2012 Теоретические основы прикладной дискретной математики №3(17)

DOI 10.17223/20710410/17/2

УДК 512.62

О ПОСТРОЕНИИ ВОЗМОЖНО ОДНОСТОРОННИХ ФУНКЦИЙ НА ОСНОВЕ АЛГОРИТМИЧЕСКОЙ НЕРАЗРЕШИМОСТИ ПРОБЛЕМЫ ЭНДОМОРФНОЙ СВОДИМОСТИ В ГРУППАХ

С. Ю. Ерофеев, В. А. Романьков

Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия

E-mail: stepan.erofeev@gmail.com, romankov48@mail.ru

Рассматривается схема построения возможно односторонней функции в группе с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости. Анализируются предпосылки криптографической стойкости предлагаемой схемы. В качестве приложения предлагается схема аутентификации с нулевым разглашением пользователей в системе. Отмечается, что для её криптостойкости требуется неразрешимость более сильной проблемы двукратной эндоморфной сводимости.

Введение

Работа относится к «криптографии, основанной на группах» (group-based cryptography), — современному направлению, возникшему на рубеже XX и XXI столетий. Основными объектами в нём являются абстрактные бесконечные группы, а основной целью — построение на этих группах криптографических схем и протоколов. Исследования ведутся методами теории групп, теории сложности и теории вычислений.

Современное состояние полученных в этой области результатов отражено в монографиях [1, 2] (см. также обзор второго автора [3]).

Основной целью настоящей работы является представление конструкции возможно односторонней функции на основе алгоритмической неразрешимости проблемы эндоморфной сводимости в группах.

Односторонние (в другой терминологии *однонаправленные*) функции являются неотъемлемой частью криптографических схем и протоколов. Теоретически их существование при формальном определении до сих пор не установлено. В то же время односторонние функции являются основным инструментом во многих разделах и приложениях криптографии, в частности, они применяются в электронных подписях, протоколах аутентификации, алгоритмах генерации псевдослучайных последовательностей и т. п. Конечно, используемые с указанной целью функции можно назвать только *возможно односторонними*.

Относительно общей теории односторонних функций см. монографии [4 – 6]. В работах Л. А. Левина [7, 8] приведена универсальная функция, которая автоматически является односторонней, если существует хотя бы одна формально односторонняя функция. Такие функции названы *полными односторонними* функциями. Для их построения Л. А. Левин использовал нумерацию всех машин Тьюринга [7] и комбинаторный тайлинг [8]. Отсюда видно, что такое построение имеет чисто теоретическое значение. В работе А. А. Кожевникова и С. И. Николенко [9] приведены другие примеры полных односторонних функций.

В данной работе предлагается новый кандидат на роль односторонней функции. В качестве платформы для неё рассматривается бесконечная группа с разрешимой

проблемой равенства и неразрешимой проблемой эндоморфной сводимости. Конкретное предложение — свободная метабелева группа M_n достаточно большого ранга n.

Теоретическая база в данном случае была заложена в работе В. А. Романькова [10], где доказана неразрешимость проблемы эндоморфной сводимости в свободных метабелевых группах достаточно большого ранга. Заметим, что разрешимость проблемы равенства в свободных метабелевых группах ко времени появления работы [10] была не только хорошо известна, но уже существовали вполне эффективные с практической точки зрения алгоритмы её решения.

Более точно, В. А. Романьков в работах [10, 11] ввёл в рассмотрение интерпретацию диофантовых уравнений в свободных нильпотентных группах ступени $\geqslant 9$ и в свободных метабелевых группах достаточно большого ранга, позволяющую перенести алгоритмическую неразрешимость 10-й Проблемы Гильберта, установленную Ю. В. Матиясевичем в [12, 13] (см. также [14]), на алгоритмическую неразрешимость проблемы эндоморфной сводимости в рассматриваемых группах. Оценка на ранг следовала из результатов Матиясевича.

В работе [3] дан обзор исследований по криптографии, основанной на группах. Объяснены возможности использования неразрешимых и трудноразрешимых алгоритмических проблем теории групп в качестве основы для построения криптографических схем и протоколов. Об этих возможностях и их реализациях см. также [1, 2, 15 – 19].

В работе [3] введено понятие диофантовой криптографии. Показана универсальность диофантова языка, позволяющая записывать на нём функции многих известных схем и протоколов криптографии. Подчёркнута объединяющая роль диофантовой криптографии. Описаны её возможности, вытекающие из неразрешимости 10-й Проблемы Гильберта. Данная работа также основана на представленном в [3] материале. Более того, в [3] подробно обоснованы достоинства свободных метабелевых групп как платформ для построения криптографических схем и протоколов, что также лежит в основе предлагаемой конкретной реализации протокола аутентификации с нулевым разглашением.

1. Односторонние функции

Неформально *односторонней* называется функция f, значение $y = f(x)$ которой легко вычислимо по аргументу x, а обращение, то есть вычисление по данному y хотя бы одного аргумента x', такого, что $y = f(x')$, является трудной задачей.

Обычно первое из этих условий трактуется как существование детерминированного алгоритма, вычисляющего по аргументу (*входу*) x значение $y = f(x)$ за *время* (количество шагов), не превышающее $p(|x|)$, где $p(\cdot)$ — некоторый полином, $|x|$ — размер входа.

Второе условие, то есть трудность обращения, означает, что любой вероятностный алгоритм, полиномиальный по $|y|$, вычисляет x' с условием $y = f(x')$ с пренебрежимо малой вероятностью.

В первом томе монографии О. Голдрейха [4] даны следующие определения.

Определение 1 (сильно односторонняя функция). Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется *сильно односторонней*, если выполнены следующие требования:

а) существует детерминированный полиномиальный по времени алгоритм $\mathcal{A}$, вычисляющий по аргументу x значение $y = f(x)$;

б) для любого вероятностного полиномиального по времени алгоритма $\mathcal{B}$, любого полинома $p(\cdot)$ и всех достаточно больших натуральных чисел n выполняется неравен-

ство

$$\Pr\left[\mathcal{B}(f(U_n), 1^n) \in f^{-1}(f(U_n)\right] < \frac{1}{p(n)},$$

где U_n означает случайную величину, равномерно распределенную на $\{0,1\}^n$. Заметим, что алгоритму предписан размер его выхода. Это объясняется тем, что размер аргумента x может не вычисляться как полиномиальная функция от $|y|$. В [4] приводится пример, когда в качестве значения функции $f(x)$ берется $|x|$. Заметим, однако, что в данном примере вход x' с условием $y = f(x')$ находится очевидным образом и может быть записан с использованием компрессии полиномиально от $|y|$. Это показывает, что определение 1, возможно, нуждается в коррекции. Алгоритмы с компрессионной записью получили в настоящее время существенное развитие в теории вычислений и в теории групп; см. по этому поводу [20 – 22].

Определение 2 (слабо односторонняя функция). Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется *слабо односторонней*, если выполнены следующие требования:

а) = а) из определения 1;

б) существует полином $p(\cdot)$, такой, что для любого вероятностного полиномиального по времени алгоритма $\mathcal{B}$ и всех достаточно больших натуральных чисел n выполняется неравенство

$$\Pr\left[\mathcal{B}(f(U_n), 1^n) \notin f^{-1}(f(U_n)\right] > \frac{1}{p(n)}.$$

В [4] доказано, что существование слабо односторонней функции влечет существование сильно односторонней функции.

Приведённые определения связаны с бинарным представлением аргументов и значений функций. Для задания возможно односторонней функции, определённой на группе, можно использовать следующие соображения. Во-первых, на конечно порождённой группе G с фиксированным множеством порождающих элементов можно задать словарную метрику, согласно которой расстояние $|g|$ от элемента g до 1 (его длина) равна наименьшей длине группового слова от фиксированного множества порождающих элементов группы, записывающего элемент g. Расстояние между элементами g и f определяется как $|gf^{-1}|$. Метрика позволяет естественным образом определить сферы $\mathbb{S}_r$ и шары $\mathbb{B}_r$ радиуса r, которые дадут стратификацию множества элементов группы. Определения 1 и 2 переписываются следующим образом.

Определение 1′ (сильно односторонняя функция). Функция $\varphi : G \to G$ называется *сильно односторонней*, если выполнены следующие требования:

а) существует детерминированный полиномиальный по времени алгоритм $\mathcal{A}$, вычисляющий по аргументу g значение $f = \varphi(g)$;

б) для любого вероятностного полиномиального по времени алгоритма $\mathcal{B}$, любого полинома $p(\cdot)$ и всех достаточно больших натуральных чисел n выполняется неравенство

$$\Pr\left[\mathcal{B}(\varphi(U_n), \mathbb{B}_n) \in \varphi^{-1}(\varphi(U_n)\right] < \frac{1}{p(n)},$$

где U_n означает случайную величину, равномерно распределенную на $\mathbb{B}_n$. Как и раньше, алгоритму предписан размер его выхода.

Определение 2′ (слабо односторонняя функция). Функция $\varphi : G \to G$ называется *слабо односторонней*, если выполнены следующие требования:

а) = а) из определения $1'$;

б) существует полином $p(\cdot)$, такой, что для любого вероятностного полиномиального по времени алгоритма $\mathcal{B}$ и всех достаточно больших натуральных чисел n выполняется неравенство

$$\Pr\left[\mathcal{B}(\varphi(U_n), \mathbb{B}_n) \notin \varphi^{-1}(\varphi(U_n)\right] > \frac{1}{p(n)}.$$

Во многих случаях приведённые определения сводятся к определениям 1 и 2 кодированием элементов группы бинарными последовательностями.

Известными кандидатами на роль односторонних являются следующие функции.

Степенная функция

$$f : x \longmapsto c = x^e \bmod n, \tag{1}$$

определённая на кольце $\mathbb{Z}_n$ вычетов по модулю n, где $n = pq$ — произведение больших различных (секретных) простых чисел. Для её обратимости требуется взаимная простота показателя e со значением функции Эйлера $\varphi(n) = (p-1)(q-1)$.

Задача обращения функции (1) равносильна нахождению решения диофантова уравнения

$$c = \zeta_1^e + n\zeta_2$$

относительно переменных ζ_1, ζ_2, или, что равносильно, задаче обращения диофантовой функции

$$d(\zeta_1, \zeta_2) = \zeta_1^e + n\zeta_2.$$

Функция (1) используется в качестве функции шифрования в системе RSA и в качестве цифровой подписи на основе RSA. Эта функция фигурирует также в ряде других схем, базирующихся на сложности задачи разложения чисел на множители.

Показательная функция

$$g : x \longmapsto g^x, \tag{2}$$

определённая на кольце целых чисел $\mathbb{Z}$ со значениями в конечном поле $\mathbb{F}_q$ порядка q, где g — порождающий элемент мультипликативной (циклической) группы $\mathbb{F}_q^*$. Криптостойкость её основана на трудности вычисления дискретного логарифма в конечных полях.

Её обращение равносильно обращению некоторой диофантовой функции $d(\zeta_1, \ldots, \zeta_k)$. Это следует из результатов Ю. В. Матиясевича [12, 13].

В случае простого конечного поля $\mathbb{F}_p = \mathbb{Z}_p$ характеристики p явный вид полинома $d(\zeta_1, \ldots, \zeta_k)$ можно найти в [23, 24].

Функция (2) используется, например, в системе шифрования Эль Гамаля, известных протоколах Диффи — Хеллмана, Масси — Омуры, базовом протоколе Эль Гамаля цифровой подписи и других схемах (см. по этому поводу [25, 26]).

Два приведённых выше примера криптографических функций являются частными случаями диофантовых функций. Диофантова криптография, относительно которой см. [3], позволяет не только использовать универсальный диофантов язык для представления многих известных криптографических функций, но также играть объединяющую роль для этих функций, записывая системы соответствующих им диофантовых уравнений. При этом появляется дополнительная возможность комбинирования и преобразования переменных.

2. 10-я Проблема Гильберта и проблема эндоморфной сводимости

2.1. 10-я Проблема Гильберта

Диофантовым называется полином $d(\zeta_1, \ldots, \zeta_k)$ с целыми коэффициентами от независимых коммутирующих переменных $\zeta_1, \ldots, \zeta_k$.

Уравнение вида

$$d(\zeta_1, \ldots, \zeta_k) = 0 \tag{3}$$

называется *диофантовым уравнением*. Ю. В. Матиясевич в работе [12] (полное доказательство в [13], см. также [14]) установил неразрешимость 10-й Проблемы Гильберта, тем самым завершив усилия ряда математиков, в частности Д. Робинсон, М. Дэвиса и Х. Патнэма. А именно, он доказал, что не существует алгоритма, определяющего по произвольному диофантову уравнению (3), обладает ли оно решением в целых числах. Данный результат часто называют неразрешимостью 10-й Проблемы Гильберта. Более того, Ю. В. Матиясевич заметил, что существует фиксированный диофантов полином $d_0(\zeta_1, \ldots, \zeta_k)$, такой, что алгоритмически неразрешима проблема существования решений в целых числах в классе диофантовых уравнений вида

$$d_0(\zeta_1, \ldots, \zeta_k) = c, \tag{4}$$

где c — произвольное целое число.

В работе Ю. В. Матиясевича и Д. Робинсон [27] неразрешимость 10-й Проблемы Гильберта установлена для класса уравнений от 13 переменных, в докладе Ю. В. Матиясевича [28] было объявлено, что количество переменных может быть уменьшено до 9. Эта оценка изложена со всеми деталями в работе Д. Джонса [29].

Функция $d_0(\zeta_1, \ldots, \zeta_k)$ может рассматриваться в качестве кандидата на роль односторонней функции. Действительно, любое её значение вычислимо за полиномиальное время от $|\zeta_1|+\ldots+|\zeta_k|$. В то же время из-за неразрешимости 10-й Проблемы Гильберта нельзя указать полиномиальный по времени алгоритм, вычисляющий аргумент этой функции с заданным значением.

2.2. Проблема эндоморфной сводимости

Будем говорить, что в эффективно заданной группе G разрешима проблема *эндоморфной сводимости*, если существует алгоритм, решающий для любой пары элементов g и f группы G, является ли f образом элемента g для какого-либо эндоморфизма $\varphi \in \operatorname{End} G$ или нет.

Эффективность задания группы G, способы записи её элементов и способы задания эндоморфизмов могут быть разными. Подробно об этом говорится в работе [3]. В классическом случае группа G предполагается конечно определённой и задаётся своим представлением через конечные множества порождающих элементов и определяющих соотношений вида

$$\mathcal{P}(G) = \langle x_1, \ldots, x_n | r_1 = 1, \ldots, r_m = 1 \rangle,$$

где $r_1, \ldots, r_m$ — групповые слова от $x_1, \ldots, x_n$, называемые *определяющими словами*.

Это означает, что группа G есть фактор-группа F_n/R свободной группы F_n ранга n с базисом $\{x_1, \ldots, x_n\}$ по нормальному замыканию $R = \text{нз}(r_1, \ldots, r_m)$, то есть по наименьшей нормальной подгруппе свободной группы F_n, содержащей определяющие слова $r_1, \ldots, r_m$. Группа G является каноническим гомоморфным образом группы F_n относительно гомоморфизма $g \mapsto gR$. Ядром этого гомоморфизма является R. Группа G порождается элементами $y_i = x_i R$ для $i = 1, \ldots, n$. Обычно эти элементы обозначают

так же, как их прообразы — через x_i $(i = 1, \ldots, n)$. Элементы группы G записываются, вообще говоря, неоднозначно, как групповые слова от порождающих. Эндоморфизм задается отображением порождающих $x_i \mapsto g_i$ для $i = 1, \ldots, n$. Не всякое такое отображение определяет эндоморфизм. Необходимым и достаточным условием для такого определения является проверка того, что значения определяющих слов после подстановки вместо порождающих элементов их образов равны 1 в группе G. Если группа G свободна с базисом $\{x_1, \ldots, x_n\}$, то есть множество определяющих соотношений пусто, или свободна в некотором многообразии $\mathcal{L}$ групп (свободная абелева, нильпотентная, метабелева и т. д.), то любое отображение порождающих элементов однозначно продолжается до эндоморфизма группы. Относительно многообразий групп см. монографию Х. Нейман [30].

Легко показать, что проблема эндоморфной сводимости разрешима для любой конечно порождённой абелевой группы. Из разрешимости уравнений в свободной группе F_n при любом n, доказанной Г. С. Маканиным [31], следует разрешимость проблемы эндоморфной сводимости в группе F_n. В то же время найдены достаточно просто задаваемые группы, в которых проблема эндоморфной сводимости оказалась неразрешимой. Среди них свободные метабелевы группы M_n достаточно большого ранга n. Перейдём к описанию этого результата работы [10] (см. также [3]).

Свободная метабелева группа M_n ранга n определяется как фактор-группа свободной группы F_n ранга n по второму коммутанту F_n''. Она является свободной группой многообразия всех метабелевых групп $\mathcal{A}^2$. Для свободных порождающих $x_1, \ldots, x_n$ группы M_n определяются *базисные коммутаторы* — коммутаторы от элементов базиса $x_1, \ldots, x_n$ вида $[\ldots[[x_{i_1}, x_{i_2}], x_{i_3}], \ldots, x_{i_l}]$, где $l \geqslant 2$ называется *весом* коммутатора и выполняются неравенства $i_1 > i_2$; $i_2 \leqslant i_3 \leqslant \ldots \leqslant i_l$. Сами порождающие $x_1, \ldots, x_n$ также считаются базисными коммутаторами веса 1. В базисных коммутаторах скобки стоят слева направо. Коммутаторы с такой расстановкой скобок называются *левонормированными* или *простыми*. Для них внутренние скобки обычно не указываются.

Известно [32, 33], что образы базисных коммутаторов веса i относительно канонического гомоморфизма $M_n \to M_n/\gamma_{i+1}M_n$ образуют базис свободной абелевой группы $\gamma_i M_n/\gamma_{i+1}M_n$. Здесь $\gamma_i M_n$ означает член нижнего центрального ряда группы M_n с номером i. Для произвольной группы G по определению $\gamma_1 G = G$, $\gamma_2 G = G'$ (коммутант) и для любого $i \geqslant 3$ полагается $\gamma_i G = [\gamma_{i-1}G, G]$. Напомним, что для произвольных подмножеств A и B группы G выражение $[A, B]$ означает взаимный коммутант этих подмножеств, то есть подгруппу, порождённую в G всеми коммутаторами вида $[a, b]$, где $a \in A$, $b \in B$. Группа G называется *нильпотентной*, если для некоторого i имеем $\gamma_i G = 1$. Наименьшее i с этим свойством называется *ступенью нильпотентности* группы G. Тривиальная группа имеет по определению ступень нильпотентности 0, нетривиальная абелева группа — ступень 1 и т. д. Для более детальной информации см. [30, 32 – 35].

Упорядочим все базисные коммутаторы группы M_n по возрастанию весов. Продолжим этот частичный порядок до полного, упорядочив между собой базисные коммутаторы одного веса произвольным образом. Пусть $c_1, \ldots, c_t$ $(t = t(i))$ — полный список всех базисных коммутаторов веса не больше чем i в заданном порядке. Обычно считают, что $c_j = x_j$ для $j = 1, \ldots, n$, то есть что порядок на порождающих элементах как базисных коммутаторах веса 1 соответствует порядку на индексах. Тогда любой

элемент группы M_n при $n \geqslant 2$ для любого $i \geqslant 1$ однозначно записывается в виде

$$g = \prod_{j=1}^{t} c_j^{k_j} (\mathrm{mod} \gamma_{i+1} M_n) \text{ для некоторых } k_j \in \mathbb{Z}.$$

Таким образом по модулю $\gamma_{i+1}M_n$ элементы группы M_n кодируются наборами целых чисел $(k_1, \ldots, k_t)$, где $t = t(i)$. Компоненты набора будем называть *координатами* элемента g по модулю $\gamma_{i+1}M_n$. Легко видеть, что координаты при различных i соответствуют друг другу в очевидном смысле.

Возьмём множество диофантовых уравнений вида (4). Считаем левую часть произвольным полиномом. Построим по такому уравнению пару элементов группы M_{k+2}. Элемент g строится следующим образом. Пусть наибольшая степень мономов в записи левой части (4) равна m. Полагаем $s = m$, если $m \geqslant 4$, и $s = 6$, если $m \leqslant 3$. Выделим два базисных элемента x_1 и x_2. Каждой переменной ζ_i сопоставим элемент базиса x_{i+2}. Пусть моном $\zeta_1^{l_1} \ldots \zeta_k^{l_k}$ входит в каноническую запись полинома $d_0(\zeta_1, \ldots, \zeta_k)$ с коэффициентом b. Сопоставим ему степень базисного коммутатора веса $s+2$ вида

$$[x_2, x_1, x_2, \ldots, x_2, x_3, \ldots, x_3, \ldots, x_k, \ldots, x_k]^b,$$

где порождающий x_j для $j = 3, \ldots, k+2$ имеет l_{j-2} вхождений, x_1 — одно вхождение, x_2 имеет $s - l_1 - \ldots - l_k - 1$ вхождение. Обозначим через $V(d_0)$ произведение всех полученных степеней базисных коммутаторов веса $s+2$ (по одному для каждого монома). Определим первый из элементов как

$$g = [x_2, x_1, x_1, x_2] V(d_0).$$

Второй элемент определим как

$$f = f(c) = [x_2, x_1, x_1, x_2][x_2, x_1, x_2, \ldots, x_2]^c, \tag{5}$$

где базисный коммутатор $h = [x_2, x_1, x_2, \ldots, x_2]$ второго множителя имеет вес $s+2$.

В [10] доказано, что если элемент f является эндоморфным образом элемента g в группе M_{k+2} по модулю $\gamma_{s+3}M_{k+2}$ для некоторого эндоморфизма $\mu : M_{k+2} \to M_{k+2}$, то

$$\mu(x_i) = x_i \pmod{\gamma_2 M_{k+2}} \text{ для } i = 1, 2. \tag{6}$$

И если

$$\mu(x_j) = x_1^{\alpha_{j-2}} x_2^{\beta_{j-2}} \pmod{\gamma_2 M_{k+2}} \text{ для } j = 3, \ldots, k+2, \tag{7}$$

то $\zeta_1 = \beta_1, \ldots, \zeta_k = \beta_k$ является решением диофантова уравнения (4). Таким образом, если бы существовал алгоритм, решающий проблему эндоморфной сводимости фиксированного элемента g группы M_{k+2} к элементу $f = f(c)$ для произвольного целого числа c по модулю $\gamma_{s+3}M_{k+2}$, то существовал бы алгоритм, решающий проблему существования решения у уравнений вида (4). Как мы отмечали выше, такого алгоритма нет. Значит, проблема эндоморфной сводимости в группе M_{k+2} по модулю $\gamma_{s+3}M_{k+2}$ алгоритмически неразрешима. Наоборот, по любому решению $\zeta_1 = \beta_1, \ldots, \zeta_k = \beta_k$ уравнения (4) определяется эндоморфизм μ со свойством (6), соответствующий отображению (7) для $\alpha_j = 0$ $(j = 1, \ldots, k)$. В свою очередь, в [10] (см. также [3]) показано, что проблема эндоморфной сводимости по модулю $\gamma_{s+3}M_{k+2}$ сводится к проблеме эндоморфной сводимости в группе M_r для некоторого $r = k+2+p_{k+2,s+3}$, откуда следует её неразрешимость в группе M_r' при любом $r' \geqslant r$. Объясним это более подробно.

Указанные выше построения возможны для произвольного диофантова уравнения $d(\zeta_1, \ldots, \zeta_k) = c$. Если построить элемент $g = g(d)$, где d — многочлен из левой части уравнения, то элемент $f = f(c)$ является эндоморфным образом элемента g тогда и только тогда, когда данное диофантово уравнение разрешимо в целых числах. Это называется *интерпретацией диофантовых уравнений* в свободных метабелевых группах. Легко видеть, что эндоморфная сводимость элемента g к элементу $f(c)$ в группе M_{k+2} по модулю $\gamma_{s+3}M_{k+2}$ записывается в форме группового уравнения вида

$$g(y_1, y_2, \ldots, y_{k+2}) = f(c) \pmod{\gamma_{s+3}M_{k+2}}, \tag{8}$$

где в левой части порождающие $x_1, x_2, \ldots, x_{k+2}$ заменены на соответствующие неизвестные $y_1, y_2, \ldots, y_{k+2}$. В правой части стоит произведение базисного коммутатора $[x_2, x_1, x_1, x_2]$ на степень c фиксированного базисного коммутатора $h = h(x_1, x_2)$ веса $s + 2$ из (5), то есть элемент фиксированного смежного класса по циклической подгруппе гр(h).

Известно [36], что любая вербальная подгруппа группы M_n, в частности любая подгруппа $\gamma_i M_n$, для произвольного n имеет конечную вербальную ширину. Это означает, что для любой пары натуральных чисел n, i существует слово $w_{n,i} = w_{n,i}(z_1, \ldots, z_{p_{n,i}})$, такое, что любой элемент подгруппы $\gamma_i M_n$ является значением этого слова. Точный вид слова $w_{n,i}$ указан, например, в [3]. Поэтому уравнение (8) разрешимо в группе M_{k+2} тогда и только тогда, когда в группе M_{k+2} разрешимо уравнение

$$g(y_1, y_2, \ldots, y_{k+2})w_{k+2,s+3}(z_1, \ldots, z_{p_{k+2,s+3}}) = f(c). \tag{9}$$

В свою очередь, алгоритмическая неразрешимость уравнений вида (9) означает неразрешимость проблемы эндоморфной сводимости в группе M_r, где $r = k + 2 + {} + p_{k+2,s+3}$. Очевидно, что проблема эндоморфной сводимости будет неразрешима и для любого большего чем r ранга.

3. Общая схема построения односторонних функций на основе неразрешимости проблемы эндоморфной сводимости

Пусть G — эффективно заданная группа, в которой разрешима проблема равенства и неразрешима проблема эндоморфной сводимости. Допустим, что нам необходимо построить на группе G одностороннюю функцию со значением также в G. Как правило, эффективно заданные группы конечно порождены. Поэтому предполагаем, что в G существует конечное порождающее множество $X_n = \{x_1, \ldots, x_n\}$. Произвольный элемент g группы G записывается как групповое слово $g = g(x_1, \ldots, x_n)$ от фиксированных порождающих элементов. Каждый эндоморфизм $\varphi : G \to G$ однозначно определяется своими значениями на элементах порождающего множества X_n. Если $\varphi(x_i) = h_i$ для $i = 1, \ldots, n$, то значением элемента $g = g(x_1, \ldots, x_n)$ будет элемент $\varphi(g) = g(h_1, \ldots, h_n)$. Однако не любое отображение $\varphi : X_n \to G$ продолжается до эндоморфизма в общем случае. Поэтому представляется перспективным выбирать в качестве группы G свободную группу конечного ранга некоторого многообразия групп $\mathcal{L}$. Тогда любое отображение $\varphi : X_n \to G$, где X_n — базис группы G (т. е. множество свободных порождающих группы G в многообразии $\mathcal{L}$), однозначно определяет эндоморфизм $\varphi : G \to G$. Для его задания достаточно определить образы базисных элементов, записав их в виде групповых слов от этих элементов. Ещё лучше, если в группе G есть нормальная форма записи элементов. Тогда эндоморфизм можно задать, записывая образы базисных элементов в этой нормальной форме. В работе [3] отмечено, что свободные метабелевы группы отвечают описанным требованиям.

Определим функцию $\varphi : G \to G$, сопоставляющую элементам группы, записанным в нормальной форме, нормальные формы их значений относительно эндоморфизма φ. Для эффективности соответствующих вычислений необходимо, чтобы в группе G существовал эффективный алгоритм записи элемента в нормальной форме по его представлению в виде группового слова от порождающих элементов или в каком-то другом виде, отвечающем эффективности задания группы G. Необходима также эффективная процедура вычисления нормальных форм обратного элемента и произведения элементов. Если группа G удовлетворяет этим требованиям, то получаем эффективно вычислимую функцию, определённую на множестве нормальных форм элементов группы G со значениями в этом же множестве. Если определить для элементов группы G некоторую функцию длины, например ввести на ней словарную метрику, то не существует полиномиального алгоритма, ограничивающего длину прообраза по длине образа для данной функции. Более того, никакая рекурсивная функция не даст такого ограничения. Не существует и других эффективных процедур, сводящих решение задачи поиска аргумента по значению функции к ограниченному полному перебору.

При этом, однако, возникает существенный вопрос об обращении функции на генерическом множестве значений. Возможно ли найти генерическое подмножество в множестве всех значений функции относительно естественной меры на этом множестве, на котором проблема поиска решается эффективно? Этот вопрос требует специального исследования в каждом конкретном случае (см. по этому поводу обзор [3] или более детальное изложение в [1, 2, 37]).

Рассмотрим элемент $g = g(x_1, x_2, \ldots, x_{k+2})$, построенный выше. Определим образ элемента g относительно эндоморфизма μ, фиксирующего x_1 и x_2 и отображающего x_j для $j = 3, \ldots, k+2$ в $x_j^{\beta_{j-2}}$ для некоторых целых чисел $\beta_1, \ldots, \beta_k$. В результате получим по модулю $\gamma_{s+3}M_{k+2}$ элемент $\mu(g) = f(x_1, x_2)^c$. Можно считать, что определена функция $\bar{g} : \mathbb{Z}^k \to \mathbb{Z}$ по правилу $(\beta_1, \ldots, \beta_k) \mapsto c$. Эту функцию можно рассматривать как возможно одностороннюю. Её полиномиальная вычислимость очевидна. В то же время из-за неразрешимости проблемы эндоморфной сводимости элемента g к элементу вида $f(x_1, x_2)^c$ не существует полиномиального по времени алгоритма, вычисляющего по c набор $(\beta_1, \ldots, \beta_k)$.

Отсюда можно вывести следующее общее заключение. Если бы длины значений $\varphi(x_i) = h_i$ для $i = 1, \ldots, n$, соответствующие эндоморфизму φ, переводящему g в $f = f(c)$, можно было оценить сверху полиномиальными функциями от c, то проблема эндоморфной сводимости g к f в группе M_{k+2} была бы разрешимой. Поскольку это не так, подобной оценки не существует. Это приводит к невозможности переборного решения проблемы.

Относительно возможной эффективной обратимости рассматриваемой функции на генерическом множестве значений заметим, что в работе А. Н. Рыбалова [38] доказано, что 10-я Проблема Гильберта остается алгоритмически неразрешимой на любом строго генерическом множестве диофантовых уравнений.

4. Протокол аутентификации

Впервые идея использования рассматриваемой схемы для построения протокола аутентификации на платформе группы с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости была высказана В. А. Романьковым в докладе на семинаре в Graduate Center City University of New York в 2007 г. Впоследствии идея была описана в работе Д. Григорьева и В. Шпильрайна [39]. Авторы опирались на результаты В. А. Романькова из [3, 10].

В общих чертах протокол выглядит следующим образом.

У с т а н о в к а. Выбирается бесконечная эффективно заданная группа G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости. Абонент **A** фиксирует публичный элемент g и секретный эндоморфизм φ, вычисляет и публикует образ $f = \varphi(g)$. Элементы g и f выбираются таким образом, чтобы проблема эндоморфной сводимости для пары (g, f) была трудна. Это означает, что по f трудно вычислить эндоморфизм φ, переводящий g в f.

А л г о р и т м а у т е н т и ф и к а ц и и.

1) В качестве сессионного ключа выбирается эндоморфизм (в работе [39] автоморфизм) ψ, вычисляется элемент $v = \psi(f)$ и передается в систему **C**, в которой осуществляется аутентификация пользователя **A**.
2) Система **C** с равной вероятностью выбирает случайный бит и отсылает его **A**.
3) Если **A** получает 0, то он просто публикует ψ, а **C** проверяет, что действительно v — образ f относительно ψ. Если **A** получает 1, то он вычисляет композицию $\chi = \varphi\psi$, передает её **C**, который проверяет справедливость равенства $v = \chi(g)$.

Схема выглядит как протокол аутентификации с нулевым разглашением, аналогичный известному протоколу Фиата — Шамира (см., например, [25, 26]). Однако для её криптостойкости необходимо выполнение ряда дополнительных условий. Во-первых, необходимо, чтобы существовал фигурирующий в протоколе элемент g, проблема вхождения в множество эндоморфных образов которого алгоритмически неразрешима. Как объяснялось выше, это возможно, если в качестве группы G выбрать свободную метабелеву группу M_n достаточно большого ранга n. В этом случае элемент f можно брать случайным образом из фиксированного смежного класса по циклической подгруппе $\mathrm{гр}(h)$, полагая $f = f(c)$ в соответствии с (4). Но далее аналогичные условия должны быть выполнены для пары элементов f, v. Результаты работы [10] уже не позволяют считать, что проблема вхождения в множество эндоморфных образов элемента f алгоритмически неразрешима. Но даже если бы это было так, приведённых условий все равно оказалось бы недостаточно.

Для разрешения этой ситуации можно ввести определение группы с неразрешимой двукратной проблемой эндоморфной сводимости, а именно можно доказать, что в свободной метабелевой группе M_n достаточно большого ранга можно выбрать элемент g, элемент b, циклическую подгруппу $\mathrm{гр}(h)$, элемент u и конечно порождённую абелеву группу A таким образом, что для любой пары элементов (g, f), где $f \in b\mathrm{гр}(h)$, и любой пары элементов (f, v), где $v \in uA$, одновременно алгоритмически неразрешимы проблемы эндоморфной сводимости. Более того, знание эндоморфизма χ, такого, что $\chi(g) = v$, не позволяет эффективно находить ни эндоморфизм φ, такой, что $\varphi(g) = f$, ни эндоморфизм ψ, такой, что $\psi(f) = v$. Наоборот, знание эндоморфизма ψ, такого, что $\psi(f) = v$, не позволяет восстановить ни φ, ни χ. Легко видеть, что эти условия являются необходимыми в обеспечении криптостойкости приведённого алгоритма.

Соответствующие построения проводятся эффективно. Они также основываются на неразрешимости 10-й Проблемы Гильберта и интерпретации диофантовых уравнений в свободных метабелевых группах.

Заметим также, что близкой по теме проблеме построения двукратной возможно односторонней функции посвящена работа первого автора [40]. Отсюда видно, что создание криптографических приложений, основанных на проблемах теории групп, имеет обратное влияние на развитие самой теории групп. Постановка алгоритмических проблем приобретает новые формы. Отметим в этой связи возросший интерес

к проблемам поиска. Вопросы теории сложности становятся все более актуальными и также приобретают новые формы. Достаточно ещё раз упомянуть понятие генерической сложности проблемы, возникшее главным образом при исследовании практических алгоритмов.

ЛИТЕРАТУРА

1. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-based cryptography. (Advances courses in Math., CRM, Barselona). Basel, Berlin, New York: Birkhäuser Verlag, 2008. 183 p.
2. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative cryptography and complexity of group-theoretic problems. (Amer. Math. Soc. Surveys and Monographs). Providence, RI: Amer. Math. Soc., 2011. 385 p.
3. *Романьков В. А.* Диофантова криптография на бесконечных группах // Прикладная дискретная математика. 2012. № 2. С. 15–42.
4. *Goldreich O.* Foundations of cryptography. Cambridge: Cambridge Univ. Press, 2001. V. 1. 451 p.; 2004. V. 2. 798 p.
5. *Goldwasser S. and Bellare M.* Lecture Notes on Cryptography. Cambridge: MIT, 2008.
6. *Sipser M.* Introduction to the theory of computation. PWS Publishing, 1997. 416 p.
7. *Levin L. A.* One-way Functions and Pseudorandom Generators // Combinatorica. 1987. V. 7. No. 4. P. 357–363.
8. *Левин Л. А.* Односторонние функции // Проблемы передачи информации. 2003. Т. 39. № 1. С. 103–117.
9. *Кожевников А. А., Николенко С. И.* О полных односторонних функциях // Проблемы передачи информации. 2009. Т. 45. № 2. С. 101–118.
10. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сибирский математический журнал. 1979. Т. 20. № 3. С. 671–673.
11. *Романьков В. А.* О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С. 457–471.
12. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Докл. АН СССР. 1970. Т. 191. № 2. С. 279–282.
13. *Матиясевич Ю. В.* Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. матем. 1971. № 35. С. 3–30.
14. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Наука, 1993. 223 с.
15. *Shpilrain V. and Zapata G.* Using decision problems in public key cryptography // Groups. Complexity. Cryptology. 2009. V. 1. P. 33–40.
16. *Shpilrain V. and Zapata G.* Using the subgroup membership problem in public key cryptography // Contemp. Math. V. 418. Providence, RI: Amer. Math. Soc., 2006. P. 169–179.
17. *Shpilrain V. and Zapata G.* Combinatorial group theory and public key cryptography // Applicab. Alg. Eng. Comm. Comp. 2006. V. 17. P. 291–302.
18. *Kurt Y.* A new key exchange primitive based on the triple decomposition problem // Preprint: `http://eprint.iacr.org/2006/378`
19. *Birget J.-C., Magliveras S., and Sramka M.* On public-key cryptosystems based on combinatorial group theory // Tatra Mount. Math. Publ. 2006. V. 33. P. 137–148.
20. *Lohrey M.* Word problems on compressed words // Automata, Languages and Programming. LNCS. 2004. V. 3142. P. 906–918.
21. *Lohrey M. and Schleimer S.* Efficient computation in groups via compression // LNCS. 2007. V. 4649. P. 249–258.

22. *Scheimer S.* Polynomial-time word problems // Comment. Math. Helv. 2008. V. 83. No. 4. P. 741–765.
23. *Ерофеев С. Ю.* Диофантовость дискретного логарифма // Прикладная дискретная математика. Приложение. 2011. № 4. С. 31–32.
24. *Ерофеев С. Ю.* Диофантовость дискретного логарифма // Вестник Омского университета. 2010. № 4. С. 13–15.
25. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.
26. *Романьков В. А.* Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.
27. *Matijasevich Y. V. and Robinson J.* Reduction of an arbitrary diophantine equation to one in 13 unknowns // Acta Arithmetica. 1975. V. 27. P. 521–553.
28. *Matijasevich Y. V.* Some purely mathematical results inspired by mathematical logic // Proc. Fifth Intern. Congr. Logic, Methodology and Philos. of Sci.(London, Ont.). Dordrecht, Reidel, Holland. 1977. P. 121–127.
29. *Jones J.* Universal diophantine equation // J. Symbolic Logic. 1982. V. 47. No. 3. P. 549–571.
30. *Нейман Х.* Многообразия групп. М.: Мир, 1974. 264 с.
31. *Маканин Г. С.* Уравнения в свободной группе // Изв. АН СССР. Сер. матем. 1982. Т. 46. № 6. С. 1199–1273.
32. *Hall P.* Nilpotent groups // Canad. Math. Cong. Summer Sem. Vankuver: University of Alberta, 1957. P. 12–30.
33. *Холл М.* Теория групп. М.: ИЛ, 1962. 467 с.
34. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Лань, 2009. 288 с.
35. *Курош А. Г.* Теория групп. М.: Физматгиз, 2008. 808 с.
36. *Segal D.* Words: notes on verbal width in groups // London Math. Soc. Lect. Notes. Cambridge: Cambridge Univ. Press, 2009. V. 361. 215 p.
37. *Kapovich I., Myasnikov A., Shupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. P. 665–694.
38. *Рыбалов А. Н.* О генерической неразрешимости десятой проблемы Гильберта // Вестник Омского университета. 2011. № 4. С. 19–22.
39. *Grigoriev D. and Shpilrain V.* Zero-knowledge autentification schemes from actions on graphs, groups and rings // Ann. Pure Appl. Logic. 2010. V. 162. P. 194–200.
40. *Ерофеев С. Ю.* Схемы построения двушагово односторонних функций // Вестник Омского университета. 2011. № 4. С. 15–18.