Наука и Образование
МГТУ им. Н.Э. Баумана
Сетевое научное издание
ISSN 1994-0448

Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 10. С. 70–101.
DOI: 10.7463/1014.0729483
Представлена в редакцию: 29.06.2014
Исправлена: 06.10.2014

УДК 519.40

Односторонние функции, основанные на проблеме дискретного логарифмирования в группах с условиями $C(3)$-$T(6)$

Безверхний Н. В.[1,*], **Чернышева О. А.**[1]

[*]nbezv@mail.ru

[1]МГТУ им. Н.Э. Баумана, Москва, Россия

В данной работе рассматривается возможность создания схемы открытого распределения ключей в группах, копредставление которых удовлетворяет условиям $C(3)$-$T(6)$. При этом используются следующие алгоритмы: алгоритм, решающий проблему вхождения в циклическую подгруппу, известную также как проблема дискретного логарифмирования, и алгоритм, решающий проблему равенства слов в данном классе групп. Исследование проводится с использованием геометрических методов комбинаторной теории групп (метода диаграмм над группами). Нашей задачей было построить одностороннюю функцию на группе с условиями малого сокращения $C(3)$-$T(6)$ и сравнить сложность её вычисления со сложностью вычисления обратной функции. Исследования показывают, что процедура вычисления обратной функции имеет полиномиальную сложность.

Ключевые слова: односторонняя функция, условия малого сокращения, диаграмма над группой, проблема вхождения в циклическую подгруппу.

Введение

В данной работе исследуется возможность построения односторонней функции, основанной на разрешимости алгебраической проблемы вхождения в циклическую подгруппу, известной также как проблема дискретного логарифмирования, и проблеме равенства слов в группах, удовлетворяющих условиям малого сокращения $C(3)$-$T(6)$. Наличие такой функции позволяет говорить о соответствующей схеме открытого распределения ключей. Результаты данного исследования указывают на невозможность построения криптостойкой системы с использованием указанных алгоритмов в данном классе групп.

Исследования проводятся с использованием геометрических методов комбинаторной теории групп, а именно, метода диаграмм над группами, базирующегося на следующих двух утверждениях [1, 2, 3]. Первое — лемма Ван Кампена, утверждающая, что слово равно единице в группе тогда и только тогда, когда существует односвязная диаграмма с граничной меткой, равной этому слову. Второе — лемма о сопряженных элементах группы, утвержда-

ющая, что слова u и v представляют сопряженные элементы данной группы тогда и только тогда, когда существует кольцевая диаграмма с граничными метками, равными u и v^{-1}.

При обмене информацией по открытому каналу используют односторонние функции, прямое вычисление которых должно быть гораздо менее сложным, чем вычисление обратной функции. Нашей задачей было построить одностороннюю функцию на группе с условиями малого сокращения $C(3)$-$T(6)$ и сравнить сложность ее вычисления со сложностью вычисления обратной функции.

Как уже говорилось, в данной статье построение односторонней функции базируется на проблеме дискретного логарифмирования в группах с условиями $C(3)$-$T(6)$. Надо отметить, что после доказательства в 1997 г. в работе [15] полиномиальной сложности задачи дискретного логарифмирования в мультипликативных группах конечных полей и колец вычетов при ее решении на квантовом компьютере появилась серия исследований по отысканию других сложных математических проблем, которые можно было бы использовать для построения асимметричных криптосистем. При этом мы не встречаем работ, использующих группы с условиями малого сокращения $C(p)$-$T(q)$.

Так в 1998–2001 гг. в работах [16, 17, 18, 19] были рассмотрены системы открытого распределения ключей, основанные на проблеме сопряженности в некоммутативных группах: матричных группах и группах кос.

В 2001 г. вышли работы [20, 21], в которых за основу была взята проблема дискретного логарифмирования в группах внутренних автоморфизмов полупрямых произведений групп $SL(2,\mathbb{Z}_p)$ и $\mathbb{Z}_p$, $GL(2,\mathbb{Z}_p)$ и $\mathbb{Z}_p$.

В 2007 г. в работе [22] была предложена схема, основанная на композиции двух проблем теории групп: проблемы сопряженности и проблемы дискретного логарифмирования.

Более подробную информацию и анализ криптосистем, предложенных в перечисленных работах, можно найти в статье [10].

В дальнейшем мы будем использовать следующие основные обозначения.

$w_1 \equiv w_2$ — слово w_1 графически равно слову w_2;

$w_1 = w_2$ — слово w_1 равно слову w_2;

$|w|$ — длина слова w;

∂D — граница области D;

∂M — граница карты M;

$d(v)$ — степень вершины v;

$d(D)$ — степень области D;

$i(D)$ — число внутренних ребер области D;

$\sum_M d(v)$ — сумма степеней всех вершин карты M;

$\sum_M d(D)$ — сумма степеней всех областей карты M;

$\sum_M^{\bullet}$ — суммирование по граничным вершинам или областям карты M;

$\sum_M^{\circ}$ — суммирование по внутренним вершинам или областям карты M.

1. Основные понятия комбинаторной теории групп

Образующие элементы и определяющие соотношения. Если дано отображение α символов a, b, c, ... в группу G, причем $\alpha(a) = g$, $\alpha(b) = h$, $\alpha(c) = k$, ..., то мы говорим, что (относительно α) a определяет g, b определяет h, c определяет k, ..., a^{-1} определяет g^{-1}, b^{-1} определяет h^{-1}, c^{-1} определяет k^{-1}, ...

Далее, слово $W \equiv f_1 \dots f_n$ в символах a, b, c, ... определяет элемент $g_1 g_2 \dots g_n$, где f_i определяет g_i. Этот элемент обозначают $W(g, h, k, \dots)$. Пустое слово определяет нейтральный элемент 1 из G. Если слова U и V определяют элементы p и q группы G, то U^{-1} определяет p^{-1} и V^{-1} определяет q^{-1}.

Если каждый элемент группы G определяется некоторым словом в символах a, b, ..., то символы a, b, ... называются *порождающими* или *образующими символами* (относительно отображения α) группы G, а элементы g, h, k, ... — *порождающими* или *образующими элементами* группы G.

Если слово $R(a, b, c, \dots)$ определяет нейтральный элемент 1 группы G, то говорят, что $R(a, b, c, \dots)$ равно единице в G. Равенство

$$R(a, b, c, \dots) = S(a, b, c, \dots)$$

называется *соотношением*, если слово RS^{-1} равно единице в G.

Пустое слово и слова aa^{-1}, $a^{-1}a$, bb^{-1}, $b^{-1}b$, cc^{-1}, $c^{-1}c$, ... равны единице в любой группе; их называют тривиально равными единице или тривиальными словами.

Пусть слова P, Q, R, ... равны единице в группе G. Будем говорить, что слово W выводимо из слов P, Q, R, ..., если W можно преобразовать в пустое слово за конечное число шагов, каждый из которых состоит в выполнении одной из следующих операций:

1) вставка одного из слов P, P^{-1}, Q, Q^{-1}, R, R^{-1}, ... или одного из слов, тривиально равных единице, либо между любыми двумя соседними символами из W, либо перед W, либо после W;

2) вычеркивание из слова W части (отрезка) слова W, совпадающей с одним из слов P, P^{-1}, Q, Q^{-1}, R, R^{-1}, ... или словом, тривиально равным единице.

Всякое слово W, выводимое из единичных слов P, Q, R, ..., само является единичным, т.е. представляет единичный элемент группы.

Если каждое единичное слово выводимо из единичных слов P, Q, R, ..., то множество P, Q, R, ... называется *множеством определяющих слов* группы G относительно порождающих a, b, c, ... Если P, Q, R, ... — множество определяющих слов группы G относительно порождающих a, b, c, ..., то выражение вида $G = (X; R)$ называется *копредставлением* группы G.

Копредставление называется *конечно порожденным*, если число образующих в нем конечно. Если конечно порожденное копредставление содержит конечное число определяющих слов, то мы называем его *конечно определенным*.

Каждая группа G обладает копредставлением, которое можно получить, вводя свой порождающий символ для каждого элемента группы G и выбирая в качестве множества определяющих слов все слова в этих образующих, равные единице в G.

Построение группы по образующим и определяющим словам. Слова W_1 и W_2 в символах $a, b, c, \ldots$ называются *эквивалентными* ($W_1 \sim W_2$), если W_1 можно преобразовать в W_2 за конечное число шагов, каждый из которых состоит в выполнении одной из следующих операций:

1) вставка одного из слов P, P^{-1}, Q, Q^{-1}, R, R^{-1}, $\ldots$ или одного из слов, тривиально равных единице, либо между любыми двумя соседними символами из W, либо перед W, либо после W.

2) вычеркивание из слова W части (отрезка) слова W, совпадающей с одним из слов P, P^{-1}, Q, Q^{-1}, R, R^{-1}, $\ldots$. или словом, тривиально равным единице.

Класс эквивалентности всех слов в символах a, b, c, $\ldots$, эквивалентных слову W, будем обозначать через $\{W\}$, а слово W или любое другое слово, содержащееся в $\{W\}$, будем называть *представителем* класса $\{W\}$.

Умножение классов эквивалентности определяется посредством равенства $\{W_1\}\cdot\{W_2\} = \{W_1W_2\}$.

Множество G классов эквивалентности, определяемых отношением $\sim$ на множестве всех слов в символах $a, b, c, \ldots$, является группой относительно умножения, определенного выше. Более того, относительно отображения, которое a переводит $\{a\}$, b — в $\{b\}$ и т.д. группа G имеет представление $\langle a,\ b,\ c,\ \ldots;\ P(a,b,c,\ldots),\ Q(a,b,c,\ldots),\ R(a,b,c,\ldots),\ \ldots\rangle$.

Таким образом, каждому элементу группы соответствует единственный класс эквивалентных слов. Поэтому возникает проблема: представляют ли два данных слова один и тот же элемент группы, или эквивалентны ли два данных слова. Эта проблема называется *проблемой равенства* или *проблемой слов*.

Если группы G' и G имеют одно и то же представление, то они изоморфны.

Всякое формальное выражение, имеющее вид представления, на самом деле является представлением некоторой группы.

Таким образом, каждая группа имеет представление, а каждое представление определяет единственную группу.

Следует отметить, что различные представления могут определять одну группу, но не существует алгоритма, определяющего, так ли это для двух заданных представлений. Этому вопросу посвящена *проблема изоморфизма групп*.

Фундаментальные проблемы Дэна. Выше были сформулированы две алгоритмические проблемы: равенства и изоморфизма. Они относятся к числу фундаментальных проблем Дэна. Пусть группа G определена посредством заданного представления. К фундаментальным проблемам Дэна относят следующие алгоритмические проблемы:

1) *проблема слов* — для произвольного слова W в алфавите образующих группы G выяснить за конечное число шагов, определяет ли W единичный элемент в G;

2) *проблема сопряженности* — для двух произвольных слов W_1 и W_2 в алфавите образующих G распознать за конечное число шагов, определяют ли W_1 и W_2 сопряженные элементы группы G;

3) *проблема изоморфизма* — для произвольной группы G', определенной посредством другого представления, выяснить за конечное число шагов, изоморфна ли G' группе G.

Проблема слов была решена для многих классов представлений того или иного специального вида, например, для представлений, в которых есть не более одного определяющего слова (группы с одним соотношением); для представлений, которые конечно порождены и в которых для каждой пары порождающих символов a и b среди определяющих соотношений содержится соотношение $ab = ba$ (абелевы группы); для представлений, в которых каждая пара определяющих слов имеет весьма малое по сравнению с их длинами общее подслово (группы с малыми сокращениями).

Тем не менее существуют конечные представления, для которых проблему слов решить нельзя, т.е. не существует алгоритма, распознающего за конечное число шагов по произвольному слову W этого представления, определяет ли W единичный элемент. Таким образом, нет процедуры для решения проблемы слов, которая работала бы для каждого представления, или в классе всех групп [4].

Проблема сопряженности еще более трудна, чем проблема слов. В самом деле, сопряженность слова W_2 пустому слову W_1 есть не что иное, как равенство слова W_2 пустому слову W_1, поэтому решение проблемы сопряженности дает, в частности, решение проблемы слов. Таким образом, в классах групп с разрешимой проблемой сопряженности разрешима и проблема слов.

Проблема изоморфизма является наиболее трудной из трех проблем Дэна. Обычно ограничиваются рассмотрением представлений для G и G' из некоторого специального класса. В частности, проблема изоморфизма может быть разрешима в следующих случаях: если представления для G и G' не содержат определяющих слов; если представление для G и G' конечно определены и каждое содержит соотношение вида $ab = ba$ для любой пары своих порождающих символов; если одно из представлений не содержит определяющих слов, а другое имеет единственное определяющее слово.

Граф группы. *Графом* или *одномерным комплексом* называют множество из элементов двух типов, называемых вершинами и ребрами, которые удовлетворяют следующим постулатам:

1) каждому ребру E однозначно сопоставлена упорядоченная пара вершин P, P' (не обязательно различных), называемых граничными вершинами E, при этом вершина P называется начальной вершиной ребра E, а P' — конечной;

2) каждому ребру E сопоставлено единственное ребро E^{-1} отличное от E (называемое обратным для E), такое, что $(E^{-1})^{-1} = E$;

3) если E начинается в P и заканчивается в P', то E^{-1} начинается в P' и заканчивается в P.

Следует отметить, что в графе вершины P и P' могут оказаться соответственно началом (концом) нескольких различных ребер.

В случае, когда граф состоит из одной вершины, являющейся началом и концом всех ребер, граф называется сингулярным.

Два графа Γ и Γ^* называются изоморфными, если существует взаимно однозначное отображение T вершин и ребер графа Γ на вершины и ребра графа Γ^* соответственно, при котором сохраняются отношения «быть начальной вершиной», «быть конечной вершиной», «быть обратным для».

Любые два сингулярных графа с одинаковым числом ребер изоморфны. Через S_n обозначается сингулярный граф с $2n$ ребрами: s_1, s_1^{-1}, s_2, s_2^{-1}, $\ldots$, s_n, s_n^{-1}.

Определим теперь граф Γ группы G, заданной на некотором фиксированном множестве образующих a_ν. В качестве вершин графа Γ возьмем элементы группы G.

Ребро графа Γ определяется его начальной и конечной вершинами, цветом (т.е. соответствующим ему образующим) и ориентацией (т.е. указанием, в какую сторону относительно его начальной вершины направлена стрелка). Таким образом, ребро полностью определяется тройкой $(g_1, g_2; a_\nu^\varepsilon)$, где g_1 и g_2 ($g_2 = g_1 \cdot a_\nu^\varepsilon$) — начало и конец ребра соответственно, a_ν — соответствующий ему образующий, а $\varepsilon = \pm 1$ характеризует его ориентацию.

Рассмотрим несколько необходимых условий, при которых граф Γ будет изоморфен графу группы. Граф группы является связным. Действительно, всякий элемент $g \in G$ определяется произведением $g = a_{\nu_1}^{\varepsilon_1} a_{\nu_2}^{\varepsilon_2} \cdots a_{\nu_r}^{\varepsilon_r}$. Если $g_j = a_{\nu_1}^{\varepsilon_1} a_{\nu_2}^{\varepsilon_2} \cdots a_{\nu_j}^{\varepsilon_j}$ и $E_j = (g_{j-1}, g_j; a_{\nu_j}^{\varepsilon_j})$, то путь $E_1 E_2 \ldots E_r$ связывает 1 с g. Поэтому граф Γ, изоморфный графу группы, должен быть связным.

Граф группы имеет раскрашенные и ориентированные ребра; следовательно, граф Γ должен допускать возможность раскраски и ориентации ребер. Чтобы сделать это свойство точным, используем сингулярные графы.

Сингулярный граф S_n с $2n$ ребрами s_1, s_1^{-1}, s_2, s_2^{-1}, $\ldots$, s_n, s_n^{-1} является простейшим примером графа, ребра которого могут быть раскрашены в n цветов и ориентированы. Именно, s_ν интерпретируется как положительно ориентированное ребро некоторого цвета, а s_ν^{-1} — как отрицательно ориентированное ребро того же цвета. Вообще граф может быть «раскрашен n цветами и ориентирован», если ассоциировать с каждым из его ребер некоторое ребро s_n. Это приводит к следующему определению.

Раскраска в n цветов и ориентация графа Γ есть отображение M его ребер в ребра S_n при следующих условиях:

1) для каждой вершины $P \in \Gamma$ ребра Γ, инцидентные P, взаимно-однозначно отображаются на все ребра из S_n;

2) $M(E^{-1}) = (M(E))^{-1}$ для каждого ребра $E \in \Gamma$.

Первое из этих условие говорит о том, что любой вершине P из Γ инцидентно одно ребро каждого цвета и направления, а второе условие — что цвет E^{-1} тот же, что у E, а его ориентация противоположна.

Очевидно, что граф группы, порожденной n образующими $a_1, a_2, \ldots, a_n$ имеет раскраску и ориентацию, а именно, отображение ребер $(g_\mu, g_\lambda; a_\nu^\varepsilon)$ в s_ν^ε. Однако не каждый граф, допускающий раскраску и ориентацию, является графом группы.

Если M — раскраска и ориентация графа Γ и $\pi = E_1 \ldots E_r$ есть путь в Γ, то полагаем $M(\pi) = M(E_1) \ldots M(E_r)$ и будем говорить, что путь π покрывает путь $M(\pi)$.

Раскраска и ориентация M графа Γ называется правильной, если для любых двух путей π и π' из Γ, таких, что $M(\pi) = M(\pi')$, путь π замкнут тогда и только тогда, когда замкнут путь π'.

Пусть Γ — связный граф с правильной раскраской в n цветов и ориентацией M. Тогда Γ изоморфен графу некоторой группы G с n образующими $a_1, \ldots, a_n$. Слова $W(a_\nu)$ в алфавите $a_1, \ldots, a_n$ взаимно однозначно соответствуют путям в Γ с началом в некоторой фиксированной вершине P_0 при отображении $W(a_\nu) \mapsto \pi$, где π покрывает $W(s_\nu)$. Единичными словами G являются те слова $R(a_\nu)$, которые соответствуют замкнутым путям в Γ.

Задача о построении графа группы G по представлению $G = \langle a, b, c, \ldots; P, Q, R, \ldots \rangle$, очевидно, эквивалентна проблеме слов для этого представления.

Диаграммы над группами. Допустим, что группа G имеет представление $G = \langle X; R \rangle$. Пусть $F = \langle X; \rangle$ — свободная группа с базисом X (она не имеет других соотношений, кроме тривиальных), и N — нормальное замыкание множества R в F (т.е. подгруппа группы F, порожденная элементами frf^{-1}, где $f \in F$, $r \in R$). Тогда $G = F/N$.

Элемент w из F представляет единицу в фактор-группе G тогда и только тогда, когда $w \in N$. Далее, $w \in N$ тогда и только тогда, когда в свободной группе F он является произведением элементов, сопряженных с элементами множества $R^{\pm 1}$: $w = c_1 \cdots c_n$, где $c_i = u_i r_i u_i^{-1}$, r_i или r_i^{-1} лежат в R. С каждым таким произведением мы свяжем некоторую диаграмму на евклидовой плоскости, содержащую всю существенную информацию о произведении $c_1 \cdots c_n$.

Пусть E^2 — евклидова плоскость. Если $S \subseteq E^2$, то через ∂S обозначена граница множества S, через $\bar{S}$ — его топологическое замыкание, а через $-S$ — множество $E^2 - S$. Вершина — это некоторая точка в E^2. Ребро — ограниченное подмножество в 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 своих вершин, ребер и областей. Граница для M будет обозначаться символом ∂M. 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.

Ребро можно направить в любую сторону. Если e — ориентированное ребро, идущее от концевой точки v_1 к концевой точке v_2, то v_1 — начальная вершина этого ребра, а v_2 — конечная вершина. Противоположным образом ориентированное ребро, обратное к ребру e, обозначается через e^{-1} и идет 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 точки ребер e_i и e_j различны.

Если D — область из M с данной ориентацией, то любой цикл минимальной длины, включающий в себя все ребра из ∂D, в котором все ребра ориентированы в соответствии с ориентацией области D, называется граничным циклом этой области. Если M связна и односвязна, то граничный цикл для M — это цикл α минимальной длины, содержащий все ребра из границы для 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 без ребер карты M, начинающихся вершиной v.

Диаграммой над группой F называется ориентированная карта M вместе с функцией φ, сопоставляющей каждому ориентированному ребру e карты M метку $\varphi(e)$ из F таким образом, что если e — ориентированное ребро из M, а e^{-1} — противоположным образом ориентированное ребро, то $\varphi(e^{-1}) = \varphi(e)^{-1}$.

Если α — путь в M, $\alpha = e_1 \ldots e_k$, то положим $\varphi(\alpha) = \varphi(e_1) \ldots \varphi(e_k)$. Если D — область из M, то ее меткой называется элемент $\varphi(\alpha)$, где α — граничный цикл области D.

Пусть F — свободная группа с данным базисом. С каждой конечной последовательностью $(c_1, \ldots, c_n)$ нетривиальных элементов свободной группы F можно связать диаграмму $M(c_1, \ldots, c_n)$, являющуюся ориентированной картой с функцией метки φ со значениями в F, удовлетворяющей следующим условиям:

1) если e — ребро из M, то $\varphi(e) \neq 1$;

2) M связна и односвязна с выделенной вершиной O на ∂M, при этом существует граничный цикл $e_1 \ldots e_t$ карты M, начинающийся в O и такой, что $\varphi(e_1) \ldots \varphi(e_t) = c_1 \ldots c_n$;

3) если D — произвольная область из M и $e_1 \dots e_j$ — произвольный граничный цикл этой области, то $\varphi(e_1) \dots \varphi(e_j)$ — циклически приведенная перестановка некоторого c_i.

Теорема 1 ([2]). Если F — свободная группа, то для произвольной последовательности $c_1, \dots, c_n$, $n \geq 0$, нетривиальных элементов из F существует диаграмма $M(c_1, \dots, c_n)$, удовлетворяющая условиям 1–3.

Теорема 2 ([2]). Пусть M — связная односвязная диаграмма с областями $D_1, \dots, D_m$. Допустим, что α — граничный цикл для M, начинающийся в вершине $v_0 \in \partial M$, и пусть $w = \varphi(\alpha)$. Тогда существуют метки r_i областей D_i и элементы u_i из F, $1 \leq i \leq m$, такие, что

$$w = (u_1 r_1 u_1^{-1}) \cdots (u_m r_m u_m^{-1}).$$

Подмножество R свободной группы F называется симметризованным, если все элементы из R приведены и из $r \in R$ следует, что все циклические перестановки элементов $r^{\pm 1}$ также лежат в R.

Пусть R — симметризованное подмножество элементов группы F. Диаграмма M называется R-диаграммой, если для любого граничного цикла δ любой области D из M имеем $\varphi(\delta) \in R$.

Пусть R — симметризованное подмножество свободной группы F и N — нормальное замыкание в F множества R. Если w — произвольный элемент из F, то $w \in N$ тогда и только тогда, когда существует связная односвязная R-диаграмма M, такая, что метка на границе карты M равна w.

2. Группы с условиями малого сокращения

Диаграммы над группами с условиями $C(p)$-$T(q)$. Предположим, что r_1 и r_2 — различные элементы из R, такие, что $r_1 = bc_1$ и $r_2 = bc_2$. В этом случае элемент b называется куском относительно множества R.

Предположения о малом сокращении состоят в том, что куски — относительно малые части элементов из R. Обычное условие имеет метрический вид $C'(\lambda)$, где λ — положительное действительное число. Условие $C'(\lambda)$ означает, что 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. Оно означает, что никакой элемент из R не является произведением менее чем p кусков.

Условие $T(q)$ означает следующее. Пусть $3 \leq h < q$. Предположим, что $r_1, \dots, r_h$ — элементы из R, такие, что последовательные элементы r_i, r_{i+1} не являются взаимно обратными. Тогда по крайней мере одно из произведений $r_1 r_2, \dots, r_{h-1} r_h, r_h r_1$ является приведенным.

Пусть R — симметризованное подмножество свободной группы F. Последовательность $c_1, \dots, c_n$ элементов, сопряженных с элементами множества R, называется минимальной

R-последовательностью, если произведение $w = c_1 \cdots c_n$ не может быть записано как произведение менее чем n сопряженных с элементами из R.

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 $\varphi(\delta_2) = f_2$. Диаграмма M называется приведенной, если всегда $f_2 \neq f_1^{-1}$.

Теорема 3. [2] Диаграмма M минимальной R-последовательности приведена.

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

Пусть v — вершина карты M. Степень $d(v)$ вершины v — это число ориентированных ребер с начальной вершиной v. Если оба конца некоторого ребра e совпадают с v, мы считаем e дважды. Если D — область из M, то степень $d(D)$ области D есть число ребер в граничном цикле для D. Символ $i(D)$ обозначает число внутренних ребер из D, причем снова ребро, встречающееся в граничном цикле для D дважды, считается два раза.

Следующая лемма дает геометрическую интерпретацию условий $C(p)$ и $T(q)$.

Теорема 4 ([2]). Пусть R — симметризованное множество элементов свободной группы F и M — приведенная R-диаграмма. Тогда верны следующие утверждения:

1) если R удовлетворяет условию $C(k)$, то каждая область D из M, такая, что $\partial D \cup \partial M$ не содержит ребер, имеет степень $d(D) \geq k$;

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

Пусть p и q — такие натуральные числа, что $1/p + 1/q = 1/2$. Хорошо известно, что единственными парами такого вида являются $(3, 6)$, $(4, 4)$ и $(6, 3)$. Если M — непустая карта, все внутренние вершины которой имеют степень не менее p, а все области имеют степень не менее q, то она будет называться $[p, q]$-картой. Если M — непустая карта, все внутренние вершины которой имеют степень не менее p, а все внутренние области имеют степень не менее p, то она будет называться (p, q)-картой.

Знаки суммирования $\sum$ будут означать суммирование по вершинам или областям карты M. Так, $\sum d(v)$ есть сумма степеней всех вершин карты M, а $\sum d(D)$ — сумма степеней всех областей карты M. Обозначение $\sum^\bullet$ будет употребляться для суммирования по граничным вершинам или областям, а $\sum^\circ$ — суммирование по внутренним областям или вершинам. Таким образом, $\sum^\bullet d(v)$ — сумма степеней всех граничных вершин карты M, а $\sum^\circ d(D)$ — сумма степеней всех внутренних областей. В случае необходимости будет добавляться индекс, именующий карту, о которой идет речь.

Пусть M — произвольная карта. Тогда V будет означать число вершин карты M. Число неориентированных ребер карты M будет обозначаться буквой E, а число областей этой карты — буквой F. Символ $V^\bullet$ обозначает число граничных вершин карты M, $F^\bullet$ — число граничных областей и $E^\bullet$ — число граничных ребер с учетом кратности. Если M связна и односвязна, то $E^\bullet$ — число ребер в граничном цикле для M. Чтобы получить $E^\bullet$ в общем случае, нужно сложить числа ребер в циклах, необходимых для описания границы карты M.

При исследовании диаграмм над группами с условиями $C(p)$-$T(q)$ полезной оказывается следующая формула кривизны. Полагаем, что натуральные числа p и q связаны равенством $1/p + 1/q = 1/2$.

Теорема 5 ([2]). Если M — односвязная $[p, q]$-карта, содержащая не менее двух вершин, то

$$\sum\nolimits_M^\bullet \left[\frac{p}{q} + 2 - d(v)\right] \geq p.$$

Если M – односвязная (q, p)-карта, содержащая более чем одну область, то

$$\sum\nolimits_M^\bullet \left[\frac{p}{q} + 2 - i(D)\right] \geq p.$$

Теорема 6 ([2]). Если M — $[p, q]$-карта, каждая компонента которой является либо односвязной, либо кольцевой, то

$$E_M^\bullet \leq \frac{q}{p} \sum\nolimits_M^\bullet [p - d(v)] \tag{1}$$

и

$$V_M^\bullet \leq \frac{q}{p} \sum\nolimits_M^\bullet [p - d(v)] \tag{2}$$

Обозначим через M_1 подкарту карты M, получающуюся вычеркиванием всех изолированных вершин. Пусть M — произвольная карта. Граничный слой карты M состоит из всех граничных вершин, ребер, содержащих граничные вершины, и граничных областей карты M.

Для $[p, q]$-карты M введем обозначение

$$\sigma(M) = \sum\nolimits_M^\bullet [p - d(v)].$$

Теорема 7 (о площади [2]). Если M_1 — односвязная $[p, q]$-карта, то

$$V_M \leq \frac{q}{p^2} \sigma(M)^2.$$

Если M —- односвязная (q, p)-карта, то

$$F_M \leq \frac{q}{p^2} \left(\sum\nolimits_M^\bullet [p - i(D)]\right)^2.$$

Теорема 8 ([2]). Пусть F — конечно порожденная свободная группа, R — конечное симметризованное множество элементов группы F и N — нормальное замыкание множества R. Если R удовлетворяет либо условию $C(6)$, либо условиям $C(4)$ и $T(4)$, либо условиям $C(3)$ и $T(6)$, то проблема равенства слов в группе F/N алгоритмически разрешима.

Говорят, что в группе $G = \langle X;\ R\rangle$ разрешима проблема вхождения в циклическую подгруппу, если для любых слов w и v в алфавите X можно выяснить, существует ли такое число $n \in \mathbb{Z}$, что слова w^n и v представляют один и тот же элемент группы G.

Теорема 9 ([2]). Пусть F — конечно порожденная свободная группа, R — конечное симметризованное множество элементов группы F и N — нормальное замыкание множества R. Если R удовлетворяет либо условию $C(6)$, либо условиям $C(4)$ и $T(4)$, либо условиям $C(3)$ и $T(6)$, то проблема вхождения в циклическую подгруппу в группе $G = F/N$ алгоритмически разрешима. При этом целое число n, для которого выполняется равенство слов w^n и v в группе G, может быть вычислено.

Тем самым, в указанных классах групп разрешима проблема дискретного логарифмирования.

В этой статье рассматривается один из трех упомянутых классов групп с условиями $C(p)$-$T(q)$, а именно, класс $C(3)$-$T(6)$, поскольку работа с ним оказывается проще, чем в двух других. Это объясняется тем, что любой кусок в таком классе имеет единичную длину, что и доказано ниже.

Сокращения в ($C(3)$-$T(6)$)-группах. В группах с условиями $C(p)$-$T(q)$ длина произвольного куска может быть отлична от единицы. Но если $q > 4$, то все куски имеют единичную длину [14].

Действительно, предположим, что $r_1 \equiv abr_1'$, $r_2 \equiv abr_2'$ — различные определяющие соотношения, где a, b, r_1, r_2 — непустые слова в алфавите X, и рассмотрим слова из R, обратные к r_1, r_2, а также их циклические перестановки: $u_1 \equiv br_1'a$, $u_2 \equiv a^{-1}(r_2')^{-1}b^{-1}$, $u_3 \equiv br_1'a$, $u_4 \equiv a^{-1}(r_2')^{-1}b^{-1}$. Последовательность u_1, u_2, u_3, u_4, u_1 противоречит условию $T(6)$. Значит, общее начало ab двух определяющих соотношений из R имеет единичную длину.

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

1) $r \equiv r_1r_2$,

2) $w \equiv w_1w_2w_3$,

3) $r_1 \equiv w_2$,

4) слово r_2 либо пусто, либо является куском,

5) слова $w_1r_2^{-1}$, $r_2^{-1}w_3$ несократимы в свободной группе.

В случае замены слова w равным ему в группе G словом $w_1r_2^{-1}w_3$ будем говорить, что в w выполнено R-сокращение. R-сокращение в слове w, являющемся степенью некоторого

слова v: $w = v^s$, называется длинным, если $|w_2| \geq |v|$. Если же $|w_2| < |v|$, то R-сокращение называется коротким.

Если не требуется перечисления всех образующих и определяющих слов, будем писать $X = \{x_1, \dots x_n\}$ и $R = \{r_1, \dots, r_m\}$, подразумевая при этом, что в X содержатся также $x_1^{-1}, \dots, x_n^{-1}$, а в R — все циклические перестановки и инверсии $r_1, \dots, r_m$.

Пусть у нас имеется группа $G = \langle X;\ R\rangle$, 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 $v = acb$, то есть $w = acbacb$. Используя определяющее соотношение $r_2 = acb$, заменяем первое вхождение acb в w пустым словом. В данном случае мы выполнили в слове w длинное R-сокращение, так как $|acb| = |v|$. Если в любой циклической перестановке слова w нет R-сокращений, то слово w называется циклически R-несократимым.

Определим понятие $\bar{R}$-сокращения с использованием диаграмм. Также дадим геометрическое определение R-сокращения. Для этого рассмотрим следующие понятия.

Рассмотрим диаграмму M. Область $D \subset M$ называется дэновской [8], если:

1) $\partial D \cap \partial M$ — последовательная часть границы ∂M (т.е. $\partial D \cap \partial M = p$ — подпуть в граничных циклах области D и диаграммы M);

2) $i(D) \in \{0,\ 1\}$.

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

1) $\partial D_i \cap \partial M = p$ — последовательная часть границы ∂M;

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

3) 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;

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

5) $\partial D_i \cap \partial D_{i+1}$, $i = 1,\ \dots,\ k - 1$, — ребро.

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 копредставлением $G = reprXR$, 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 $G = \langle X;\ R\rangle$, в которой существует полоса Π, граничное слово которой является подсловом в v.

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

Действительно, из определений R-и $\bar{R}$-сокращений следует, что в результате такого сокращения длина слова строго уменьшается. Поэтому, записав произвольное слово w на окружности C и выполняя в его циклических перестановках R- и $\bar{R}$-сокращения, получим либо пустое слово, что невозможно, поскольку $w \neq 1$ в G, либо непустое слово w_0, в циклических перестановках которого нет R- и $\bar{R}$-сокращений.

3. Основные понятия криптографии

Можно выделить два разных подхода к защите конфиденциальной информации: ограничение доступа и шифрование. При использовании первого подхода информация не изменяется, а затрудняется доступ к ней, например, требуется знание паролей. При шифровании информация изменяется с использованием известного только законным пользователям способа. Доступ к зашифрованной информации, как правило, не ограничивается.

Криптографическая система (криптосистема, или шифр) состоит в преобразовании сообщения M, которое называется открытым текстом, с помощью шифровальной схемы таким образом, что только законный получатель может обратить это преобразование и восстановить сообщение.

Шифровальная схема обращается к функции шифрования E, которой кроме открытого текста M требуется также шифровальный ключ K, являющийся параметром, специфическим для каждого преобразования. Функция шифрования определяется алгоритмом, и результат процесса шифрования $E(K, M) = C$ называется шифрованным текстом или криптограммой. Текст C предается по незащищенному каналу, где противник может рассматривать его, запоминать, работать с ним и заменить его на C'.

Для создания системы обмена конфиденциальной информацией выбирается класс криптоалгоритмов. Обычно полагают, что класс криптоалгоритмов известен и задачей вскрытия системы обмена конфиденциальной информацией является нахождение ключа.

При проведении криптоанализа могут быть выполнены некоторые условия:

1) канал связи доступен;

2) класс криптоалгоритмов известен;

3) фрагмент открытого сообщения и соответствующая ему часть закрытого сообщения известны;

4) по произвольному сообщению можно получить соответствующее ему закрытое сообщение.

Система обмена конфиденциальной информацией называется криптостойкой, если при выполнении всех перечисленных допущений не существует эффективного алгоритма ее вскрытия.

Симметричные криптосистемы. В классической криптографии имеется два основных преобразования открытого текста сообщений вместе с их комбинациями:

1) транспозиции, или перестановки, переупорядочивают группу символов в соответствии с некоторым правилом, не меняя их, т.е. если сообщение M составлено из m блоков, $M = B_1B_2\dots B_m$, где каждый блок B_i содержит n символов $B_i = b_{i,1}b_{i,2}\dots b_{i,n}$, $i = 1,\ 2,\ \dots,\ m$, то шифрованный текст — это $C = C_1C_2\dots C_m$, где $C_i = b_{i,\pi(1)}b_{i,\pi(2)}\dots b_{i,\pi(n)}$ для каждого $i = 1,\ 2,\ \dots,\ m$, а π — фиксированная перестановка целых чисел $1, 2, \dots, n$.

2) подстановки замещают символы открытого текста соответствующими символами из алфавита шифрованного текста (ключ задает отображение), т.е. если сообщение — это $M = a_1a_2\dots a_n$, то шифрованный текст $C = f_1(a_1)f_2(a_2)\dots f_n(a_n)$ определяется с помощью n отображений из алфавита открытого текста в алфавит шифрованного текста.

3) Комбинация транспозиций и подстановок дает шифр подстановки/перестановки.

Асимметричные криптосистемы. Понятия криптосистемы открытого ключа было впервые введено Диффи и Хеллманом в 1976 г.

В традиционной (симметричной) криптографии каждая из переписывающихся сторон должна иметь копию общего секретного ключа, что создает сложнейшую проблему управления ключами. В асимметричных криптосистемах используются два ключа: открытый и секретный.

Открытый ключ может быть опубликован в справочнике наряду с именем пользователя. В результате любой желающий может зашифровать с его помощью свое письмо и послать закрытую информацию владельцу соответствующего секретного ключа.

Чтобы такая система имела право на существование, должен найтись простой метод, позволяющий получать процедуры E и D друг из друга. Желательно, чтобы процедуры E и D обладали следующими свойствами:

1) если M — открытый текст сообщения, то E и D должны быть такими, что $D[E(M)] = M$, т.е. расшифровка зашифрованного текста M дает M.

2) как E, так и D могут быть легко вычислены;

3) знание E не приводит к легкому способу вычисления D;

4) для каждого сообщения M должно быть $E[D(M)] = M$ (это полезно для реализации подписей).

Криптосистемы с открытым ключом основаны на понятии односторонней функции. Если для любого x имеет место соотношение $f(g(x)) = x$, то функцию $g(x)$ называют обратной функции $f(x)$ и обозначают через $f^{-1}(x)$. Сложность алгоритма вычисления значения $f(x)$ по значению x будем называть сложностью функции $f(x)$. Функция $f(x)$ называется односторонней, если ее сложность существенно меньше сложности обратной ей функции $f^{-1}(x)$.

Стоит отметить, что в настоящее время не существует функций, односторонность которых доказана.

Односторонние функции. Хорошо известным источником односторонних функций является задача факторизации больших чисел. Это сложная вычислительная задача. Для оценки сложности алгоритма, по которому целое число N может быть разложено на простые множители, часто используют функцию $L_N(\alpha, \beta) = \exp(\beta(\ln N)^{\alpha}(\ln \ln N)^{1-\alpha})$. Если такой алгоритм имеет сложность $O(L_N(0, \beta))$, то он является полиномиальным. Однако при сложности алгоритма $O(L_N(1, \beta))$ на его реализацию потребуется уже экспоненциальное время. Таким образом, скорость роста функции $L_N(\alpha, \beta)$ при $0 < \alpha < 1$ больше полиномиальной и меньше экспоненциальной. Поэтому про алгоритм со сложностью $O(L_N(\alpha, \beta))$ при $0 < \alpha < 1$ говорят, что он является субэкспоненциальным.

Сложные задачи, связанные с факторизацией (дано число $N = pq$, но не известен ни один из его простых делителей):

• факторизация — найти делители p и q числа $N = pq$;

• задача RSA — даны числа C и E, последнее из которых удовлетворяет соотношению НОД$(E, (p-1)(q-1)) = 1$. Требуется найти такое число m, что $m^E = C(modN)$;

• тест на квадратичный вычет — определить, является ли заданное число A полным квадратом по модулю N;

• извлечение квадратных корней по заданному модулю — по данному числу A, удовлетворяющему условию $A \equiv x^2(modN)$, вычислить x.

Другой класс односторонних функций связан с дискретным логарифмированием.

Пусть G — конечная абелева группа. Проблема вычисления дискретных логарифмов (ПДЛ) состоит в определении целого числа x, которое при данных $A,\ B \in G$ удовлетворяет соотношению $A^x = B$.

Для некоторых групп задача ПДЛ довольна проста. Однако, например, в мультипликативной группе конечного поля наилучший из известных алгоритмов решения ПДЛ — это метод квадратичного решета в числовом поле. Сложность вычисления дискретных логарифмов в этом случае оценивается как $L_N(1/3, c)$, где c — некоторая константа, зависящая от типа поля.

Для групп, подобных эллиптической кривой, задача дискретного логарифмирования еще более трудна. Сложность алгоритма, реализующего наилучший из доступных в настоящее время методов вычисления дискретных логарифмов, экспоненциальна.

Задачи, связанные с ПДЛ (дана конечная абелева группа G и ее элемент A):

• задача Диффи — Хеллмана — для заданных элементов $A \in G$, $B = A^x$ и $C = A^y$ вычислить $D = A^{xy}$;

• проблема выбора Диффи — Хеллмана — для заданных элементов $A \in G$, $B = A^x$, $C = A^y$ и $D = A^z$ требуется определить, является ли z произведением $x \cdot y$.

Пример протокола открытого распределения ключей. В статье [10] рассматриваются криптосистемы открытого распределения ключей, основанные на композиции двух проблем теории групп: проблемы сопряженности в некоммутативной группе и проблемы дискретного

логарифмирования в ее циклической подгруппе. Разрешимость некоторых из этих проблем в группах с условиями $C(p)$-$T(q)$ доказана в работах [5, 6, 7, 9]

В предлагаемых системах для построения общего ключа абоненты A и B выбирают общую неабелеву группу G и ее элемент g достаточно большого простого порядка.

Протокол получения общего ключа выглядит следующим образом.

1. Абонент A выбирает случайно элемент $X_1 \in G$ с условием $X_1 g \neq g X_1$ и число $x_1 \in Z_p$ (Z_p — поле классов вычетов по простому модулю p, элементы которого отождествляются с числами $0, 1, \ldots, p-1$), затем вычисляет элемент $Y_1 = X_1 g^{x_1} X_1^{-1}$ и отправляет его абоненту B.

2. Абонент B выбирает случайно элемент $X_2 \in G$ с условием $X_2 g \neq g X_2$ и число $x_2 \in Z_p$, вычисляет элемент $Y_2 = X_2 g^{x_2} X_2^{-1}$ и отправляет его абоненту A.

3. Абонент A вычисляет $K_1 = (X_1 Y_2 X_1^{-1})^{x_1} = X_1 X_2 g^{x_2 x_1} X_2^{-1} X_1^{-1}$.

4. Абонент B вычисляет $K_2 = (X_2 Y_1 X_2^{-1})^{x_2} = X_2 X_1 g^{x_1 x_2} X_1^{-1} X_2^{-1}$.

Если X_1 и X_2 выбраны так, что $X_1 X_2 = X_2 X_1$, то $K_1 = K_2 = K$, и K есть общий ключ абонентов A и B.

При выполнении этого протокола возникает техническая проблема выбора коммутирующих между собой и не коммутирующих с g элементов X_1, X_2. Эта проблема преодолевается путем выбора X_1, X_2 степенями одного и того же элемента h. Тогда вместо случайного выбора X_1, X_2 абоненты A и B выбирают соответственно случайные натуральные числа y_1, y_2, меньшие порядка элемента h, и в качестве X_1, X_2 используют соответственно элементы h^{y_1}, h^{y_2} группы G. При этом элемент h и числа y_1, y_2 выбираются так, чтобы h имел достаточно большой простой порядок, а элементы h^{y_1}, h^{y_2} не коммутировали с g. Общим секретным ключом будет $h^{y_1+y_2} g^{x_1 x_2} h^{-(y_1+y_2)}$.

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

В данной работе рассматривается возможность создания схемы открытого распределения ключей в группах, копредставление которых удовлетворяет условиям $C(3)$-$T(6)$. Таким образом, задача заключается в разработке процедуры получения общего секретного ключа с использованием открытого канала связи. Далее этот ключ может использоваться в системах симметричного шифрования.

Участники процесса:

1. Абонент A;
2. Абонент B;
3. Противник E.

Открытая информация:

1. Группа $G = reprXR$, копредставление которой удовлетворяет условиям $C(3)$-$T(6)$.
2. Слово w, представляющее некоторый элемент в G.

Алгоритм получения секретного ключа:

1. Абонент A выбирает произвольное целое число $n \in \mathbb{Z} \setminus \{0\}$ (закрытый ключ), вычисляет открытый ключ $K_1 = w^n$ и отправляет его абоненту B.

2. Абонент B выбирает произвольное целое число $m \in \mathbb{Z} \setminus \{0\}$ (закрытый ключ), вычисляет открытый ключ $K_2 = w^m$ и отправляет его абоненту A.

3. Абонент A вычисляет секретный ключ $K_1' = (K_2)^n = (w^m)^n$.

4. Абонент B вычисляет секретный ключ $K_2' = (K_1)^m = (w^n)^m$.

5. В группе G слова K_1' и K_2' равны и представляют элемент группы G с представителем $w^{nm} = K$.

Таким образом, K – общий секретный ключ.

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

Задача противника – получить секретный ключ K. Для этого необходимо определить один из закрытых ключей: n или m. Будем считать, что противник пытается вычислить n. Очевидно, что если $|w| = p$, а $|K_1| = q$, то $n = q/p$. Таким образом, значение закрытого ключа легко вычисляется по открытому ключу. Поэтому наша задача — провести преобразование w^n таким образом, чтобы n нельзя было легко вычислить, т.е. нужно заменить w^n некоторым словом v, которое равно w^n в группе G. В этом и будет состоять вычисление односторонней функции.

Односторонняя функция для получения открытого ключа. По аналогии с R- и $\bar{R}$-сокращениями определим следующие понятия. Будем говорить, что в слове w есть R-удлинение, если существует такой элемент $r \in R$, 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. Другими словами, если при R-сокращении подслово исходного слова заменяется буквой, то при R-удлинении буква исходного слова заменяется подсловом определяющего соотношения. И здесь мы пользуемся отмеченным выше свойством представлений с условием $T(q)$ при $q > 4$: любая буква является куском. Поэтому существует не меньше двух определяющих соотношений, с помощью которых можно выполнить R-удлинение в любой букве данного слова.

Будем говорить, что в слове w есть $\bar{R}_3$-удлинение, если существуют такие элементы r_1, r_2, $r_3 \in R$, 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) $w \equiv w_1w_2w_3w_4$;

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

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

7) $r_{23} \equiv r_{12}^{-1}$;

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

9) слова r_{12}, r_{13}, r_{22}, r_{23}, r_{32}, r_{33}, w_2, w_3 являются кусками;

В случае замены слова w равным ему в группе G словом $w_1r_{11}r_{21}r_{31}w_4$ будем говорить, что в w выполнено $\bar{R}_3$-удлинение.

Очевидно, что обратным преобразованием к R-удлинению будет R-сокращение, а к $\bar{R}_3$-удлинению – $\bar{R}$-сокращение с построением полосы из 3-х областей.

Для получения открытого ключа K_1 была предложена следующая функция $F(w, n)$. На вход $F(w, n)$ подается слово w и закрытый ключ n. Если $n < 0$, то $F(w, n) = F(w^{-1}, |n|)$. Функция $F(w, n)$ возвращает слово $v = w^n$, при этом в каждом вхождении слова w в v проводятся следующие преобразования:

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

2) R-удлинение в k-й позиции;

3) свободное сокращение в k-й и $(k + 1)$-й позициях, если такое сокращение возможно;

4) R-сокращение в позициях от k до $k + j$, $j = |r| - 2$, где $r \in R$ — определяющее соотношение, которое используется для сокращения, если такое сокращение возможно; если же такое сокращение провести невозможно, то выполняется преобразование 5;

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

6) $\bar{R}_3$-удлинение в k-й и $(k + 1)$-й позициях, если такое удлинение возможно.

Заметим, что можно было добавить еще два преобразования: $\bar{R}$-сокращение и $\bar{R}$-удлинение с помощью k соотношений при $k > 3$, в отличие от преобразования 6, в котором $k = 3$. Но это сильно усложнило бы и вычисление прямой функции.

Количество преобразований, их вид, а также позиция k в слове w выбираются случайным образом. Чтобы сделать процесс еще менее детерминированным, будем при каждом преобразовании использовать случайную перестановку множества R.

Ясно, что преобразования 1, 2 и 5 можно выполнить всегда. Причем, количество различных преобразований 1 равно числу образующих в X, количество различных преобразований 5 равно числу определяющих соотношений в R (вместе с циклическими перестановками и инверсиями). Так как любая буква в слове — это кусок, то существует, как минимум, два определяющих соотношения, которые можно использовать для R-удлинения в любой позиции слова w.

Понятно, что функция $F(w, n)$ должна удовлетворять следующим условиям:

1) на выходе должно получаться слово $v \neq w^n$ в свободной группе;

2) слово v должно быть таким, что $v \not\equiv w_1^n$, т.е. слово v не должно представлять собой степень n некоторого слова w_1, где $w_1 = w$ в группе G;

3) слово v должно быть равно слову w^n в группе G;

4) не должно существовать простого алгоритма, который позволял бы по v вычислить n или привести v к слову w^n, по которому уже легко определить n.

Условие 1, очевидно, выполняется, так как преобразования 1–4, 6 выбираются с равной вероятностью, а вероятность того, что возможны три из них равна единице. К тому же преобразования применяются ко всем вхождениям w в v. Поэтому вероятность того, что во всех вхождениях w в v будет произведено одно и более преобразований, зависит от их возможного количества. Для того, чтобы сделать случайным изменение длины каждого вхождения w в v, количество p преобразований в каждом w было решено также сделать случайным числом (в данной работе рассматривалась функция с $p \in [0.5|w|, 2|w|]$; как показали эксперименты, этого значения достаточно для выполнения условий 1 и 2).

Условие 2 также выполняется, так как в силу того, что вид преобразований, их количество в каждом w и, главное, позиция в слове w, где каждое преобразование выполняется, выбираются случайно, то ситуация, при которой во всех n вхождениях w в v будут произведены одинаковые преобразования, практически невозможна.

Условие 3 выполняется, так как ни одно преобразование из 1–6 не приводит к нарушению равенства слова v слову w^n в группе G.

Чтобы определить, выполняется ли условие 4, проанализируем возможные действия противника. Понятно, что, так как длина каждого вхождения w в v меняется случайно и, следовательно, $|v|$ не зависит от $|w|$, то n по v определить нельзя. Значит, единственное, что может сделать противник — попытаться восстановить слово w^n из v.

Пусть противник знает слово w и слово $v = w^n$. Чтобы получить слово w^n из слова v, необходимо провести преобразования, обратные тем, которые проводит функция $F(w, n)$: свободные сокращения, R-сокращения и $\bar{R}_3$-сокращения (т.е. $\bar{R}$-сокращения с построением полосы из трех областей). Так как прямые преобразования проводятся случайным образом, противник вынужден провести все указанные выше сокращения в слове v. Но в самом слове w могут быть данные сокращения, поэтому целесообразно сначала привести w к несократимому виду. Итак, у противника имеется слово $w_1 = w$, в котором нет указанных сокращений. Его задача — получить слово w_1^n из слова v. Для этого он в слове v проводит указанные три типа сокращений. Но так как $F(w, n)$ меняет слово случайно, а противник проводит сокращения слева направо по длине слова, то велика вероятность того, что сокращения будут произведены не там, где до этого были сделаны удлинения (стоит отметить, что в данном случае свободные и R-сокращения, которые делает функция $F(w, n)$, не играют роли) и w^n не будет восстановлено.

Оценка сложности $F(w, n)$. Оценим сложность процедуры получения открытого ключа. Так как $F(w, n)$ включает в себя операции, различные по сложности, определим

сначала наиболее сложную операцию и по ней оценим сверху сложность $F(w,n)$. Сложность операции в данном случае будем измерять в количестве сравнений букв, необходимых для проведения преобразования.

Наименее сложными являются преобразования 1 и 5, которые не требуют проведения сравнения букв. Таким образом, считаем, что $T_1 = T_5 = O(1)$.

Следующим по сложности идет 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+1} с x_k^{-1} и x_{k-1} с x_k^{-1}. Следовательно, $T_3 = O(1)$.

Сложность операции 2 (R-удлинение) зависит от количества n_R элементов в R и требует на каждом этапе поиска подходящего определяющего соотношения одного сравнения. Так как в R имеется как минимум два определяющих соотношения, имеющих общее начало (в виде одной буквы), то в худшем случае необходимое определяющее соотношение будет найдено на $(n_R - 1)$-м этапе поиска. Следовательно, для R-удлинения $T_2 = 1 \cdot (n_R - 1)$. (Следует отметить, что здесь, как и во всей работе, предполагается линейная процедура поиска.)

Наиболее сложными являются преобразования 4 (R-сокращение) и 6 ($\bar{R}_3$-удлинение). Преобразование 6 заключается в поиске трех определяющих соотношений (следовательно, имеется зависимость от n_R), для двух из которых проводится сравнение одной буквы, для третьего — двух букв. Так как в R имеется как минимум два определяющих соотношения, начинающихся на одну букву, а каждое двухбуквенное начало встречается в R только один раз, то $T_6 = 1 \cdot (n_R - 1) + 1 \cdot (n_R - 1) + 2 \cdot n_R = 3 \cdot n_R - 2$.

Сложность R-сокращения оценивается как $T_4 = (n_{\text{rmax}} - 1) \cdot n_R$, где $n_{\text{rmax}} = \max\limits_{r \in R} |r|$.

В дальнейшем сложность будет оцениваться в количестве построенных областей.

Итак, пусть функция $F(w,n)$ производит в каждом вхождении w в w^n в среднем p преобразований. Тогда всего преобразований в слове w^n будет $p' = np$, где p меняется от $0.5|w|$ до $2|w|$. Будем считать, что все преобразования — R-сокращения. Тогда оценка сверху для сложности $F(w,n)$ составляет $T_v = 2|w|n$. Так как считаем, что $|w| \ll n$, получаем $T_v = O(n)$. Таким образом, сложность получения открытого ключа K_1 линейно зависит от закрытого ключа n.

Получение закрытого ключа n противником. Противник получает по открытому каналу слово $v = F(w,n)$ и слово w. Чтобы узнать закрытый ключ, ему нужно решить уравнение относительно n: $w^n = v$ в группе G или, что то же самое, $w^n v^{-1} = 1$ в группе G. Для этого противник должен последовательно возводить w в степень k, где $k = \overline{1,n}$ (будем считать, что $n > 0$) и решать проблему равенства слов в группе G.

Для решения проблемы равенства слов в группах с условием $C(3)$-$T(6)$ используются процедуры циклических $R, \bar{R}$-сокращений: единственным циклически $R, \bar{R}$-несократимым словом, равным единице в группе G, является пустое слово [8]. Таким образом, после выполнения во всех циклических перестановках произвольного слова x всех $R, \bar{R}$-сокращений

получается либо циклически $R, \bar{R}$-несократимое слово x_1 (здесь $|x_1| \geq 1$) при $x \neq 1$ в G, либо пустое слово, если $x = 1$ в группе G.

Следовательно, противник, выполняя в слове $w^k v^{-1}$ все циклические $R, \bar{R}$-сокращения, будет получать непустые циклически $R, \bar{R}$-несократимые слова пока $k \neq n$; когда k станет равно n он получит единицу.

Получение оценки для n. Чтобы оценить сложность вычисления секретного ключа n, получим оценку сверху для n. Рассмотрим методику получения верхней оценки числа n с использованием вероятностных методов.

Оценка сверху получается исходя из следующего предположения: считаем, что вероятность того, что $|v| \geq |w^n|$ гораздо больше вероятности $|v| < |w^n|$. Докажем это, оценив вероятность следующих событий:

• под действием функции $F(w, n)$ при i-м преобразовании в k-й позиции произошло удлинение слова;

• под действием функции $F(w, n)$ при i-м преобразовании в k-й позиции произошло сокращение слова;

• под действием функции $F(w, n)$ при i-м преобразовании в k-й позиции длина слова не уменьшилась.

Среди шести преобразований, выполняемых функцией $F(w, n)$, имеется два преобразования сокращения и четыре преобразования удлинения. Выбор между пятью преобразованиями происходит с равной вероятностью.

Вероятность возможности R-удлинения равна вероятности возможности вставки тривиального слова и равна 1. Поэтому вероятности преобразований 1 и 2 в k-й позиции составляют, соответственно,

$$p_1 = \frac{1}{5} \cdot 1 = \frac{1}{5} \quad \text{и} \quad p_2 = \frac{1}{5} \cdot 1 = \frac{1}{5}.$$

Не будем оценивать вероятность возможности провести в k-й позиции $\bar{R}_3$-удлинение. Заметим только, что при преобразовании 6 длина слова либо увеличивается, либо не изменяется. Считаем, что $p_6 = \frac{1}{5}$.

Чтобы в k-й позиции произошло свободное сокращение, нужно, чтобы выполнялось хотя бы одно из двух равенств: $x_{k+1} = x_k^{-1}$ или $x_{k-1} = x_k^{-1}$. Если $|X| = n_x$, то число возможных различных двухбуквенных сочетаний в позициях k и $k+1$ составляет n_x^2, из которых n_x сочетаний вида $x_j x_j^{-1}$. Заметим, что k может быть равно $|w|$ или 1, т.е. в этом случае x_k — последняя или первая буква в слове. Таким образом, вероятность возможности свободного сокращения в позициях k и $k+1$ равна вероятности возможности свободного сокращения в позициях $k-1$ и k и составляет

$$p = \frac{n_x}{n_x^2 + n_x} = \frac{1}{n_x + 1}.$$

Вероятность свободного сокращения в k-й позиции составляет

$$p_3 = 2p \cdot \frac{1}{5} = \frac{2}{5(n_x + 1)}.$$

Оценим вероятность возможности R-сокращения в k-й позиции. Пусть $|X| = n_x$, $|R| = n_R$. Для простоты будем считать, что для всех $r_i \in R$ справедливо $|r_i| = 3$. Для R-сокращения необходимо выполнение следующего условия: $(\exists r \in R)(r = r_1 r_2 \wedge x_k x_{k+1} = r_1)$. Число различных двухбуквенных сочетаний (с учетом возможности $k = |w|$) составляет $n_x^2 + n_x$, число двухбуквенных сочетаний, в которых возможно провести R-сокращение, равно n_R. Следовательно, вероятность возможности R-сокращения в k-й позиции составляет

$$p = \frac{n_R}{n_x^2 + n_x}.$$

Пусть теперь $|r_i| = s + 1$. Тогда

$$p = \frac{n_R}{n_x^s + n_x^{s-1} + \ldots + n_x}.$$

Следует отметить, что при росте s числитель растет линейно (так как R содержит все циклические перестановка каждого r_i-го определяющего соотношения), а знаменатель — экспоненциально. Таким образом, при увеличении длины определяющих соотношений уменьшается вероятность возможности выполнить R-сокращение в k-й позиции.

Таким образом, максимальная вероятность R-сокращения в k-й позиции составляет

$$p_4 = \frac{1}{5} \frac{n_R}{n_x^{n_{rmin}-1} + n_x^{n_{\text{rmin}}-2} + \ldots + n_x},$$

где $n_{\text{rmin}} = \min\limits_{r \in R} |r|$.

Если R-сокращение невозможно, то в k-й позиции выполняется преобразование 5. Таким образом, минимальная вероятность вставки определяющего соотношения между x_k и x_{k+1} составляет

$$p_5 = \frac{1}{5}\left(1 - \frac{n_R}{n_x^{n_{\text{rmin}}-1} + n_x^{n_{\text{rmin}}-2} + \ldots + n_x}\right).$$

Обозначим через P_{short} вероятность того, что $|w'| < |w|$, через P_{long} вероятность того, что $|w'| > |w|$, а через $P_{\text{long+const}}$ вероятность $|w'| \geq |w|$; здесь w — исходное слово, w' — слово w после i-го преобразования. Тогда

$$P_{\text{long}} = p_1 + p_2 + p_5 == \frac{1}{5} \cdot \left(3 - \frac{n_R}{n_x^{n_{\text{rmin}}-1} + n_x^{n_{\text{rmin}}-2} + \ldots + n_x}\right);$$

$$P_{\text{long+const}} = P_{\text{long}} + p_6 + \left(\frac{1}{5} - p_3\right) = \frac{1}{5}\left(5 - \frac{n_R}{n_x^{n_{\text{rmin}}-1} + n_x^{n_{\text{rmin}}-2} + \ldots + n_x} - \frac{2}{n_x + 1}\right);$$

$$P_{\text{short}} = p_3 + p_4 = \frac{1}{5}\left(\frac{2}{n_x + 1} + \frac{n_R}{n_x^{n_{\text{rmin}}-1} + n_x^{n_{\text{rmin}}-2} + \ldots + n_x}\right).$$

Рассмотрим пример группы $G = \langle X;\ R\rangle$, для которой

$$X = \left\{a,\ b,\ c,\ a^{-1},\ b^{-1},\ c^{-1}\right\},$$

$$R = \Big\{cab,,\ bca,\ abc,\ b^{-1}a^{-1}c^{-1},\ a^{-1}c^{-1}b^{-1},\ c^{-1}b^{-1}a^{-1}\ ,$$
$$bac,\ cba,\ acb,\ c^{-1}a^{-1}b^{-1},\ a^{-1}b^{-1}c^{-1},\ b^{-1}c^{-1}a^{-1}\Big\}.$$

Подсчитаем $P_{\text{long+const}}$ и P_{short}:

$$P_{\text{long+const}} = \frac{1}{5}\left(5 - \frac{12}{6^2+6} - \frac{2}{6+1}\right) = \frac{31}{35}, \quad P_{\text{short}} = \frac{1}{5}\left(\frac{2}{6+1} + \frac{12}{6^2+6}\right) = \frac{4}{35}.$$

Видно, что вероятность события $F(w,n) = v \geq w^n$ гораздо больше, чем $F(w,n) = v < w^n$. Поэтому за оценку сверху можно принять

$$n_{\max} = \frac{|v|}{|w|}.$$

Таким образом, для нахождения секретного ключа n надо проверять равенства в группе G для всех $k = \overline{1,\ n_{\max}}$ вида: $w^k v^{-1} = 1$.

Теперь можно оценить сложность восстановления секретного ключа n по открытой информации, включающей в себя значения w и v. Но отложим решение этой задачи до следующего пункта, а пока попытаемся получить оценки числа n другим способом. Будем анализировать диаграммы равенства слов в группе G с условиями $C(3)$-$T(6)$.

Воспользуемся следующим результатом из [7].

Теорема 10. Если в приведенной односвязной R-диаграмме M с границей $\partial M = \sigma \cup \tau$ слова $\varphi(\sigma)$ и $\varphi(\tau)$ R-, $\bar{R}$-несократимы, то существует константа $C > 0$, для которой

$$|\varphi(\sigma)| \leq C|\varphi(\tau)|, \quad |\varphi(\tau)| \leq C|\varphi(\sigma)|.$$

В статье [6] приводится алгоритм построения нормальной формы w_0 слова w, сопряженной в группе G с $w^\varepsilon, \varepsilon \in \{1,2\}$, такой, что все степени слова w_0 R-, $\bar{R}$-несократимыми.

Сравнивая длины слов w^n и w_0^n, замечаем, что из несократимости последнего следует, что $|w^n| \geq |w_0^n|$, поскольку, как говорилось выше, при выполнении R-, $\bar{R}$-сокращений длина слова строго уменьшается. Если же окажется, что слово w^n несократимо, то к нему применимы неравенства, аналогичные приводимым ниже для w_0^n.

Действительно, в статье [7] доказано, что если R-, $\bar{R}$-несократимые слова u, v сопряжены в ($C(3)$-$T(6)$)-группе G, то $\dfrac{|u|}{9} \leq |v| \leq 9|u|$.

Итак, в группе G выполнены соотношения $w_0^n \sim w^n = v$, где v получено прямым вычислением односторонней функции. Заменим слово v равным ему в группе G несократимым словом v_0. Тогда существует число C, для которого выполнены следующие неравенства:

$$|w_0^n| \leq C|v_0| \leq C|v|$$

откуда

$$n \le \frac{C|v_0|}{|w_0|} \le \frac{C|v|}{|w_0|}.$$

Сказанное выше позволяет записать и обратные неравенства:

$$C|w_0^n| \ge |v_0| \implies n \ge \frac{|v_0|}{C|w_0|}.$$

Таким образом,

$$\frac{|v_0|}{C|w_0|} \le n \le \frac{C|v_0|}{|w_0|}.$$

Заметим, что в приведенных здесь оценках предполагается, что $|w_0^n| = n|w_0|$.

Сложность получения n. Сложность будем измерять количеством не дэновских, а просто областей: это позволит учитывать сложность $\bar{R}$-сокращений.

Зная границы, в которых заключено число n, проверяем в группе G равенства

$$w_0^k = v_0, \quad k \in \left[\frac{|v_0|}{C|w_0|}, \frac{C|v_0|}{|w_0|}\right].$$

По теореме о площади число областей в диаграмме равенства $w_0^k = v_0$ не превышает $O((k|w_0| + |v_0|)^2)$. Легко проверить, что суммирование таких оценок в указанных выше пределах для k приводит к верхней оценке сложности порядка $O(|v_0|^3)$.

Таким образом, сложность получения закрытого ключа n оценивается сверху полиномиальной функцией от n: $T_n = O(n^3)$.

Заметим, что эта оценка не изменится, если учесть сложность приведения слов w, v к несократимому виду w_0, v_0, соответственно, поскольку эта процедура в соответствии с теоремой о площади оценивается квадратичной функцией длины исходных слов w и v.

Требования к группе G и слову w. Предполагается, что слово w выбрано случайным образом. Оно не должно удовлетворять требованиям свободной или R-, $\bar{R}$-несократимости. Однако все же два требования к нему предъявляются:

- $w \ne 1$ в группе G;
- слово w должно представлять в группе G элемент бесконечного порядка.

Необходимость выполнения первого требования очевидна, так как если $w = 1$ в группе G, то $w^n = 1$ в G при всех n. Значит, единичными будут как открытые ключи K_1 и K_2, так и секретный ключ K.

Второе требование также является необходимым, поскольку если w представляет элемент конечного порядка, то $w^p = 1$ для некоторого p. Следовательно, противнику нужно будет найти не n, а остаток от деления n на p, что является гораздо более простой задачей, если учесть, что само p может быть найдено следующим образом.

В статьях [12, 13] доказано, что слово w в алфавите X тогда и только тогда представляет элемент конечного порядка в группе G с условиями $C(3)$-$T(6)$, когда $w \equiv v^s$ и в множестве R существует определяющее соотношение вида $r \equiv u^t$, причем слова u, v сопряжены в G. Следовательно, нужно либо организовать проверку конечности порядка w, либо потребовать, чтобы в R не было определяющих соотношений, которые представлены в виде степени какого-либо слова, что предпочтительнее.

Мы считаем, что группа G, используемая для шифрования, должна удовлетворять только условиям $C(3)$-$T(6)$. Однако, хотелось бы работать в таких группах, которые были бы оптимальны с точки зрения криптостойкости системы. Поэтому проанализируем, как копредставление группы влияет на следующие факторы:

- сложность получения открытого ключа;
- стойкость открытого ключа к обратным преобразованиям;
- длина открытого ключа;
- сложность взлома системы, измеренная в количестве областей;
- временная сложность вскрытия системы.

Любая группа полностью определяется своим копредставлением $\langle X;\ R\rangle$. Поэтому параметры группы, которые могут влиять на перечисленные факторы, — это мощность алфавита $|X|$, количество определяющих соотношений в симметризованном множестве $|R|$ и длина определяющих соотношений $|r_i|$. Нужно отметить, что между этими параметрами существует связь. Так, от $|X|$ зависит либо $|R|$, либо $|r_i|$, так как каждый элемент $x \in X$ должен встречаться в определяющих соотношениях как минимум два раза. Количество определяющих соотношений зависит от их длины, так как $|R|$ включает в себя все циклические перестановки определяющих слов. Поэтому будем рассматривать влияние только $|R|$ и $|r_i|$, считая, что данные два параметра зависят от $|X|$.

Временна́я сложность получения открытого ключа возрастает как с увеличением $|R|$, так и с увеличением $|r_i|$, поскольку возрастает временная сложность R-сокращений и $\bar{R}_3$-удлинений. При этом сложность, измеренная в областях, не меняется.

Длина открытого ключа увеличивается при увеличении $|r_i|$, так как при R-удлинении, $\bar{R}_3$-удлинении и вставке определяющего соотношения слово w получает большее приращение. Данный факт положительно влияет на криптостойкость алгоритма, но затрудняет дальнейшее использование такого ключа. Увеличение $|R|$ на данный фактор влияет неоднозначно: с одной стороны, увеличивается вероятность $\bar{R}_3$-удлинения, с другой стороны, также увеличивается вероятность R-сокращения.

Криптостойкость открытого ключа к обратным преобразованиям характеризуется вероятностью того, что после свободных сокращений, R- и $\bar{R}_3$-сокращений ключ не будет представлять w^n (что позволило бы противнику избежать процедуры решения проблемы слов при взломе). На данный фактор положительно влияет $|R|$.

Сложнее оценить влияние $|r_i|$ на сложность вскрытия системы (криптостойкость алгоритма). Так, сложность получения n имеет верхнюю оценку, полиномиально зависящую

от длины открытого ключа, которая возрастает при возрастании $|r_i|$. Временна́я сложность построение самих областей также увеличивается при возрастании $|r_i|$. В то же время, сложность, измеренная в областях, при увеличении $|r_i|$ может уменьшаться, так как за одно R- и $\bar{R}$-сокращение слово будет сокращаться на большее число букв.

Сложность $\bar{R}$-сокращений достигает максимума, когда $|r_i| = 3$ для всех $r_i \in R$, так как именно в этом случае каждая полоса сокращает слово ровно на одну букву.

Заключение

Оценка временно́й сложности носит субъективный характер. Понятно, что временна́я сложность вскрытия будет зависеть как от производительности вычислительной системы, так и от эффективности применяемых алгоритмов. В данной работе мы ограничились оценкой сложности, выраженной в количестве областей.

Был определен общий вид схемы открытого распределения ключей, основанной на проблеме равенства слов в группах с условиями $C(3)$-$T(6)$. Для этой схемы была предложена процедура генерирования открытого ключа, характеризующаяся линейной сложностью. Также была получена оценка криптостойкости алгоритма получения секретного ключа и исследовано влияние различных факторов на данный параметр.

Исследования показывают, что задача, на которой основана разработанная схема, имеет полиномиальную сложность решения. Поэтому криптостойкость такой системы недостаточна для обеспечения необходимого уровня защиты информации. Однако, надежность можно повысить, комбинируя проблему слов с другими алгебраическими проблемами: вхождения в циклическую подгруппу, сопряженности.

Список литературы

1. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп: пер. с англ. М.: Наука, 1974. 456 с.
2. Линдон Р., Шупп П. Комбинаторная теория групп: пер. с англ. М.: Мир, 1980. 448 с.
3. Ольшанский А.Ю. Геометрия определяющих соотношений в группах. М.: Наука, 1989. 448 с.
4. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Тр. Математического ин-та АН СССР. 1955. Т. 44. С. 1–144.
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 условиями $C(3)$-$T(6)$ // Известия ТулГУ. Естественные науки. 2010. Вып. 1. С. 6–25.

7. Безверхний Н.В. Проблема сопряженного вхождения в циклическую подгруппу в группах с условиями $C(3)$-$T(6)$ // 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. трудов. Тула: Изд-во ТГПУ им. Л.Н. Толстого, 1994. С. 4–58.
9. 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. трудов. Тула: изд-во ТГПУ им. Л.Н. Толстого. 2001. С. 120–139.
10. Глухов М.М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1, № 4. С. 5–22.
11. Паршикова Е.В. Проблема слабой степенной сопряженности в группах с условием $C(4)$-$T(4)$ // Алгоритмические проблемы теории групп и полугрупп: межвуз. сб. науч. трудов. Тула: Изд-во ТГПУ им. Л.Н. Толстого, 2001. С. 179–185.
12. Безверхний Н.В. О кручении о и разрешимости проблемы вхождения в циклическую подгруппу в группах с условием $C(6)$ // М., 1995. Деп. в ВИНИТИ, № 2033–В95.
13. Bogley W.A., Pride S.J. Aspherical relative presentations // Proc. of Edinburg Math. Soc. Ser. 2. 1992. Vol. 35, no. 1. P. 1–39. DOI: 10.1017/S0013091500005290
14. Gersten Sh., Short H.B. Small cancellation theory and automatic groups // Inventiones Mathematicae. 1990. Vol. 102, iss. 1. P. 305–334. DOI: 10.1007/BF01233430
15. Shor P.W. Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer // SIAM Journal on Computing. 1997. Vol. 26, no. 5. P. 1484–1509. DOI: 10.1137/S0097539795293172
16. An algebraic method for public key cryptography // Mathematical Research Letters. 1999. Vol. 6, no. 3. P. 287–291. DOI: 10.4310/MRL.1999.v6.n3.a3
17. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J., Park C. New Public-Key Cryptosystem Using Braid Groups // In: Advances in Cryptology — CRYPTO 2000. Springer Berlin Heidelberg, 2000. P. 166–183. (Ser. Lecture Notes in Computer Science; vol. 1880). DOI: 10.1007/3-540-44598-6_10
18. Yamamura A. Public-key cryptosystems using the modular group // In: Public Key Cryptography. Springer Berlin Heidelberg, 1998. P. 203–216. (Ser. Lecture Notes in Computer Science; vol. 1431). DOI: 10.1007/BFb0054026
19. Yamamura A. A Functional Cryptosystem Using a Group Action // In: Information Security and Privacy. Springer Berlin Heidelberg, 1999. P. 314–325. (Ser. Lecture Notes in Computer Science; vol. 1587). DOI: 10.1007/3-540-48970-3_26

20. Paeng S.-H., Ha K.-C., Kim J.H., Chee S., Park C. New Public Key Cryptosystem Using Finite Non Abelian Groups // In: Advances in Cryptology — CRYPTO 2001. Springer Berlin Heidelberg, 2001. P. 470–485. (Ser. Lecture Notes in Computer Science; vol. 2139). DOI: 10.1007/3-540-44647-8_28

21. Paeng S.-H., Kwon D., Ha K.-C., Kim J.H. Improved public key cryptosystem using non abelian groups. Cryptology ePrint Archive: Report 2001/066. Available at: http://eprint.iacr.org/2001/066, accessed 01.09.2014.

22. Sakalauskas E., Tvarijonas P., Raulinaitis A. Key agreement protocol (KAP) using conjugacy and discrete logarithms problems in group representation level // Informatica. 2007. Vol. 18, no. 1. P. 115–124.

Science & Education of the Bauman MSTU
Electronic journal
ISSN 1994-0448

Science and Education of the Bauman MSTU, 2014, no. 10, pp. 70–101.
DOI: **10.7463/1014.0729483**
Received: 29.06.2014
Revised: 06.10.2014

One-way functions based on the discrete logarithm problem in the groups meeting conditions $C(3)$-$T(6)$

Bezverkhniy N. V.[1,*], **Chernisheva O. A.**[1]

[*]nbezv@mail.ru

[1]Bauman Moscow State Technical University, Moscow, Russia

Keywords: one-way functions, small cancellation conditions, diagrams in groups, membership problem for cyclic subgroups.

In this work we are consider a possibility to create schemes of open key distribution in the groups meeting conditions $C(3)$-$T(6)$. Our constructions use the following algorithms.

1. The algorithm that solves the membership problem for cyclic subgroups, also known as the discrete logarithm problem.

2. The algorithm that solves the word problem in this class of groups.

Our approach is based on the geometric methods of combinatorial group theory (the method of diagrams in groups).

In a cryptographic scheme based on the open key distribution one-way functions are used, i.e. functions direct calculation of which must be much easier than that of the inverse one. Our task was to construct a one-way function using groups with small cancelation conditions $C(3)$-$T(6)$ and to compare the calculation complexity of this function with the calculation complexity of its inverse.

P.W. Shor has shown in the paper that there exists a polynomial algorithm that can be implemented in a quantum computer to solve the discrete logarithm problem in the groups of units of finite fields and the rings of congruences mod n. This stimulated a series of investigations trying to find alternative complicated mathematical problems that can be used for construction of new asymmetric cryptosystems. For example, open key distribution systems based on the conjugacy problem in matrix groups and the braid groups were proposed.

In the other papers the constructions used the discrete logarithm problem in the groups of inner automorphisms of semi-direct products of $SL(2,\mathbb{Z})$ and $\mathbb{Z}_p$ and $GL(2,\mathbb{Z}_p)$ and $\mathbb{Z}_p$. groups. The paper of E. Sakalauskas, P. Tvarijonas, A. Raulinaitis proposed a scheme that uses a composition of two problems of group theory, namely the conjugacy problem and the discrete logarithm problem.

Our results show that the scheme that we propose is of polynomial complexity. Therefore its security is not sufficient for further applications in communications. However the security can be improved through combining the word problem with other algebraic problems such as the problem of the membership in the cyclic subgroups and the conjugacy problem.

References

1. Magnus W., Karras A., Solitar D. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*. John Wiley and Sons, Inc., New York-London-Sydney, 1966. 444 p. (Russ. ed.: Magnus W., Karras A., Solitar D. *Kombinatornaja teorija grupp*. Moscow, Nauka Publ., 1974. 456 p.).
2. Lyndon R., Schupp P. *Combinatorial group theory*. Springer-Verlag, Berlin, 1977. (Russ. ed.: Lyndon R., Schupp P. *Kombinatornaja teorija grupp*. Moscow, Mir Publ., 1980. 448 p.).
3. Ol'shanskii A.Iu. *Geometriia opredeliaiushchikh sootnoshenii v gruppakh* [The geometry of dening relations in groups]. Moscow, Nauka Publ., 1989. 448 p. (in Russian).
4. Novikov P.S. On the algorithmic unsolvability of word identity problem in group theory. *Tr. Matematicheskogo in-ta AN SSSR* [Proc. of Mathematical Institute of the USSR Academy of Sciences], 1955, vol. 44, pp. 1–144. (in Russian).
5. Bezverkhnij N.V. On the solvability of the general word problem for a cyclic subgroup of a group with condition $C(6)$. *Fundamental'naia i prikladnaia matematika*, 1999, vol. 5, no. 1, pp. 39–46. (in Russian).
6. Bezverhnij N.V. Normal forms for elements of infinite order in group with $C(3)$-$T(6)$ condition. *Izvestija TulGU. Estestvennye nauki*, 2010, iss. 1, pp. 6–25. (in Russian).
7. Bezverhnij N.V. The power conjugacy search problem in a cyclic subgroup in groups with the condition $C(3)$-$T(6)$. *Diskretnaja matematika*, 2012, vol. 24, iss. 4, pp. 27–46. (English Translation: *Discrete Mathematics and Applications*, 2012, vol. 22, iss. 5–6, pp. 521–544. DOI: 10.1515/dma-2012-036).
8. Bezverhnij V.N. On normalizers of elements in $C(p)$-$T(q)$-groups. *Algoritmicheskie problemy teorii grupp i polugrupp: mezhvuz. sb. nauch. trudov* [Algorithmic problems of the theory of groups and semigroups: interuniversity collection of scientific papers]. Tula, Tolstoi TSPU Publ., 1994, pp. 4–58. (in Russian).
9. Bezverhnij V.N., Parshikova E.V. The solution of problems of integration in a cyclic subgroup of a group with condition $C(4)$-$T(4)$. *Algoritmicheskie problemy teorii grupp i polugrupp: mezhvuz. sb. nauch. trudov* [Algorithmic problems of the theory of groups and semigroups: interuniversity collection of scientific papers]. Tula, Tolstoi TSPU Publ., 2001, pp. 120–139. (in Russian).
10. Glukhov M.M. An analysis of some key distribution public systems based on non-abelian groups. *Matematicheskie voprosy kriptografii*, 2010, vol. 1, no. 4, pp. 5–22. (in Russian).

11. Parshikova E.V. The problem of weak power conjugacy in groups with condition $C(4)$-$T(4)$. *Algoritmicheskie problemy teorii grupp i polugrupp: mezhvuz. sb. nauch. trudov* [Algorithmic problems of the theory of groups and semigroups: interuniversity collection of scientific papers]. Tula, Tolstoi TSPU Publ., 2001, pp. 179–185. (in Russian).
12. Bezverhnij N.V. *O kruchenii i o razreshimosti problemy vhozhdenija v ciklicheskuju podgruppu v gruppah s usloviem* $C(6)$ [On torsion and solvability of the general word problem for a cyclic subgroup of a group with condition $C(6)$]. Moscow, 1995. Dep. VINITI no. 2033–V95. (in Russian).
13. Bogley W.A., Pride S.J. Aspherical relative presentations. *Proc. of Edinburg Math. Soc. Ser. 2*. 1992, vol. 35, no. 1, pp. 1–39. DOI: 10.1017/S0013091500005290
14. Gersten Sh., Short H.B. Small cancellation theory and automatic groups. *Inventiones Mathematicae*, 1990, vol. 102, iss. 1, pp. 305–334. DOI: 10.1007/BF01233430
15. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 1997, vol. 26, no. 5, pp. 1484–1509. DOI: 10.1137/S0097539795293172
16. Anshel I., Anshtl 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
17. Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J., Park C. New Public-Key Cryptosystem Using Braid Groups. In: *Advances in Cryptology — CRYPTO 2000*. Springer Berlin Heidelberg, 2000, pp. 166–183. (Ser. *Lecture Notes in Computer Science*; vol. 1880). DOI: 10.1007/3-540-44598-6_10
18. Yamamura A. Public-key cryptosystems using the modular group. In: *Public Key Cryptography*. Springer Berlin Heidelberg, 1998, pp. 203–216. (Ser. *Lecture Notes in Computer Science*; vol. 1431). DOI: *10.1007/BFb0054026*
19. Yamamura A. A Functional Cryptosystem Using a Group Action. In: *Information Security and Privacy*. Springer Berlin Heidelberg, 1999, pp. 314–325. (Ser. *Lecture Notes in Computer Science*; vol. 1587). DOI: 10.1007/3-540-48970-3_26
20. Paeng S.-H., Ha K.-C., Kim J.H., Chee S., Park C. New Public Key Cryptosystem Using Finite Non Abelian Groups. In: *Advances in Cryptology — CRYPTO 2001*. Springer Berlin Heidelberg, 2001, pp. 470–485. (Ser. *Lecture Notes in Computer Science*; vol. 2139). DOI: 10.1007/3-540-44647-8_28
21. Paeng S.-H., Kwon D., Ha K.-C., Kim J.H. *Improved public key cryptosystem using non abelian groups*. Cryptology ePrint Archive: Report 2001/066. Available at: http://eprint.iacr.org/2001/066, accessed 01.09.2014.
22. Sakalauskas E., Tvarijonas P., Raulinaitis A. Key agreement protocol (KAP) using conjugacy and discrete logarithms problems in group representation level. *Informatica*, 2007, vol. 18, no. 1, pp. 115–124.