b_{2k+1} являются подсловами слова $\varphi(\sigma)$, а метки c_{2k+2} — слова $\varphi(\tau)$, метки $b_{\ldots}$ имеют только нечетные номера, а метки $c_{\ldots}$ — только четные.

Здесь мы временно, в рамках доказательства данной леммы, ориентируем границу диаграммы по часовой стрелке.

Поскольку множества X, R образующих и определяющих соотношений конечны, то при некоторых k, l, $k < l$ метка a_{2k+1} совпадет с меткой a_{2l+1}, и тогда вместо области D_{2l+1} с меткой $\varphi(\partial D_{2l+1}) \equiv a_{2l+1}b_{2l+1}a_{2l+2}^{-1}$ можно будет использовать область D_{2k+1}, к которой приклеить D_{2k+2}, и так далее до D_{2l}, после которой снова вернуться к D_{2k+1}. Так строится циклический $(2,2)$-слой, который можно замкнуть в 1-слойную кольцевую диаграмму.

Заметим, что при построении односторонней функции в рамках данной статьи представляет интерес работа со словами w большой длины. Возможно, расстояние от области D_{2l+1} до области D_{2k+1} не достаточно велико. Тогда можно воспользоваться k-детерминированностью группы G и продолжить построение 1-слойной диаграммы, приклеив к области D_{2k+1} не D_{2l+2}, а любую другую из оставшихся $k-2$ областей с буквой a_{2l+1} в граничной метке. Повторяем такие подмены до тех пор, пока не будет построено достаточно длинное слово.

Лемма доказана. Теорема доказана.

Этап 2. Маскирующие преобразования слова:

2.1) вставка между k-й и $(k+1)$-й позициями тривиального слова $x_i x_i^{-1}$, где $x_i \in X$ выбирается случайным образом;

2.2) R-удлинение в k-й позиции;

2.3) свободное сокращение в k-й позиции, если такое сокращение возможно;

2.4) вставка между k-й и $(k+1)$-й позициями определяющего слова $r_i \in R$, которое выбирается случайным образом;

2.5) $\bar{R}_3$-удлинение в k-й позиции, если такое удлинение возможно.

Уточним некоторые детали реализации предложенной схемы.

1. Тип преобразования и позиция k в слове δ выбираются случайным образом.

2. Преобразования применяются к отдельному вхождению слова w в δ.

3. Число преобразований в каждом вхождении w в δ представляет собой случайное число из отрезка $[0,5|w|;2|w|]$. Данный диапазон был выбран на основании экспериментальных данных и обеспечивает до 100% модифицированных вхождений слова w в δ, а также достаточную (на основании визуальной оценки) вариабельность этих вхождений. Число преобразований в остальных частях открытого ключа (т.е. подсловах v_A, v_B) составляет $2|v_A|$, $2|v_B|$ для каждого вхождения слова v_A, v_B в δ.

Сформулируем требования, предъявляемые к процедуре получения открытого ключа. Пусть процедура принимает на вход некоторое слово δ и возвращает слово ε. Требуется, чтобы:

1) $\varepsilon = \delta$ в группе G;

2) $\varepsilon \neq \delta$ в свободной группе;

3) для любого подслова вида w^n в δ такого, что $\delta = \gamma_1 w^n \gamma_2$ для некоторых γ_1 и γ_2, не существует такого w_1, $w_1 = w$ в группе G, что $\varepsilon = \gamma_1' w_1^n \gamma_2'$ для некоторых γ_1' и γ_2';

4) не должно существовать простого алгоритма, который позволял бы по ε найти δ или секретные ключи.

Покажем, что описанная выше процедура получения открытого ключа удовлетворяет указанным требованиям.

Требование 1 выполняется, так как ни одно из преобразований из 1)–5) не приводит к нарушению равенства слов в группе G.

Рассмотрим требование 2. Поскольку каждое из преобразований 1)–5) переводит данное слово δ в слово δ_1, не равное ему графически, то нарушение требования 2 может наблюдаться в двух случаях: 1) когда исходное слово не подвергалось преобразованиям, 2) когда подверглось парам взаимно обратных преобразований. (Примером, иллюстрирующим случай 2), является вставка между k-й и $(k+1)$-й позициями тривиального слова $x_i x_i^{-1}$ с последующим свободным сокращением в $(k+1)$-й и $(k+2)$-й позициях полученного слова.)

Вероятность реализации случая 1) можно минимизировать за счет увеличения общего числа преобразований. Снижение частоты возникновения случая 2) достигается, в частности, за счет случайного выбора позиции в слове δ, которое подвергается преобразованию.

Кроме того, снижению частоты последовательности взаимно обратных преобразований 3), 1) способствует случайный выбор тривиального слова для вставки. Так, например, если множество X содержит n_X символов (и соответственно n_X обратных к ним) и в некоторой позиции слова δ было произведено свободное сокращение с образованием слова δ_1 длины n, то вероятность обратного преобразования с учетом случайного выбора позиции для модификации и случайного выбора пары $x_i x_i^{-1}$ составляет $1/(n2n_X)$ (вставка в начало и конец слова δ_1 считается одним и тем же преобразованием). И конечно можно производить нечетное число преобразований и таким образом исключить принципиальную возможность реализации случая 2).

Условие 3 выполняется за счет того, что преобразования применяются к каждому вхождению w в δ. При этом вид преобразований и позиция в слове w выбираются случайно, вследствие чего ситуация, при которой во всех n вхождениях w в v будут произведены одинаковые преобразования, является маловероятной.

Для того чтобы определить, выполняется ли условие 4, проанализируем возможные действия противника E. Требования 2 и 3 гарантируют, что противник не имеет возможности узнать секретные слова и степени, исходя из вида открытых ключей и их произведений.

Таким образом, единственным возможным вариантом действий E является поиск секретных ключей посредством перебора. В процессе сравнения открытого ключа со словом-кандидатом противник производит преобразования, которые использовались при синтезе открытого ключа, ограничиваясь при этом теми из них, которые приводят к уменьшению длины слова: это свободные сокращения, R-сокращения и $\bar{R}_3$-сокращения.

В процессе синтеза открытого ключа преобразования, обратные указанным, проводились случайным образом, т.е. их последовательность и локализация неизвестны E. В результате

велика вероятность того, что противник произведет сокращения не там, где были до этого сделаны удлинения, в результате чего, приведение слова к несократимому виду потребует большего количества операций, по сравнению с оптимальной стратегией, в точности соответствующей выполнению преобразований, обратных тем, что выполнялись абонентами A и B при построении сообщений.

Не зная заранее секретные значения n, v, противник проверяет равенство слов в группе для произвольных значений n', v', которые он перебирает по определенной схеме. Во-первых, каждая такая проверка оказывается достаточно трудоемкой процедурой, во-вторых, число таких проверок тоже велико и определяется длиной секретного слова v и величиной показателя степени n. Оценка сложности процедуры восстановления значений n, v по открытому ключу будет дана ниже. Но начнем с оценки сложности прямой процедуры построения открытого ключа.

5. Оценка сложности получения открытого ключа

Верхняя оценка сложности получения открытого ключа может быть получена на основании трудоемкости наиболее сложной операции. Под трудоемкостью T_k операции k будем понимать количество сравнений букв, необходимых для проведения преобразования.

Начнем с оценки трудоемкости этапа 2 получения открытого ключа.

Очевидно, что наименее трудоемкими являются преобразования 1) и 4), которые не требуют проведения сравнения букв. Таким образом, считаем, что $T_1 = T_4 = O(1)$.

Следующим по трудоемкости является преобразование 3) — свободное сокращение. Данная операция требует не более двух сравнений: чтобы узнать, есть ли в k-й позиции свободное сокращение, нужно сравнить X_k с X_{k-1} и X_k с X_{k+1}. Следовательно, T_3 также есть $O(1)$.

Оценим трудоемкость операции 2) — R-удлинения. Напомним, что в группах с условиями $C(p)$–$T(q)$ при $q > 4$ все куски имеют единичную длину. Учитывая этот факт, а также то, что множество R симметризовано, получим, что поиск требуемого куска достаточно провести среди начальных символов определяющих соотношений.

Так как в R имеется как минимум два определяющих соотношения, имеющих общее начало, согласно определению куска, то в худшем случае для получения подходящего определяющего соотношения потребуется $n_R - 1$ сравнений, где n_R — мощность множества R. Таким образом, трудоемкость операции R-удлинения составит $(n_R - 1)$.

Наиболее трудоемким является преобразование 5) — $\bar{R}_3$-удлинение. В процессе $\bar{R}_3$-удлинения ищутся два однобуквенных совпадения (трудоемкость при этом составит $(n_R - 1) + (n_R - 1) = 2(n_R - 1)$) и одно двухбуквенное. Поскольку каждое двухбуквенное начало встречается в R не более одного раза, суммарная трудоемкость $\bar{R}_3$-удлинения равна $T_5 = 2(n_R - 1) + 2n_R = 4n_R - 2$ при наличии в R соотношения с соответствующим двухбуквенным началом.

Возникает проблема существования двухбуквенного начала в слове из множества R. Как мы видели в доказательстве леммы 1, искусственное добавление к множеству R пары определяющих соотношений abc, bac и новых образующих c, c^{-1} к множеству X не нарушает свойства $C(3)$ копредставления $G = (X, R)$, но может привести к нарушению условия $T(6)$. Значит, надо искать тройку областей, образующих полосу, которую можно использовать для $\bar{R}_3$-удлинения данного слова в выбранной позиции. В случае неудачи заменять $\bar{R}_3$-удлинение R-удлинением.

Таким образом, наиболее трудоемкой операцией в общем случае является $\bar{R}_3$-удлинение, поэтому в дальнейшем трудоемкость будет оцениваться количеством построенных полос.

Теперь мы в состоянии дать верхнюю оценку трудоемкости этапа 2 процедуры получения открытого ключа. Подсчитаем число преобразований, которым подвергается исходное слово $\delta \in \{w^k v_A, w^{k+l} v_A w^{-l}, w^l v_B, v_A w^{k+l} v_B\}$.

Слово δ состоит из подслов вида w^{n_1} и подслов $v \in \{v_A, v_B\}$. Количество модификаций в каждом подслове $w \in \delta$ не превосходит $2|w|$, а в каждом подслове v составляет в точности $2|v|$. Для удобства будем использовать такие слова v, что $|v| = (n_2 - 1)|w|$, для некоторого $n_2 \in \mathbb{N}$.

Верхняя оценка $T_{(2)}$ трудоемкости этапа 2 получения открытого ключа получается, если полагать, что все преобразования, производимые в слове K, являются $\bar{R}_3$-удлинениями. Пусть слово δ длины n содержит n_1 подслов w и длина подслова v в δ ограничена сверху числом $n_2|w|$. Тогда трудоемкость этапа 2 получения открытого ключа не превосходит величины

$$T_{(2)} = (2|w|n_1 + 2n_2|w|)T_5 = 2(n_1 + n_2)|w|(4n_R - 2) = 2n(4n_R - 2).$$

Теперь оценим сложность получения $(2, 2)$-слоя, на границе которого читается слово δ, $|\delta| = n$ (этап 1 получения открытого ключа).

Заметим, что построение $(2, 2)$-слоя, исходя из заранее выбранных слов $w, v \in \{v_A, v_B\}$, при фиксированном множестве определяющих соотношений R может оказаться затруднительным и даже невозможным, например, если слово w является меткой границы однослойной кольцевой диаграммы, в которой присутствуют 2-пары и 3-пары областей. (Области образуют 2-пару, если они имеют одно общее внутреннее ребро, по одному ребру на внешнем участке σ границы 1-слойной диаграммы и единственную вершину на внутреннем участке границы τ. Аналогично определяется 3-пара с той лишь разницей, что на участке σ вместо ребер — вершина, а на τ вместо вершины — ребра.) Легко проверить, что такая кольцевая диаграмма не может быть объединена по одному из двух граничных циклов с кольцевой диаграммой типа $(2, 2)$ в приведенную 2-слойную кольцевую диаграмму.

Поэтому порядок действий выбираем обратный: вместо того, чтобы по выбранному слову w строить $(2, 2)$-слой, одна из меток которого совпадает с w или его степенью, начинаем с построения самого периодического $(2, 2)$-слоя, а слово w получаем автоматически как одну из его меток $\varphi(\sigma)$ или $\varphi(\tau)$.

Процедура построения $(2,2)$-слоя может быть реализована при выполнении следующих условий.

Группа G с копредставлением $(X;R)$ называется детерминированной, если каждый символ множества X входит ровно в два определяющих соотношения из R. Если же каждый символ из X входит ровно в k определяющих соотношений из R, то группу G будем называть детерминированной степени k, или k-детерминированной. В случае, если каждый символ из X входит не менее, чем в k соотношений из R, группу G будем называть детерминированной степени не меньше, чем k. Ясно, что при $k=2$ детерминированная группа степени k оказывается просто детерминированной.

Очевидно, что в детерминированной группе существует единственный $(2,2)$-слой, и он является периодическим в следующем смысле: при увеличении длины слоя области в нем начинают повторяться. Интересно, что отказ от свойства $(2,2)$ отменяет и единственность, и периодичность слоя. Теряется и свобода выбора как слова w, так и секретного ключа v, что сводит к нулю попытку построить одностороннюю функцию с использоанием таких групп.

Далее предполагаем, что группа является детерминированной степени не меньше k при $k \geq 3$. Наращиваем слой очередной областью, выбирая случайным образом одно из не менее, чем $(k-1)$ соотношений.

После формирования периода слоя, соответствующего основанию степени w^{n_1}, что гарантировано леммой 1, повторяем этот период n_1 раз и снова случайным образом формируем «хвост» $(2,2)$-слоя, который будет соответствовать слову $v \in \{v_A, v_B\}$. Тем самым построение слова δ закончено. Надо отметить, что число периодических $(2,2)$-слоев с периодом длины s в k-детерминированной группе равно $(k-1)^s$. Значит, при большой длине слов w, v запас слов оказывется достаточно велик, чтобы с ним можно было работать, не опасаясь того, что противник разработает базу исходных ключей и по ней сформирует все возможные открытые ключи. Кроме того, следует учесть, что длина слова v может быть сколь угодно большой.

Использование $(2,2)$-слоев для формирования слова w целесообразно применить и для формирования секретного ключа v. Саму процедуру построения слова v на базе «хвоста» $(2,2)$-слоя, построенного для слова w^n, и ее целесообразность обсудим ниже (см. лемму 2). Перед этим рассмотрим модификациию схемы получения общего секретного ключа. Причина для такой модификации следующая.

Рассмотрим этап 2 процесса получения общего секретного ключа абонентом A. Напомним, что в ходе данного этапа абонент B получает от A открытый ключ $K_1 = w^k v_A$ и передает A открытый ключ $K_1' = w^{k+l} v_A w^{-l}$.

После умножения $w^k v_A$ на w^{-l} справа B требуется продолжить $(2,2)$-слой с граничной меткой $w^k v_A$ до $(2,2)$-слоя с граничной меткой $w^k v_A w^{-l}$, чтобы гарантировать $R, \bar{R}$-несократимость преобразуемого слова. Однако это может быть сопряжено с определенными трудностями, поскольку перед отправкой абоненту B абонент A модифицировал слово $K_1 = w^k v_A$ с помощью преобразований 1)–5). Описанное затруднение можно устранить, если вместо

$K_1 = w^k v_A$ абонент A будет передавать B открытый ключ $K_1 = w^k v_A w$. После внесения соответствующих изменений схема получения общего секретного ключа абонентом A примет следующий вид.

1. Абонент A выбирает произвольное, кроме нуля, целое число k — закрытый ключ 1, произвольное слово v_A в алфавите X — закрытый ключ 2. Далее A вычисляет открытый ключ $K_1 = w^k v_A w$ и отправляет его абоненту B.

2. Абонент B умножает K_1 на w^l слева и на w^{-l-1} справа и передает A полученный открытый ключ $K_1' = w^{k+l} v_A w^{-l}$.

3. Абонент A умножает K_1' на w^{-k} слева и на w^k справа и получает секретный ключ $K_1'' = w^l v_A w^{k-l}$.

Схема получения секретного ключа абонентом B остается неизменной.

Лемма 2. Для любого копредставления $G = (X; R)$ с условиями $C(3)$–$T(6)$ и любой периодической кольцевой диаграммы M типа $(2, 2)$ над этим копредставлением с границей $\partial M = \sigma \cup \tau$ и граничными метками $\varphi(\sigma) \equiv w^n$, $\varphi(\tau) \equiv (u^n)$ существует односвязная 1-слойная диаграмма N над $(X; R)$, содержащая сколь угодно много областей, которую можно вставить в M, разрезав последнюю по любому ребру с вершинами на внутреннем и внешнем граничных циклах. При этом полученная кольцевая 1-слойная диаграмма будет приведенной, ее граничные метки будут циклически $\bar{R}$, R-несократимыми.

Доказательство. Напомним, что диаграмма является приведенной, если в ней нет сократимых пар областей. Таким образом, утверждается, что после вставки диаграммы N в диаграмму M полученная диаграмма $M \cup N$ не будет содержать сократимых пар областей.

Построение кольцевой 1-слойной периодической диаграммы M с граничными циклами σ, τ, граничной меткой $\varphi(\sigma) \equiv w^n$ будем считать законченным, в соответствии с леммой 1.

Для работы модифицированной схемы обмена ключами надо гарантировать возможность удлинения 1-слойной односвязной диаграммы типа $(2, 2)$, которая является результатом разрезания соответствующей кольцевой 1-слойной диаграммы, и построения так называемого «хвоста», соответствующего слову v — секретному ключу. Длина слова v не ограничена, поэтому надо научиться строить «хвост» сколь угодно большой длины.

Кроме того, модифицированная схема обмена ключами предполагает возможность склеивания удлиненной «хвостом» N односвязной диаграммы с граничной меткой $\varphi(\sigma) \equiv w^n v$ в 1-слойную кольцевую диаграмму $M \cup N$ с сохранением свойства $\bar{R}, R$-несократимости граничных меток. Приступим к реализации алгоритма построения «хвоста» N.

Представим разрезанную диаграмму M в виде прямоугольника с границей $\sigma \cup \tau \cup \alpha \cup \beta$, где $\varphi(\sigma) \equiv w^n$, $\varphi(\tau) \equiv u^n$, τ — внутренняя граница кольцевой диаграммы M, а α, β — копии ребра диаграммы M, по которому был сделан разрез.

Пусть ребро α входит в граничный цикл области D_1, ребро β — области D_m, $\alpha \cap \sigma \neq \varnothing$, $\alpha \cap \tau \neq \varnothing$, $\beta \cap \sigma \neq \varnothing$, $\beta \cap \tau \neq \varnothing$, причем из периодичности кольцевой диаграммы M следует,

что область D_1 имеет ребро на σ и только вершину на τ, а область D_m — наоборот, и m кратно n.

Построение диаграммы N выглядит следующим образом. Выбирая случайным образом соотношения из множества R, строим $(2,2)$-слой N.

Первый шаг. Начинаем с соотношения $r_{m+1} \equiv \varphi(\beta)^{-1} r_{m+1}^r$. Здесь $\varphi(\beta) \in X$ — метка ребра β в граничном цикле области D_m (границы областей ориентированы по часовой стрелке), r_{m+1}^r — слово в алфавите X, соотношение r_{m+1} используем как метку области D_{m+1} с вершиной на τ и ребром γ_{m+1} на σ. Третье ребро области D_{m+1} обозначим β_{m+1}.

Второй шаг. Случайным образом выбираем соотношение $r_{m+2} \equiv \varphi(\beta_{m+1})^{-1} r_{m+2}^r$ — граничную метку области D_{m+2} с вершиной на σ и ребром δ_{m+2} на τ. Третье ребро этой области обозначим β_{m+2}.

Третий и последующие шаги повторяют первый и второй попеременно: шаги с нечетными номерами генерируют область с ребром на σ, а с четными — с ребром на τ. Этот процесс построения «хвоста» N можно продолжать сколь угодно долго. Действительно, каждая буква, то есть метка ребра β_{m+s}, является куском, значит, входит в граничные циклы хотя бы двух областей, образующих несократимую пару. Но наша цель — замкнуть кольцевую диаграмму $M \cup N$, сохранив $\bar{R}$, R-несократимость ее граничных меток.

В некоторый случайный момент принимаем решение о прекращении наращивания «хвоста» N. Теперь задача ставится следующим образом: как можно скорее замкнуть кольцо $M \cup N$ с сохранением $\bar{R}$, R-несократимости граничных меток. Для этого начинаем искать в R слово, с помощью которого сформируется область D_{end} с ребром на τ и вершиной на σ, $\partial D_{end} = \beta_{end}\beta_{end+1}\delta_{end}$, где $\varphi(\beta_{end+1}) \equiv \varphi(\alpha)^{-1} \equiv \varphi(\beta)$. Последнее условие гарантирует возможность склейки построенной диаграммы в кольцо.

Если на некотором шаге случайный выбор падает на слово $r_1 \equiv \varphi(\partial D_1)$, и расположение области в диаграмме совпадает с расположением D_1, то есть ребро на σ и вершина на τ, то кольцо замкнулось.

Иначе продолжаем случайное блуждание по множеству слов R, отслеживая области с четными номерами. Если на очередном шаге будет выбрана область D_r с ребром δ_r на τ такая, что $\varphi(\beta_r) \equiv \varphi(\beta_{t-1})$ при нечетном $t < m$, то кольцо можно замкнуть, склеив по ребрам β_r и β_{t-1}. При этом степень слова w может уменьшиться, но, благодаря периодичности диаграммы M, этот недостаток построенного кольца легко компенсировать вставкой недостающего числа областей, соответствующих слову с меткой w. Выполняя такую вставку, мы предполагаем, что ребро β_{t-1} имеет наименьший номер $t-1$ среди всех ребер в M, по которым возможна указанная выше склейка.

Может оказаться, что ребро β_{t-1}, позволяющее сделать склейку кольца, принадлежит области $D_t \subset N$. Этот случай сложнее предыдущего. Покажем, как в этой ситуации строится кольцевая диаграмма с несократимыми метками.

Надо считать, что $\varphi(\beta_{t-2}) \neq \varphi(\beta_{r-1})$, так как иначе склейку можно было бы сделать с помощью ребер β_{t-2}, β_{r-1}. Склеиваем область D_r с копией области D_{t-1} по ребрам β_r, β_{t-1}.

Получаем пару областей, имеющих на σ только вершину, а на продолжении τ — по ребру. Далее склеиваем по ребру β_{t-2} область D_{t-1} (точнее, ее копию)с копией области D_{t-2}. И так далее до тех пор, пока не дойдем до области (копии) D_{l+1}, где диаграмма M состоит из областей $D_1, \ldots, D_l$.

По построению «хвоста» N области D_1, D_{l+1} различные. Значит, можно приклеить копию области D_1 к области D_{l+1} (копии) по ребру β_l, не получив при этом сократимую пару. Значит, кольцо замыкается. Две замыкающие области D_1, D_{l+1} имеют по ребру на σ.

Построенная кольцевая диаграмма имеет циклически $\bar{R}, R$-несократимые граничные метки, что следует из ее структуры: области с ребрами на σ и τ строго чередуются за исключением двух пар областей: (D_1 и копия D_{l+1}) и (D_r и копия D_{t+1}). В первой паре обе области имеют ребра на σ, во второй паре обе области имеют ребра на τ. Легко проверить (доказательство приводится в работах [6, 7, 11, 8]), что на граничные циклы такой кольцевой диаграммы нельза наклеить ни полосу, ни дэновскую область. Теорема доказана.

Таким образом, построение однослойной кольцевой диаграммы с $\bar{R}, R$-несократимой граничной меткой $\varphi(\sigma)$ в процессе обмена общим секретным ключом имеет место в двух случаях: для открытых ключей $w^k v_A$ и $w^l v_B$.

Трудоемкость построение кольцевой диаграммы складывается из трудоемкости построения диаграммы с граничной меткой w и диаграммы с граничной меткой $v \in \{v_A, v_B\}$. В первом случае надо сослаться на алгоритм построения периодической кольцевой однослойной диаграммы типа $(2, 2)$, приведенный в доказательстве леммы 1. Во втором случае используется алгоритм построения «хвоста» из леммы 2. Оценим сложность этих алгоритмов.

Обе процедуры сначала строят диаграмму без учета ее зацикливания, и лишь в некоторый момент, когда принимается решение о том, что построенное слово — метка участка σ построенной диаграммы, имеет достаточно большую длину, начинается поиск области, позволяющей замкнуть построенную однослойную диаграмму в кольцо.

Трудоемкость первого этапа оценить легко: для построения слоя с граничной меткой участка σ длины $|\varphi(\sigma)| < |w|$ понадобится не более $(|w| - 1)n_R$ сравнений символов. То же верно и для первого этапа построения «хвоста» с граничной меткой, не превышающей по длине $|v_A|$: понадобится не более $(|v| - 1)n_R$ сравнений символов. В итоге первые этапы используют не более $(|w| - 1)n_R + (|v| - 1)n_R \leq n \cdot n_R - 2n_R$ сравнений символов, т.е. для этапа 1 имеем

$$T_{(1)} = O(n).$$

С учетом этой оценки вместе с

$$T_{(2)} = (2|w|n_1 + 2n_2|w|)T_5 = 2(n_1 + n_2)|w|(4n_R - 2) = 2n(4n_R - 2)$$

для суммарной трудоемкости T получения открытого ключа получаем оценку

$$T = O(n).$$

6. Получение закрытых ключей противником и оценка сложности

Для синтеза общего секретного ключа $w^l v_A w^{k-l}$ противник E должен использовать не менее двух из четырех доступных ему открытых ключей $w^k v_A$, $w^{k+l} v_A w^{-l}$, $w^l v_B$, $w^{k+l} v_B$. При этом он может использовать как сами ключи, так и их произведения. Тем не менее, в любом случае такое слово будет содержать некоторую степень w, а также некоторое случайное слово. Поэтому без ограничения общности будем полагать, что действия противника состоят в получении k и v_A из $w^k v_A$ или v_B и l из $w^l v_B$.

Рассмотрим получение k и v_A из открытого ключа $w^k v_A$. Далее будем обозначать открытый ключ, с которым работает противник, через ε, а слово, которое синтезирует E в процессе перебора — $w^m v$, $|v| = n$.

Противник осуществляет поиск закрытых ключей посредством перебора: имея сведения об общей структуре открытого ключа, E синтезирует слово вида $w^m v$ и варьирует значения параметров (m, v), пока не получит верное в G равенство $w^m v = \varepsilon$.

Возможность, получения последнего равенства за конечное число шагов вытекает из разрешимости проблемы равенства слов в группах, удовлетворяющих условиям $C(3)$–$T(6)$.

Собственно проверка равенства слов основывается на утверждении о том, что единственным циклически $\bar{R}, R$-несократимым словом, равным единице в группе G, является пустое слово. Для проверки равенства $w^m v \varepsilon^{-1} = 1$ строится кольцеая R-диаграмма с граничной меткой $w^m v \varepsilon^{-1}$ и в ней проводятся $\bar{R}, R$-сокращения. При этом получается либо $\bar{R}, R$-несократимое слово — метка внутренней границы сформированной в процессе $\bar{R}, R$-сокращений кольцевой диаграммы, либо пустое слово, что означает следующее. Построена односвязная диаграмма с граничной меткой $w^m v \varepsilon^{-1}$. Следовательно, $w^m v \varepsilon^{-1} = 1$. Секретные ключи (m, v) найдены.

Оценим трудоемкость описанной процедуры получения закрытых ключей. Для этого, во-первых, требуется дать верхнюю оценку количества пар (m, v), которые будут использованы в процессе перебора, а во-вторых, оценить трудоемкость $\bar{R}, R$-сокращений, проводимых для каждой пары (m, v).

В качестве верхней оценки будем использовать $|w^m v| \leq |\varepsilon|$. Получить нижнюю оценку длины $w^m v$ не удается, поэтому будем считать, что противник рассматривает значения m, начиная с 1, и для каждого фиксированного значения перебирает все слова v, начиная с пустого слова, шаг за шагом увеличивая их длину на единицу до того момента, пока не будет нарушено соотношение $|w^m v| \leq |\varepsilon|$. Понятно, что этим перебор может и не закончиться, но оценка сложности будет дана.

Оценим количество пар (m, v), удовлетворяющих указанному соотношению для фиксированного $|\varepsilon|$. Получаем, что m пробегает целые значения от 1 до $[|\varepsilon|/|w|]$ (при $v = 1$). При каждом фиксированном m в качестве v используются всевозможные слова длины от 0 до $[|\varepsilon| - m|w|]$; при этом количество слов длины k составляет $(2n_X)^k$. В результате общее

количество пар (m, v) при фиксированном m равно

$$n_v(m) = \sum_{i=1}^{k_1(m)} (2n_X)^i = 2n_X \frac{(2n_X)^{k_1(m)} - 1}{2n_X - 1} = k_2((2n_X)^{k_1(m)} - 1),$$

где

$$k_1(m) = [|\varepsilon| - m|w|, \quad k_2 = \frac{n_X}{n_X - 1}.$$

Таким образом, общее количество пар (m, v) составит

$$n_{(m,v)} = \sum_{m=0}^{N} n_v(m), \quad N = \left[\frac{|\varepsilon|}{|w|}\right],$$

откуда

$$n_{(m,v)} = \sum_{m=0}^{N} k_2\Big((2n_X)^{k_1(m)} - 1\Big) = k_2 \sum_{m=0}^{N} \Big((2n_X)^{|\varepsilon| - m|w|} - 1\Big) \geq k_2(2n_X)^{|\varepsilon|}.$$

Значит, $n_{(m,v)} = O(\eta^{|\varepsilon|})$, где $\eta = 2n_x$.

Для каждой фиксированной пары (m, v) противнику требуется провести $\bar{R}, R$-сокращения в диаграмме равенства слов $\varepsilon, w^m v$. Оценим трудоемкость этих сокращений, измеренную в количестве областей диаграмм. Число областей в односвязной диаграмме называют площадью диаграммы. В соответствии с известной теоремой о площади, верной для диаграмм над копредставлениями с условиями $C(p)$–$T(q)$, $(p, q) \in \{(3, 6), (4, 4), (6, 3)\}$, площадь такой диаграммы ограничена квадратичной функцией длины границы диаграммы [2]. Значит, с учетом числа пар (m, v) можно оценить сложность восстановления секретных ключей произведением $O(\eta^n)$ на η^2, что не вносит принципиальной разницы по сравнению с экспоненциальной зависимостью числа пар (m, v) от n, где n — длина входного слова ε. Итак, сложность восстановления секретных ключей растет как показательная функция η^{n+2}.

Заключение

Подводя итог, скажем, что разработанная схема обмена секретными ключами по открытому каналу связи вместе с достоинством, состоящим в значительной сложности несанкционированного восстановления секретных ключей, не лишена и недостатков. Основная проблема — найти способ применения данной схемы на практике: секретные ключи, полученные по открытому каналу, представляют один элемент группы $G = (X; R)$, но являются в общем случае разными словами в алфавите X. Если бы группа была конечной, то можно было бы задать действие полученного общего ключа на элементы группы, получив представление подстановками. А с такой информацией уже можно строить шифры. Для бесконечной группы вопрос остается открытым.

Одним из путей решения этой проблемы является следующий. Вычислять единый представитель сформированного секретного ключа, определив его как слово, кратчайшее в лексикографическом смысле. Такой представитель единственный и предоставляет возможность дальнейшей работы обоим абонентам.

Список литературы

1. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп: пер. с англ.. М.: Наука, 1974. 456 с. [Magnus W., Karrass A., Solitar D. Combinatorial group theory. N.Y.: Interscience Publ., 1966. 444 p.].
2. Линдон Р.К., Шупп П. Комбинаторная теория групп: пер. с англ. М.: Мир, 1980. 447 с. [Lyndon R.C., Schupp P.E. Combinatorial group theory. B.; N.Y.: Springer, 1977. 339 p.].
3. Ольшанский А.Ю. Геометрия определяющих соотношений в группах. М: Наука, 1989. 446 с.
4. Gersten S.M., Short H.B. Small cancellation theory and automatic groups // Inventiones mathematicae. 1990. Vol. 102, no. 1. Pp. 305–334. DOI: 10.1007/BF01233430
5. Безверхний Н.В. Разрешимость проблемы вхождения в циклическую подгруппу в группах с условием $C(6)$ // Фундаментальная и прикладная математика. 1999. Т. 5, №1. С. 39–46.
6. Безверхний Н.В. Нормальные формы для элементов бесконечного порядка в группах с условием $C(3)$–$T(6)$ // Изв. Тульского гос. ун-та. Естественные науки. 2010. Вып. 1. С. 6–25.
7. Безверхний Н.В. Проблема сопряженного вхождения в циклическую подгруппу в группах с условием $C(3)$–$T(6)$ // Дискретная математика. 2012. Т. 24, вып. 4. С. 27–46.
8. Безверхний В.Н. О нормализаторах элементов в $C(p)$–$T(q)$-группах // Алгоритмические проблемы теории групп и полугрупп: Межвуз. сб. науч. тр. Тула: Изд-во Тул. гос. педагогич. ун-та им. Л.Н.Толстого, 1994. С. 4–58.
9. Безверхний Н.В. О кручении и разрешимости проблемы вхождения в циклическую подгруппу в группах с условием $C(6)$ // Деп. ВИНИТИ 1995. № 2033-В95.
10. Bogley W.A., Pride S.J. Aspherical relative presentations // Proc. of the Edinburg Math. Soc. 1992. Vol. 35, no. 1. Pp. 1–39. DOI: 10.1017/S0013091500005290
11. Безверхний Н.В. Односторонние функции и композиция проблем сопряженности и дискретного логарифмирования в $C(3)$–$T(6)$-группах // Математика и математическое моделирование. 2015. № 5. С. 43–63 DOI: 10.7463/mathm.0515.0820675
12. Безверхний Н.В., Чернышёва О.А. Односторонние функции, основанные на проблеме дискретного логарифмирования в группах с условиями $C(3)$–$T(6)$ // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 10. С. 70–101. DOI: 10.7463/1014.0729483
13. Безверхний В.Н., Паршикова Е.В. Решение проблемы вхождения в циклическую подгруппу в группах с условиями $C(4)$–$T(4)$ // Алгоритмические проблемы теории групп и полугрупп: Межвуз. сб. науч. тр. Тула: Изд-во Тул. гос. педагогич. ун-та им. Л.Н. Толстого, 2001. С. 120–139.

14. Глухов М.М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1, № 4. С. 5–22.
15. Паршикова Е.В. Проблема слабой степенной сопряженности в группах с условием $C(4)$–$T(4)$ // Алгоритмические проблемы теории групп и полугрупп: Межвуз. сб. науч. тр. Тула: Изд-во Тул. гос. педагогич. ун-та им. Л.Н. Толстого, 2001. С. 179–184.
16. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. on Computing. 1997. Vol. 26, no. 5. Pp. 1484–1509. DOI: 10.1137/S0097539795293172
17. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Mathematical Research Letters. 1999. Vol. 6, no. 3. Pp. 287–291. DOI: 10.4310/MRL.1999.v6.n3.a3
18. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J.-S., Park C. New public-key cryptosystem using braid groups // Advances in Cryptology — CRYPTO 2000: 20th Annual Intern. Cryptology Conf. (Santa Barbara, CA, USA, August 20–24, 2000): Proc. B.; Hdbl.: Springer, 2000. Pp. 166–183. DOI: 10.1007/3-540-44598-6_10
19. Yamamura A. Public-key cryptosystems using the modular group // Public-key cryptography: PKC 1998: 1st Intern. Workshop on practice and theory in public key cryptography (Pacifico Yokohama, Japan, February 5–6, 1998): Proc. B.; Hdbl.: Springer, 1998. Pp. 203–216. DOI: 10.1007/BFb0054026
20. Yamamura A. A functional cryptosystem using a group action // Information security and privacy: 4th Australasian Conf. on Information Security and Privacy: ACISP 1999 (Wollongong, NSW, Australia, April 7–9, 1999): Proc. B.; Hdbl.: Springer, 1999. Pp. 314–325. DOI: 10.1007/3-540-48970-3_26
21. Paeng S.H., Ha K.C., Kim J.H., Chee S., Park C. New public key cryptosystem using finite non abelian groups // Advances in cryptology – CRYPTO 2001: 21st Annual Intern. Cryptology Conf. (Santa Barbara, CA, USA, August 19–23, 2001): Proc. B.; Hdbl.: Springer, 2001. Pp. 470–485. DOI: 10.1007/3-540-44647-8_28
22. Paeng S.H., Kwon D., Ha K.-Ch., Kim J.H. Improved public key cryptosystem using finite non abelian groups. Cryptology ePrint Archive: Report 2001/066. Режим доступа: http://eprint.iacr.org/ 2001/066, (дата обращения 15.12.2018).
23. Sakalauskas E., Tvarijonas P., Raulinaitis A. Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level // Informatica. 2007. Vol. 18, no. 1. Pp. 115–124.
24. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества словв теории групп // Тр. Матем. ин-та АН СССР. 1955. Т. 44. С. 1–444.

Mathematics & Mathematical Modelling
Electronic journal
http://mathmelpub.ru ISSN 2412-5911

Mathematics and Mathematical Modeling, 2018, no. 6, pp. 88–111.
DOI: **10.24108/mathm.0618.0000151**
Received: 04.11.2018

Asymmetric Secret Key Transfer Scheme over an Open Channel in k-Deterministic Groups with the Conditions $C(3)$–$T(6)$

Bezverkhniy N. V.[1,*], **Nikitina M. V.**[2] [*] nbezv@mail.ru

[1]Bauman Moscow State Technical University, Russia;
[2]Russian Telecommunications Corporation, Moscow, Russia

Keywords: group; presentation; group diagram; equality problem

The article solves a problem of developing a scheme to provide a secret key exchange over an open communication channel. The basic idea of creating such a scheme is well known. It is based on a concept of the one-way function. This refers to the functions whose values are calculated much easier than the inverse function values.

When developing the one-way functions a recognition algorithm of words equality in groups with conditions of small cancellation $C(3)$–$T(6)$ is used. In this case, the group is represented by a set of its generating and determining relations. All the work to accomplish development of algorithms and evaluate their complexity is carried out using the group diagrams of equality. The existence of such diagrams is proved in the well-known van Campen lemma. The paper result is the following.

The proposed scheme for the exchange of secret keys has the following properties. Direct algorithms have a linear complexity, and a complexity of the inverse algorithms is exponential. It should be noted that the algorithms complexity was estimated by the areas of the corresponding group diagrams, which are determined by the number of areas they include. The constructed secret key represents some element of a pre-selected group with conditions $C(3)$–$T(6)$. It can be represented in an infinite number of ways by words in the alphabet from the generators of the group. Thus, the remaining obstacle to the practical application of the key exchange scheme developed is the ambiguity of the secret key record. Finding a common representative as the lexicographically shortest word in the class of equal words turns out to be too difficult. Thus, this question remains open. Although the task of exchanging secret keys itself can be formally considered as solved.

References

1. Magnus W., Karrass A., Solitar D. *Combinatorial group theory*. N.Y.: Interscience Publ., 1966. 444 p. (Russ. ed.: Magnus W., Karras A., Solitar D. *Kombinatornaia teoriia grupp*. Moscow: Nauka Publ., 1974. 455 p.).

2. Lyndon R.C., Schupp P.E. *Combinatorial group theory*. B.; N.Y.: Springer, 1977. 339 p. (Russ. ed.: Lyndon R.C., Schupp P.E. *Kombinatornaia teoriia grupp*. Moscow: Mir publ., 1980. 447 p.).
3. Olshanskij A.Yu. *Geometriia opredeliayushchikh sootnoshenij v gruppakh* [Geometry of defining relations in groups]. Moscow: Nauka Publ., 1989. 446 p. (in Russian).
4. Gersten S.M., Short H.B. Small cancellation theory and automatic groups. *Inventiones mathematicae*, 1990, vol. 102, no. 1, pp. 305–334. DOI: 10.1007/BF01233430
5. Bezverkhnii N.V. On the solvability of the general word problem for a cyclic subgroup of a group with the condition $C(6)$. *Fundamental'naia i prikladnaia matematika* [Fundamental and Applied Mathematics], 1999, vol. 5, no. 1, pp. 39–46 (in Russian).
6. Bezverkhnii N.V. Normal forms for elements of infinite order in groups with conditions $C(3)$–$T(6)$. *Izvestiia Tulskogo gosudarstvennogo universiteta. Estestvennye nauki* [Proc. of the Tula State Univ. Natural science], 2010, no. 1, pp. 6–25 (in Russian).
7. Bezverkhnii N.V. The power conjugacy search problem in a cyclic subgroup in groups with condition $C(3)$–$T(6)$. *Discrete Mathematics and Applications*, 2012, Vol. 22, no. 5-6, pp. 521–544. DOI: 10.1515/dma-2012-036
8. Bezverkhnii V.N. O normalizatorakh elementov v $C(p)$–$T(q)$-gruppakh [On normalizers of elements in $C(p)$–$T(q)$ groups]. *Algoritmicheskie problemy teorii grupp i polugrupp* [Algorithmic problems of group theory and semigroups]. Tula: Tula State Pedagogical Univ. Publ., 1994. Pp. 4–58 (in Russian).
9. Bezverkhnii N.V. O kruchenii i o razreshimosti problemy vkhozhdeniia v tsiklicheskuyu podgruppu v gruppakh s usloviem $C(6)$ [On torsion o and solvability of the problem of entering into cyclic subgroup in groups with condition $C(6)$]. Dep. VINITI 1995. No. 2033-B95 (in Russian).
10. Bogley W.A., Pride S.J. Aspherical relative presentations. *Proc. of the Edinburg Math. Soc.*, 1992, vol. 35, no. 1, pp. 1–39. DOI: 10.1017/S0013091500005290
11. Bezverkhnii N.V. One-way functions and composition of conjugacy and discrete logarithm problems in the small cancellation groups. *Matematika i matematicheskoe modelirovanie* [Mathematics & Mathematical Modelling], 2015, no. 5, pp. 43–63. DOI: 10.7463/mathm.0515.0820675 (in Russian)
12. Bezverkhnii N.V., Chernysheva O.A. One-way functions based on the discrete logarithm problem in the groups meeting conditions $C(3)$–$T(6)$. *Nauka i obrazovanie MGTU im N.E. Baumana* [Science and Education of the Bauman MSTU], 2014, no. 10, pp. 70–101. DOI: 10.7463/1014.0729483 (in Russian)
13. Bezverkhnii V.N., Parshikova E.V. Reshenie problem vkhozhdeniia v tsiklicheskuyu podgruppu v gruppakh s usloviem $C(4)$–$T(4)$ [The solution of the problem of entering the cyclic subgroup in groups with conditions $C(4)$–$T(4)$]. *Algoritmicheskie problemy teorii grupp i polygrupp* [Algorithmic problems of group and semigroup theory]. Tula: Tula State Pedagogical Univ. Publ., 2001. Pp. 120–139 (in Russian).

14. Glukhov M.M. On the analysis of some public key distribution systems based on non-abelian groups. *Matematicheskie voprosy kriptografii* [Mathematical Problems of Cryptography], 2010, vol. 1, no. 4, pp. 5–22 (in Russian).
15. Parshikova E.V. Problema slaboj stepennoj sopriazhennosti v gruppakh s usloviem $C(4)$–$T(4)$ [The problem of weak power conjugacy in groups with condition $C(4)$–$T(4)$]. *Algoritmicheskie problemy teorii grupp i polygrupp* [Algorithmic problems of group theory and semigroups]. Tula: Tula State Pedagogical Univ. Publ., 2001. Pp. 179–184 (in Russian).
16. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Computing*, 1997, vol. 26, no. 5, pp. 1484–1509. DOI: 10.1137/S0097539795293172
17. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 1999, vol. 6, no. 3, pp. 287–291. DOI: 10.4310/MRL.1999.v6.n3.a3
18. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J.-S., Park C. New public-key cryptosystem using braid groups. *Advances in Cryptology — CRYPTO 2000: 20th Annual Intern. Cryptology Conf. (Santa Barbara, CA, USA, August 20–24, 2000): Proc*. B.; Hdbl.: Springer, 2000. Pp. 166–183. DOI: 10.1007/3-540-44598-6_10
19. Yamamura A. Public-key cryptosystems using the modular group. *Public-key cryptography: PKC 1998: 1st Intern. Workshop on practice and theory in public key cryptography (Pacifico Yokohama, Japan, February 5–6, 1998): Proc*. B.; Hdbl.: Springer, 1998. Pp. 203–216. DOI: 10.1007/BFb0054026
20. Yamamura A. A functional cryptosystem using a group action. *Information security and privacy: 4th Australasian Conf. on Information Security and Privacy: ACISP 1999 (Wollongong, NSW, Australia, April 7–9, 1999): Proc*. B.; Hdbl.: Springer, 1999. Pp. 314–325. DOI: 10.1007/3-540-48970-3_26
21. Paeng S.H., Ha K.C., Kim J.H., Chee S., Park C. New public key cryptosystem using finite non abelian groups // *Advances in cryptology – CRYPTO 2001: 21st Annual Intern. Cryptology Conf. (Santa Barbara, CA, USA, August 19–23, 2001): Proc*. B.; Hdbl.: Springer, 2001. Pp. 470–485. DOI: 10.1007/3-540-44647-8_28
22. Paeng S.H., Kwon D., Ha K.-Ch., Kim J.H. Improved public key cryptosystem using finite non abelian groups. Cryptology ePrint Archive: Report 2001/066. Available at: http://eprint.iacr.org/ 2001/066, accessed 15.12.2018.
23. Sakalauskas E., Tvarijonas P., Raulinaitis A. Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, 2007, vol. 18, no. 1, pp. 115–124.
24. Novikov P.S. On the algorithmic unsolvability of the word problem in group theory. *Trudy Matematicheskogo instituta AN SSSR* [Proc. of the Mathematical Institute of the Academy of Sciences of USSR], 1955, vol. 44, pp. 1–144 (in Russian).