МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.62

ДИОФАНТОВА КРИПТОГРАФИЯ НА БЕСКОНЕЧНЫХ ГРУППАХ

В. А. Романьков

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

E-mail: romankov48@mail.ru

В работе даётся краткое представление криптографии, основанной на группах («group-based cryptography»), — современного направления, главными объектами в котором являются абстрактные бесконечные группы, а основной целью — построение на них криптографических примитивов, систем и протоколов. Исследования по этому направлению ведутся методами теории групп, теории сложности и теории вычислений. Обращается внимание на использование неразрешимых и трудноразрешимых алгоритмических проблем теории групп в качестве основы обозначенного построения. Обсуждаются аспекты сложности алгоритмических проблем и связанных с ними проблем поиска. Объясняется универсальность диофантова языка в криптографии. Отмечается его объединяющая роль.

В качестве возможных платформ для криптографических систем и протоколов предлагается использовать свободные метабелевы группы. Приводятся основания для такого использования, в том числе алгоритмическая разрешимость в этих группах проблемы равенства и наличие нормальных форм записи элементов группы. Ещё одним основанием является алгоритмическая неразрешимость в таких группах проблемы существования решений у групповых уравнений и алгоритмическая неразрешимость проблемы эндоморфной сводимости, вытекающих из неразрешимости 10-й Проблемы Гильберта. Предполагается, что в последующей работе автора совместно с С. Ю. Ерофеевым материал данной работы будет использован для построения на свободных метабелевых группах возможно односторонних функций и протоколов аутентификации с нулевым разглашением.

Ключевые слова: *криптография, основанная на группах, алгоритмическая проблема, проблема поиска, генерическая сложность, диофантов язык, диофантова криптография, свободная метабелева группа, проблема эндоморфной сводимости.*

Введение

Понятие «криптография, основанная на группах» (англ. вариант — *group-based cryptography*) появилось сравнительно недавно — на рубеже XX и XXI столетий. Так обозначено направление исследований, основными объектами которого являются абстрактные бесконечные группы, а основной целью — построение на них криптографических систем и протоколов. Исследования ведутся методами теории групп, теории сложности и теории вычислений.

Данному направлению посвящены монографии [1, 2], а также множество статей, затрагивающих самые разные вопросы. Часть из этих работ представляет криптографические примитивы, другая описывает криптографические системы и протоколы,

третья исследует вопросы сложности и т. д. Некоторые работы посвящена вскрытию слабостей представленных систем и протоколов. Имеются и практические разработки, в том числе компьютерные программы, для использования полученных результатов на практике. Обширный список работ по данному направлению можно найти в [3].

В настоящей работе даётся краткое представление о криптографии, основанной на группах, обсуждается использование неразрешимых и трудноразрешимых алгоритмических проблем теории групп в качестве основы для построения криптографических систем и протоколов. Для обоснования возможности такого использования мы обращаем внимание на следующие аспекты:

— Как должна быть задана и какими свойствами должна обладать группа, претендующая на роль платформы для построения криптографических систем и протоколов?
— Какой должна быть алгоритмическая проблема, претендующая на роль основы для построения криптографических систем и протоколов?
— Каковы общие принципы обозначенных построений и чем должна обуславливаться их криптостойкость?

Подобные вопросы уже неоднократно рассматривались в литературе. После того как вышла пионерская в данном направлении работа М. Аншеля и др. [4], в которой представлена схема генерации общего ключа, известная теперь как *протокол Аншель — Аншеля — Голдфельда*, появилось множество работ, эксплуатирующих те или иные алгоритмические проблемы для построения систем и протоколов. В [4] в качестве платформы берётся группа кос Артина B_n на n нитях для достаточно большого n. В качестве алгоритмической в ней рассматривается проблема сопряжённости в группе B_n двух наборов элементов $\bar{g} = (g_1, \ldots, g_k)$ и $\bar{f} = (f_1, \ldots, f_k)$. Алгоритм может быть представлен в любой группе. Конкретный её выбор обуславливается многими факторами. Во-первых, группа, выбранная в качестве платформы, должна быть удобной для реализации алгоритма. В то же время необходимо обеспечить криптостойкость алгоритма. Об этом более подробно говорится в дальнейшем. Опишем сам алгоритм в общем виде.

Пусть G — конечно порождённая группа с множеством порождающих элементов $\{x_1, \ldots, x_n\}$, которое можно считать фиксированным. Любой элемент группы G записывается в виде группового слова от порождающих элементов. *Групповым* называется слово, записанное от букв $x_1, \ldots, x_n$ и формальных обратных $x_1^{-1}, \ldots, x_n^{-1}$. Конечно, такая запись элемента неоднозначна. Во-первых, возможны сокращения подслов вида $x_i^{\varepsilon} x_i^{-\varepsilon}$ для $\varepsilon = \pm 1$. Если таких подслов нет, то слово называется *редуцированным* или *несократимым*. Если $G = F_n$ — свободная группа с базисом $\{x_1, \ldots, x_n\}$, то запись элемента в виде несократимого слова однозначна. В группе, не являющейся свободной, существуют нетривиальные слова, записывающие наравне с пустым словом тривиальный элемент. Они называются *соотношениями* группы.

Предположим, что в группе G существует нормальная форма записи её элементов. Это означает, что любой элемент может быть однозначно записан в виде канонического слова от порождающих элементов. Переход от произвольной записи элемента $g = g(x_1, \ldots, x_n)$ к его записи в нормальной форме нф(g) предполагается эффективным. Обычно он осуществляется через переписывающий процесс, получающий на входе произвольное слово от порождающих элементов и выдающий на выходе запись соответствующего элемента в нормальной форме. В свободной группе с базисом $\{x_1, \ldots, x_n\}$ это обычный процесс сокращения подслов вида $x_i^{\varepsilon} x_i^{-\varepsilon}$, о которых гово-

рилось выше. Известно, что результат — несократимое слово — не зависит от выбора порядка сокращения.

В протоколе Аншель — Аншеля — Голдфельда корреспонденты **A** и **B**, часто именуемые как Алиса и Боб, выбирают наборы элементов $\bar{g} = (g_1, \ldots, g_k)$ и $\bar{f} = (f_1, \ldots, f_k)$ группы G, причём **A** выбирает набор $\bar{g}$, а **B** — набор $\bar{f}$. Эти наборы считаются известными (*public*). Затем **A** выбирает секретное (*private*) слово $u = u(f_1, \ldots, f_k)$, а **B** — секретное слово $v = v(g_1, \ldots, g_k)$. Они могут это сделать, так как наборы известны. Далее **A** выполняет сопряжение набора $\bar{f}$ элементом u, получая набор $\bar{f}^u = (f_1^u, \ldots, f_k^u)$. Запись вида a^b означает сопряжение bab^{-1} элемента a элементом b. В дальнейшем через $[a, b]$ обозначается *коммутатор* $= aba^{-1}b^{-1}$ элементов a и b. Корреспондент **A** вычисляет и публикует нормальную форму $\text{нф}(\bar{f}^u) = (\text{нф}(f_1^u), \ldots, \text{нф}(f_k^u))$. Подобным образом корреспондент **B** вычисляет и публикует набор $\text{нф}(\bar{g}^v) = (\text{нф}(g_1^v), \ldots, \text{нф}(g_k^v))$.

Предполагается, что в группе G вычисление по опубликованным нормальным формам сопряжённых наборов элементов u и v — трудная задача. На этом основывается криптостойкость протокола. После выхода [4] появилось множество работ с анализом этой криптостойкости, где подчёркивается важность выбора параметров, ключей и т. п. Появились соответствующие рекомендации и т. п.

На выходе протокола корреспонденты получают секретный ключ. Делается это следующим образом. Корреспондент **A** вычисляет элемент

$$u\,(\text{нф}(g_1^v), \ldots, \text{нф}(g_k^v))\;u^{-1} = [v, u].$$

Корреспондент **B** вычисляет тот же самый элемент $[v, u]$ из равенства

$$v \cdot v(\text{нф}(f_1^u), \ldots, \text{нф}(f_k^u))^{-1} = [v, u].$$

Таким образом пользователи **A** и **B** генерируют общий известный только им ключ $K = \text{нф}[v, u]$.

Мы здесь не приводим и не обсуждаем конкретные свойства групп кос Артина B_n, выбранных авторами [4] в качестве платформы своего протокола. Относительно этих свойств см. классическую работу А. А. Маркова [5], монографию П. Дехорноя [6], обзор В. Я. Лина [7] или ещё какую-нибудь монографию, посвящённую группам кос Артина.

О криптографии на группах кос Артина, включая подробное описание протокола Аншель — Аншеля — Голдфельда, см. обзоры П. Дехорноя [8] и К. Мальбурга [9].

Нам важно выделить некоторые основные, с нашей точки зрения, свойства группы кос Артина, позволяющие рассматривать приведённые построения как заслуживающие внимания. Эти свойства следующие:

— Группы B_n при любом n являются конечно определёнными, то есть порождаются конечными множествами порождающих элементов, все соотношения между которыми следуют из конечного множества определяющих соотношений.
— Группы B_n обладают нормальными формами однозначной записи элементов, переход к которым от записей в виде групповых слов эффективен.
— В группах кос нахождение сопрягающего элемента u по элементу g и нормальной форме $\text{нф}(g^u)$ сопряжённого к нему элемента является трудноразрешимой задачей. Более того, она остаётся трудноразрешимой при замене одного элемента на набор элементов.

Отмеченные свойства так или иначе присутствуют в большинстве работ. Хочется ещё заметить, что в работе [4] фактически впервые существенно использовалась

некоммутативность группы. Более того, представленный протокол не являлся переносом известных протоколов теоретико-числового характера. Подобные переносы, например, в матричные группы уже были известны, но не дали толчка для последующего развития.

В последующей работе автора совместно с С. Ю. Ерофеевым «О построении возможно односторонних функций на основе алгоритмической неразрешимости проблемы эндоморфной сводимости в свободных метабелевых группах» мы перейдём к конкретным предложениям. В качестве платформы для построения криптографических примитивов, систем и протоколов выбираем свободные метабелевы группы. Свободная метабелева группа M_n ранга n, где n — натуральное число, определяется как факторгруппа F_n/F_n'' свободной группы F_n ранга n по второму коммутанту F_n''. Напомним, что коммутантом G' произвольной группы G называется её подгруппа, порождённая всеми коммутаторами $[g, f]$ элементов группы G. Подгруппа G' нормальна в группе G, фактор-группа G/G' по ней абелева. Второй коммутант G'' определяется как коммутант от коммутанта $(G')'$. Он также нормален в группе G. Группа G называется *метабелевой*, если G'' тривиален. В этом случае коммутант G' абелев, а группа G является расширением абелевой нормальной подгруппы G' с помощью абелевой факторгруппы G/G'. Отсюда её название.

Группа M_n называется *свободной метабелевой группой ранга* n, потому что в ней есть *базис* $X_n = \{x_1, \ldots, x_n\}$, состоящий из n элементов, такой, что любое отображение этого базиса $X_n \to G$ в произвольную метабелеву группу G однозначно продолжается до гомоморфизма $M_n \to G$. Говорят также, что группа M_n — *свободная группа ранга* n *многообразия всех метабелевых групп* $\mathcal{A}^2$. Базис X_n называют *множеством свободных порождающих* группы M_n. О многообразиях групп см. монографию Х. Нейман [10].

В качестве алгоритмической проблемы возьмём проблему $E(M_n)$ эндоморфной сводимости в группе M_n. Известно [11, 12], что она алгоритмически неразрешима при достаточно большом $n \geqslant n_0$. Основываясь на её алгоритмической неразрешимости, укажем метод построения функции $f_n : M_n \to M_n$, претендующей на роль односторонней функции. Наконец, используя платформу M_n и функцию f_n, предложим протокол аутентификации с нулевым разглашением пользователя в системе. Подобный протокол уже предлагался в [13], причём также со ссылкой на работу автора [12]. Однако так просто воспользоваться группами и функциями из [12] в данном случае нельзя. Мы покажем, что для криптостойкости протокола аутентификации необходима алгоритмическая неразрешимость более сильной проблемы *двукратной эндоморфной сводимости*.

Важно отметить, что алгоритмическая неразрешимость проблемы эндоморфной сводимости $E(M_n)$ при $n \geqslant n_0$, установленная в [12], базируется на алгоритмической неразрешимости 10-й Проблемы Гильберта о существовании алгоритма, определяющего по произвольному уравнению вида $d(\zeta_1, \ldots, \zeta_k) = 0$, где $d(\zeta_1, \ldots, \zeta_k)$ — многочлен с целыми коэффициентами, имеет ли это уравнение решение в целых числах. Алгоритмическая неразрешимость 10-й Проблемы Гильберта установлена Ю. В. Матиясевичем в [14] (полное доказательство в [15], см. также [16]).

В данной работе мы показываем, что диофантов язык является достаточно универсальным. На нем записываются функции и уравнения, фигурирующие во многих криптографических системах и протоколах, в том числе в системе RSA и протоколах, основанных на понятии дискретного логарифма в мультипликативных группах конеч-

ных полей. Диофантов язык позволяет объединять эти системы и протоколы в единое целое, что даёт возможность ввести в рассмотрение *диофантову криптографию*.

В заключение отметим, что построение криптографических систем и протоколов, основанных на неразрешимых и трудноразрешимых проблемах, осуществлялось многими авторами (см., например, монографии [1, 2], обзор [8], статьи [17 – 21]).

1. Бесконечные группы и алгоритмические проблемы

Рассмотрим постановку алгоритмических проблем только для групп, хотя аналоги этих проблем легко формулируются и для других алгебраических и не только алгебраических систем. Заметим, что истоки этих проблем лежат в топологии.

1.1. Постановка алгоритмических проблем

В самых общих чертах алгоритмическая проблема выглядит следующим образом. Имеется теоретико-групповое свойство $\mathbf{P}$, которое может относиться как к отдельным элементам, так и к наборам элементов, к подгруппам или подмножествам группы, к различным группам и т. п. Требуется определить, обладают ли свойством $\mathbf{P}$ указанные объекты. Более точно проблема формулируется как следующий вопрос: *существует ли алгоритм, определяющий за конечное число шагов, удовлетворяет объект $\mathcal{O}$ свойству $\mathbf{P}$ или нет*?

При постановке проблемы упоминание алгоритма часто опускается. Говорят, что проблема *алгоритмически разрешима* (или просто *разрешима*), если такой алгоритм существует, и *неразрешима* в противном случае.

При постановке алгоритмической проблемы предполагается, что группа, её элементы, подгруппы, подмножества, словом, объекты, для которых ставится проблема, заданы каким-либо эффективным образом. Способов эффективного задания существует довольно много. Далее опишем некоторые из них.

Классические алгоритмические проблемы теории групп сформулированы в начале XX столетия Максом Деном. Они ставились для класса конечно определённых групп. Это означает, что группа G, для которой ставится проблема, задана своим *конечным представлением* вида

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

Иначе говоря, группа G является фактор-группой F_n/R свободной группы F_n с базисом (множеством свободных порождающих элементов) $\{x_1, \ldots, x_n\}$ относительно *нормального замыкания* $R = \text{нз}(r_1, \ldots, r_m)$, то есть минимальной нормальной подгруппы группы F_n, содержащей элементы $r_1, \ldots, r_m$. Элементы $r_1, \ldots, r_m$ записываются в виде групповых слов от порождающих $x_1, \ldots, x_n$. Напомним, что групповое слово записывается как слово от элементов $x_1^{\pm 1}, \ldots, x_n^{\pm 1}$. Элементы $r_1, \ldots, r_m$ называются *определяющими словами*. Иногда представление (1) записывают в виде

$$\mathcal{P}(G) = \langle x_1, \ldots, x_n \mid r_1 = 1, \ldots, r_m = 1 \rangle. \tag{2}$$

Смысл задания остается тем же самым, равенства $r_i = 1$ для $i = 1, \ldots, m$ называют *определяющими соотношениями* группы G.

Через H' обозначим *коммутант* группы H, то есть подгруппу, порождённую в группе H всеми коммутаторами её элементов. Коммутант H' является нормальной подгруппой группы H, фактор-группа H/H' по которой абелева. Более того, коммутант — наименьшая подгруппа с этим свойством, то есть если фактор-группа H/N по какой-либо нормальной подгруппе N группы H абелева, то N обязательно содержит H'.

Элементы нормального замыкания $R = \text{нз}(r_1, \ldots, r_m)$ допускают описание как групповые слова следующего вида:

$$u = \prod_{j=1}^{k} (r_{i_j}^{g_j})^{\varepsilon_j}, \tag{3}$$

где $i_j \in \{1, \ldots, m\}$; $g_j \in F_n$; $\varepsilon_j = \pm 1$ для $j = 1, \ldots, k$.

Естественно определяется *канонический гомоморфизм* $F_n \to G$, переводящий произвольный элемент g группы F_n в элемент gR группы G. Группа G имеет каноническое множество порождающих элементов $y_i = x_i R$ для $i = 1, \ldots, n$. Любой элемент g группы G можно поэтому записать в виде группового слова $g = g(y_1, \ldots, y_n)$. Однако часто порождающие y_i группы G обозначают теми же буквами x_i, что и их прообразы. Элемент g записывается в виде $g(x_1, \ldots, x_n)$.

Классические алгоритмические проблемы Дена формулируются следующим образом.

1. **Проблема равенства.** Определить по двум групповым словам $g = g(x_1, \ldots, x_n)$ и $f = f(x_1, \ldots, x_n)$, записывают ли они один и тот же элемент группы G, заданной своим конечным представлением (1) или (2). Другими словами, верно ли, что в группе G справедливо равенство $g = f$. Иногда, чтобы указать группу, пишут $g =_G f$.

Рассмотрение проблемы равенства может быть сведено к случаю, когда один из элементов равен 1. Действительно, равенство $g =_G f$ выполнено тогда и только тогда, когда $gf^{-1} =_G 1$. Оно может быть также перенесено в группу F_n, поскольку равенство $g =_G 1$ равносильно тому, что слово $g = g(x_1, \ldots, x_n)$ как элемент группы F_n принадлежит нормальной подгруппе R.

Первые примеры конечно определённых групп с неразрешимой проблемой равенства были построены в 50-е годы XX столетия П. С. Новиковым в [22, 23]. Впоследствии таких примеров стало достаточно много.

2. **Проблема сопряжённости.** Определить, задают ли два слова $g = g(x_1, \ldots, x_n)$ и $f = f(x_1, \ldots, x_n)$ сопряжённые элементы группы G. Другими словами, существует ли элемент h группы G, такой, что $g^h =_G f$.

Разрешимость проблемы сопряжённости в группе G, очевидно, влечет разрешимость в G проблемы равенства. Действительно, элемент g группы G равен 1 тогда и только тогда, когда g сопряжён с 1. Обратное утверждение в общем случае неверно. Существуют конечно определённые группы, в которых проблема равенства разрешима, а проблема сопряжённости неразрешима. Первые примеры групп с неразрешимой проблемой сопряжённости, некоторые из которых имеют разрешимую проблему равенства, построены в [23].

3. **Проблема изоморфизма.** Определить по двум представлениям конечно определённых групп G и H, изоморфны эти группы или нет.

Неразрешимость проблемы изоморфизма в классе конечно определённых групп установлена С. И. Адяном [24].

Отметим ещё одну проблему, которая хотя и не была явно сформулирована Деном, но впоследствии стала одной из основных.

4. **Проблема вхождения.** Определить для произвольного элемента g данной конечно определённой группы G и произвольной её конечно порождённой подгруппы H, принадлежит g подгруппе H или нет.

Проблему вхождения часто называют *обобщённой проблемой равенства*. Очевидно, что её разрешимость влечет разрешимость проблемы равенства, равносильной про-

блеме вхождения в тривиальную подгруппу. Выделяют также проблему вхождения в фиксированную конечно порождённую подгруппу.

Известные результаты и открытые проблемы алгоритмического характера в теории групп освещены в обзорах [25 – 27].

В некоторых важных классах групп классические алгоритмические проблемы разрешимы. Например, все они разрешимы в классах свободных и конечно порождённых абелевых групп. Многие проблемы разрешимы в классах нильпотентных и полициклических групп. Имеются важные результаты о разрешимости алгоритмических проблем в матричных группах. Большое внимание уделено разработке практических алгоритмов решения алгоритмических проблем в группах (см. по этому поводу монографии [28, 29] и обзорную статью [30]).

Таким образом, первоначально при постановке алгоритмических проблем рассматривались только конечно определённые группы, элементы которых записываются в виде групповых слов. Впоследствии класс групп, для которых ставятся алгоритмические проблемы, был расширен как за счёт включения в него *рекурсивно определённых* групп, в которых множество порождающих элементов конечно, а множество определяющих соотношений может быть бесконечным рекурсивно перечислимым множеством, так и за счёт конечно порождённых подгрупп каких-нибудь известных хорошо заданных групп. Например, группа может быть задана своим конечным порождающим множеством в матричной группе над конструктивным полем или более общо — над кольцом. Группа может также быть задана как конструктивный объект в смысле теории моделей. Она может определяться и другими эффективными способами.

Класс конечно порождённых матричных групп над конструктивными кольцами представляет особый интерес. Проблема равенства в таких группах, очевидно, разрешима. Однако другие проблемы даже в достаточно просто устроенных матричных группах могут быть неразрешимыми.

Одним из самых известных является пример К. А. Михайловой матричной группы с неразрешимой проблемой вхождения, описанный в работе [31]. Эта группа есть прямое произведение $G = F_2 \times F_2$ двух копий свободной группы ранга 2. Она допускает точное представление матрицами порядка 4 над кольцом целых чисел $\mathbb{Z}$. Опишем одно из возможных таких представлений. Хорошо известно (см., например, [32, 33]), что представление (оно называется *представлением Санова*) группы F_2 матрицами порядка 2 над $\mathbb{Z}$, заданное на порождающих элементах x_1, x_2 группы F_2 следующим отображением, точное:

$$x_1 \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad x_2 \mapsto \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Точное представление группы G матрицами 4-го порядка соответствует схеме

$$\begin{pmatrix} F_2 & 0 \\ 0 & F_2 \end{pmatrix},$$

согласно которой первая копия группы F_2 представляется верхней левой клеткой, а вторая — нижней правой (остальные матричные элементы в представлении множителей группы G, как у единичной матрицы).

Неразрешимость проблемы вхождения в группе G основывается на существовании 2-порождённой конечно определённой группы с неразрешимой проблемой равенства. Пусть такая группа K задана представлением $\mathcal{P}(K) = \langle x_1, x_2 \mid r_1, \ldots, r_m \rangle$. Рассмотрим

в группе G подгруппу H, порождённую элементами вида $f_1 = (x_1, x_1)$, $f_2 = (x_2, x_2)$, $h_i = (r_i, 1)$ для $i = 1, \ldots, m$. Легко показать, что элемент $g = (g', 1)$ принадлежит H тогда и только тогда, когда g' принадлежит нормальной подгруппе $R = \text{нз}(r_1, \ldots, r_m)$ группы F_2. Неразрешимость проблемы равенства в группе $K = F_2/R$ влечет неразрешимость проблемы вхождения в подгруппу H группы G.

2. Неразрешимые и трудноразрешимые алгоритмические проблемы как основа для построения криптографических систем и протоколов

Классические алгоритмические проблемы Дена уже неоднократно предлагались в качестве основы для построения на группах криптографических примитивов, систем и протоколов. Традиционно наибольшее внимание привлекает в этой связи проблема сопряжённости. В уже упоминавшейся работе М. Аншеля и др. [4] основой криптостойкости протокола служит трудноразрешимость проблемы сопряжённости в группах кос Артина. Заметим, что проблема сопряжённости в них разрешима. Это установлено в работе Гарсайда [34]. Тем не менее, так как эффективный алгоритм для её решения до сих пор не найден, эта задача продолжает считаться трудноразрешимой (см. публикации [19, 35, 36]). Проблема равенства фигурирует в работах [37 – 39]; проблема вхождения — в работе [18]. Этот список — только малая часть работ, обсуждающих использование алгоритмических проблем в криптографии.

2.1. Проблемы поиска

Абсолютное большинство работ в криптографии, основанной на группах, в которых рассматриваются трудноразрешимые и неразрешимые проблемы, связано с решением так называемых *проблем поиска* (англ. вариант — *search problems*). Например, если в основе криптографического примитива лежит проблема сопряжённости, то обычно, как это происходит, например, в протоколе Аншель — Аншеля— Голдфельда, известно, что данные элементы или наборы элементов, если речь идёт о наборах, сопряжены. Задача заключается в эффективном нахождении сопрягающего элемента. В общих чертах, если алгоритмическая проблема ставится для объекта $\mathcal{O}$ относительно свойства $\mathbf{P}$, то проблема поиска выясняет в случае, если $\mathcal{O}$ обладает свойством $\mathbf{P}$, доказательство, или ещё говорят — *свидетельство* этого, справедливость которого легко проверить. Например, если известно, что элемент f группы G принадлежит подгруппе H, порождённой элементами $h_1, \ldots, h_k$, то требуется найти запись f в виде группового слова от этих элементов. Для проблемы равенства, аналогично, требуется найти выражение слова $u = u(x_1, \ldots, x_n)$ от порождающих элементов $x_1, \ldots, x_n$ свободной группы F_n, записывающего тривиальный элемент группы $G = F_n/R$, где $R = \text{нз}(r_1, \ldots, r_m)$ — его выражение в виде (3). Это, конечно, можно сделать простым перебором, но сейчас речь идёт о реальных вычислениях, когда такой перебор уже не может рассматриваться как эффективный.

Если алгоритмическая проблема, взятая за основу криптографического примитива, не допускает полиномиального алгоритма, то не существует также полиномиального ограничения длины входа от длины наблюдаемого выхода, значит, нельзя организовать полиномиальный перебор возможных входов, основываясь на такой оценке. Если же основная алгоритмическая проблема неразрешима, то невозможно вообще дать какую-либо оценку длины входа, зная длину выхода. В этом случае неприменим метод «грубой силы», то есть полного перебора.

Это рассуждение носит, конечно, самый общий характер. В теории сложности подобные вопросы получают строгое обоснование. Этому в основном посвящена монография [2].

3. О сложности алгоритмических проблем и соответствующих им проблем поиска

Современная теория сложности зародилась в 70-е годы XX столетия. Для нас важное значение имеет прежде всего понятие временной сложности. Действительно, криптография, основанная на группах, как, впрочем, и всякая другая область, ориентированная на практическое использование, должна заботиться о реальном времени вычислений в разрабатываемых ею протоколах. Значит, нам небезразлично, сколь долго будет работать алгоритм. В то же время при практическом использовании разрабатываемых протоколов различные входящие в них параметры, в том числе ключи, выбираются случайным образом. Значит, необходимо заботиться не только о сложности в худшем случае, когда проблему нельзя эффективно решить при каких-то специфических данных, но и о сложности, проявляющейся при случайном выборе данных. Здесь разрабатываются два основных подхода, связанные с определением понятий *сложности в среднем* и *генерической сложности*. Перейдём к общему схематическому описанию, отсылая за деталями к монографиям [1, 2, 40], сборнику [41] и статьям [42 – 45].

Итак, рассматриваем три основных вида сложности:

— сложность по худшему случаю;
— сложность в среднем;
— генерическую сложность.

О классическом понятии сложности по худшему случаю см., например, монографию [40]. Класс сложности $\mathcal{C}$ определяется спецификацией модели вычислений (для нас это многоленточная машина Тьюринга), типом вычислений (то есть использованием либо детерминированной, либо вероятностной машины Тьюринга), а также ресурсами, объём которых необходимо контролировать (обычно это время работы алгоритма, пространство, занимаемое данными, или же то и другое). Данные спецификации позволяют определить функцию сложности $f(n)$, где n — размер входа, оценивающую объём необходимых ресурсов для вычисления соответствующего ему выхода. Мы не приводим точного определения, замечая только, что оно позволяет говорить о линейной, полиномиальной или экспоненциальной сложности алгоритма. Как правило, считается, что линейные, квадратичные и в иных случаях полиномиальные для малых степеней алгоритмы достаточно быстры, а экспоненциальные медленны. Конечно, это все относительно и требует конкретизации в каждом отдельном случае.

Кратко остановимся на понятии *сложности в среднем*. Для её определения необходимо, чтобы на пространстве всех возможных входов была задана функция распределения вероятностей или хотя бы какая-нибудь аддитивная неотрицательная функция. При её задании сложность в среднем чаще всего оценивается математическим ожиданием объёма ресурсов, необходимым для работы алгоритма на случайно выбранном входе. Опять же можно говорить о линейной, полиномиальной и экспоненциальной сложности в среднем. На конечных множествах, как правило, задают равномерную функцию распределения. В бесконечном случае вопрос о задании такой функции становится более тонким. Например, задача определения «случайного» элемента группы рассматривалась многократно. Даже для конечных групп этот вопрос решается далеко не очевидным путём. Действительно, что считать случайным выбором? Уже давно стало понятным, что при учёте алгебраической структуры группы её элементы как бы становятся «неравноправными» (см. по этому поводу [46]).

В работе [47] предложен следующий возможный общий подход к построению обсуждаемого распределения на бесконечной конечно порождённой группе. Пусть груп-

па G наделена функцией натуральнозначной длины $l : G \to \mathbb{N}$, такой, что множество $\mathbb{S}_r$ всех элементов g группы G длины $l(g) = r$ для любого натурального числа r конечно. Считаем также, что $\mathbb{S}_0 = \{1\}$. Функция l в конкретных случаях может называться функцией размера, сложности и т. п. Множество $\mathbb{S}_r$ естественно называть *сферой радиуса* r. Аналогичным образом определяется *шар* $\mathbb{B}_r$ радиуса r, состоящий из всех элементов g группы G, для которых $l(g) \leqslant r$. Затем берётся одна из функций распределения $f : \mathbb{N} \cup \{0\} \to \mathbb{R}$, определённая на множестве натуральных чисел с нулем. Например, это может быть функция Пуассона, биномиального или экспоненциального распределения. Предполагается только её невырожденность, т. е. что для любого $r \in \mathbb{N}$ выполняется $f(r) \neq 0$. Для задания функции распределения вероятностей $p : G \to [0, 1]$ для любого r полагаем $p(\mathbb{S}_r) = f(r)$. Далее для любого $g \in \mathbb{S}_r$ полагаем $p(g) = 1/f(r)$, т. е. все элементы сферы $\mathbb{S}_r$ считаются равновероятными. Это определяет функцию распределения вероятностей на всей группе G, что, в свою очередь, даёт возможность говорить о сложности в среднем алгоритма.

Обычно в качестве значения $l(g)$ для элемента g конечно порождённой группы G с фиксированным конечным множеством X порождающих элементов берётся длина кратчайшей записи элемента g в виде группового слова от этих порождающих. *Расстоянием* $d(g, f)$ между элементами g и f группы G считается значение $l(gf^{-1})$. Группа G таким образом превращается в метрическое пространство, изоморфное графу Кэли, соответствующему выбранной системе порождающих элементов. Данная метрика называется *словарной*; длина элемента относительно неё есть его расстояние от 1.

Понятие сложности вычислений в среднем относительно возможных практических приложений в криптографии, основанной на группах, обладает рядом недостатков. Во-первых, возникает вопрос адекватного выбора функции распределения $f : \mathbb{N} \cup \{0\} \to [0, 1]$. Во-вторых, алгоритм может оказаться таким, что он работает чрезвычайно долго только на малой доле возможных входов, а на остальных входах он достаточно быстр. Усреднённое время его работы будет в этом случае не показательным, так как при случайном выборе «плохие» входы будут встречаться крайне редко. Хочется привести в этой связи аналогию с симплекс-методом. В работе [48] показано, что «плохие» входы для него очень специфичны, поэтому их пренебрежимо мало. Это объясняет тот факт, что на практике симплекс-метод вполне хорошо себя зарекомендовал; он широко используется, в то время как знаменитый полиномиальный алгоритм Хачияна [49] имеет в основном теоретическое значение. Более точно, А. М. Вершик и П. В. Спорышев в [50] и независимо С. Смейл в [51] показали, что симплекс-алгоритм работает с линейной сложностью на множестве полной меры.

По описанным выше причинам представляется особенно важным понятие генерической сложности. Для его введения необходимо, чтобы на множестве всех входов была определена мера со значениями в $[0, 1]$. Это не обязательно должна быть функция распределения вероятностей. *Генерическим* называется множество полной меры, дополнение к которому имеет меру 0. Работа [45] представляет точное определение генерической сложности. В ней же установлено, что для широкого класса конечно порождённых групп классические алгоритмические проблемы равенства, сопряжённости и вхождения имеют линейную сложность при их ограничении на некоторое генерическое подмножество (см. также работу [52]).

Перейдём к определениям. Рассмотрим множество всех слов (включая пустое слово) Σ^* в конечном алфавите Σ, состоящем не менее чем из двух букв. Это множество является свободным моноидом со множеством свободных порождающих Σ. Так как на элементах Σ^* естественно определено понятие длины, можно ввести для любого неот-

рицательного целого числа r понятия сферы $\mathbb{S}_r$ и шара $\mathbb{B}_r$ радиуса r, как это объяснено выше. Очевидно, что эти множества конечны и непусты.

Пусть V — произвольное подмножество моноида Σ^*. *Относительной плотностью множества V в сфере* $\mathbb{S}_r$ называется отношение

$$\rho_{\mathbb{S}_r}(V) = \frac{|V \cap \mathbb{S}_r|}{|\mathbb{S}_r|}, \tag{4}$$

где $|\cdot|$ означает число элементов.

Аналогично вводится понятие *относительной плотности множества V в шаре* $\mathbb{B}_r$:

$$\rho_{\mathbb{B}_r}(V) = \frac{|V \cap \mathbb{B}_r|}{|\mathbb{B}_r|}. \tag{5}$$

Будем использовать для определения асимптотической плотности функцию (5), хотя совершенно аналогично можно дать определение, основываясь на функции (4).

Определение 1. *Асимптотической плотностью* подмножества V моноида Σ^* называется верхний предел

$$\rho(V) = \overline{\lim_{r\to\infty}} \rho_{\mathbb{B}_r}(V). \tag{6}$$

Если в (6) существует предел, то он обозначается через $\tilde{\rho}(V)$ и называется *строгой асимптотической плотностью* множества V. В этом случае нас интересует скорость сходимости к пределу $\tilde{\rho}(V)$ последовательности $\{\rho_{B_r}(V)\}_{r\in\mathbb{N}}$. Будем говорить, что сходимость последовательности *экспоненциально быстрая*, если существуют числа $0 \leqslant \sigma < 1$ и $C \geqslant 0$, такие, что для любого r имеет место оценка

$$|\tilde{\rho}(V) - \rho_{B_r}(V)| \leqslant C\sigma^r.$$

Определение 2. Подмножество V множества Σ^* называется *генерическим*, если $\tilde{\rho}(V) = 1$, и *строго генерическим*, если сходимость $\rho_{B_r}(V) \underset{r\to\infty}{\rightrightarrows} \tilde{\rho}(V)$ экспоненциально быстрая.

Если V — генерическое множество, то дополнение к нему $V' = \Sigma^* \setminus V$ называется *пренебрежимым*. В этом случае $\tilde{\rho}(V') = 0$.

Определения 1 и 2 легко распространяются на случай, когда вместо множества Σ^* рассматривается множество $(\Sigma^*)^k$ наборов из k элементов этого множества для $k \geqslant 2$. *Длиной* набора $\bar{g} = (g_1, \ldots, g_k)$ считаем сумму длин его компонент: $l(\bar{g}) = \sum\limits_{i=1}^{k} l(g_i)$.

Можно использовать также другое определение, согласно которому

$$l(\bar{g}) = \max\{l(g_i) : i = 1, \ldots, k\}.$$

Часто алгоритмические проблемы в группах трактуют как подмножества вида $D \subseteq (\Sigma^*)^k$ для некоторого алфавита Σ и натурального числа k. Например, если в качестве Σ взять множество символов, обозначающих порождающие элементы группы G и формальные обратные к ним, то элементы моноида Σ^* могут рассматриваться как групповые слова от порождающих элементов группы G. Рассмотрим подмножество $D_1(G) \subseteq \Sigma^*$, определяющее в группе G тривиальный элемент. Проблема равенства в группе G — это вопрос о принадлежности произвольного слова $u \in \Sigma^*$ подмножеству $D_1(G)$. Проблема сопряжённости на этом языке записывается как $D\ (G) \subseteq (\Sigma^*)^2$ и состоит из таких пар (u, v) слов в алфавите Σ, которые определяют сопряженные

в группе G элементы. Проблема вхождения относительно подгруппы H, порождённой элементами $h_1, \ldots, h_{k-1}$, имеет вид $D_H(G) \subseteq (\Sigma^*)^k$, $D_H = \{(u, h_1, \ldots, h_{k-1})\}$, где u определяет элемент подгруппы H. При этом подгруппа H считается фиксированной. Можно считать также, что фиксировано множество $\{h_1, \ldots, h_{k-1}\}$ порождающих её элементов. В этом случае на вход работы алгоритма должно подаваться слово u. Если рассматривать проблему вхождения в группе G, то элементы $h_1, \ldots, h_{k-1}$ уже не должны считаться фиксированными. При этом, поскольку число k в общем случае не ограничено, проблему вхождения необходимо рассматривать как подмножество бесконечной степени $(\Sigma^*)^\infty$.

Аналогичным образом можно записать широкий круг алгоритмических проблем относительно конечно порождённых групп.

Определение 3. Алгоритм $\mathcal{A}$ решает алгоритмическую проблему $D \subseteq (\Sigma^*)^k$ с *генерической сложностью* $\mathcal{C}$, если существует генерическое подмножество $V \subseteq (\Sigma^*)^k$, такое, что на любом входе из V алгоритм $\mathcal{A}$ работает со сложностью $\mathcal{C}$. Если множество V можно выбрать строго генерическим, то говорят, что алгоритм $\mathcal{A}$ решает проблему D со *строго генерической* сложностью $\mathcal{C}$.

Обращаем внимание на тот факт, что алгоритм $\mathcal{A}$ может быть частично определённым, то есть он может оказаться неопределённым на некоторых входах, которые можно включить в дополнение V' генерического множества V из определения 3. Может так получиться, что проблема D в целом на группе G алгоритмически неразрешима, а в то же время она генерически разрешима с приемлемой сложностью $\mathcal{C}$. Опыт показывает, что это случается довольно часто и для широкого круга алгоритмических проблем (см. по этому поводу [53, 54]). Опять же можно привести аналогию с симплекс-методом из линейного программирования, который на обсуждаемом языке оказывается генерически быстрым.

В практических приложениях выбор данных осуществляется, как правило, случайным образом. Если генерическая сложность какого-либо алгоритма незначительна, то алгоритм практически всегда применим и достаточно быстр, и может быть использован в практических приложениях.

4. Диофантова криптография

Диофантовым уравнением от n переменных называется выражение вида

$$d(\zeta_1, \ldots, \zeta_n) = 0, \tag{7}$$

где $d(\zeta_1, \ldots, \zeta_n)$ — многочлен с целыми коэффициентами от обозначенных независимых коммутирующих переменных. Множество всех таких многочленов составляет кольцо $\Lambda_n = \mathbb{Z}[\zeta_1, \ldots, \zeta_n]$. Кольцо Λ_m при $m \leqslant n$ естественно вложено в кольцо Λ_n. Объединение всех таких колец обозначим через $\Lambda = \mathbb{Z}[\zeta_1, \ldots, \zeta_n, \ldots]$.

На Втором математическом конгрессе, состоявшемся в 1900 г. в Париже, выдающийся математик Д. Гильберт изложил свои знаменитые 23 математические проблемы для математиков XX столетия. Впоследствии их стали называть *Проблемами Гильберта*. Среди этих проблем присутствовала 10-я Проблема о существовании эффективной процедуры, определяющей за конечное число шагов, имеет ли произвольное диофантово уравнение целочисленные корни. Говоря современным языком, 10-ю Проблему Гильберта можно перефразировать следующим образом: существует ли алгоритм, определяющий по произвольному диофантову уравнению (7) его разрешимость в целых числах.

Алгоритмическая неразрешимость 10-й Проблемы Гильберта установлена Ю. В. Матиясевичем в работах [14, 15]. Тем самым им были успешно завершены усилия многих математиков, из которых наиболее весомый вклад в решение проблемы внесли Д. Робинсон, М. Девис и Х. Путнам.

Вернемся к криптографии. Обычно криптографическая система основывается на трудноразрешимой математической проблеме, часто теоретико-числового характера. Приведём список наиболее популярных проблем такого сорта и покажем, что с каждой из таких проблем можно связать диофантово уравнение таким образом, что любое решение этого уравнения даёт возможность эффективно выписать решение соответствующей проблемы и наоборот, решение проблемы приводит к эффективному решению соответствующего диофантова уравнения. Так как любое конечное множество диофантовых уравнений, более того, любое множество диофантовых уравнений от ограниченного числа переменных, которое, как известно из теоремы Гильберта, эквивалентно своей конечной подсистеме, равносильно одному диофантову уравнению, которое легко получается из левых частей уравнений вида (7), если взять квадраты этих левых частей и приравнять их сумму к 0, то можно эффективно сопоставлять любому конечному множеству проблем, о которых говорилось выше, одну равносильную им проблему — о разрешимости в целых числах полученного диофантова уравнения.

Приведённое рассуждение показывает, что диофантов язык является универсальным в определённом смысле. Он может быть применён для криптографических функций многих известных систем шифрования, в том числе для функции шифрования системы RSA, функции дискретного логарифма и т. п. Перечислим некоторые из упомянутых проблем и покажем, как записать соответствующие им системы диофантовых уравнений.

1. **Разложение на множители.** Для данного составного числа n найти натуральные числа $p, q \geqslant 2$, такие, что $n = p \cdot q$.

Во многих приложениях p и q — различные нечётные простые числа. Пусть

$$\mathbb{Z}^{(2)} = \{n = pq : p, q \text{ различные нечётные простые числа}\}.$$

Так как любое натуральное число, согласно теореме Лагранжа, допускает представление в виде суммы квадратов четырёх неотрицательных целых чисел, проблема разложения на множители числа $n \in \mathbb{Z}^{(2)}$, да и любого нечётного составного числа, равносильна разрешимости в целых числах диофантова уравнения

$$(\zeta_1^2 + \zeta_2^2 + \zeta_3^2 + \zeta_4^2 + 3)(\zeta_5^2 + \zeta_6^2 + \zeta_7^2 + \zeta_8^2 + 3) = n.$$

Проблема разложения на множители изучается уже сотни лет. Разрабатываются различные методы разложения, такие, как метод квадратичного решета и метод, использующий эллиптические кривые. Имеются впечатляющие разложения больших составных чисел, осуществлённые с помощью мощных параллельных вычислений. Однако до сих пор не найден эффективный алгоритм для её решения в целом. Это даёт основание считать, что проблема действительно трудна.

2. **Проблема расшифрования в RSA.** Пусть $n = pq \in \mathbb{Z}^{(2)}$. Кольцо вычетов $\mathbb{Z}_n$ используется в системе шифрования RSA в качестве платформы шифрования. Мультипликативная группа $\mathbb{Z}_n^*$ кольца $\mathbb{Z}_n$ имеет порядок $\varphi(n) = (p-1)(q-1)$, где $\varphi(n)$ обозначает функцию Эйлера. Предполагается, что натуральное число e, взаимно простое с $\varphi(n)$, выбрано как ключ шифрования. Проблема расшифрования заключается в нахождении вычета $x \in \mathbb{Z}_n$, кодирующего исходный текст, по его зашифрованному

виду $c = x^e \bmod n$. Эта проблема равносильна разрешимости диофантова уравнения $x^e = c + ny$ относительно неизвестных x и y.

Проблема расшифрования относительно системы RSA изучается последние три десятка лет, но эффективный алгоритм для её решения пока не найден.

3. **Проблема квадратичного вычета.** Пусть $n = pq \in \mathbb{Z}^{(2)}$. Для произвольного вычета $a \in \mathbb{Z}_n$ определить, существует ли вычет $x \in \mathbb{Z}_n$, такой, что справедливо сравнение $x^2 = a(\mathrm{mod} n)$.

Проблема квадратичного вычета равносильна разрешимости диофантова уравнения $x^2 = a + ny$.

Проблема квадратичного вычета лежит в основе системы шифрования Гольдвассер — Микали, на ней базируется семантическая секретность систем Накаче — Штерна и Бекалоха.

Вычисление квадратичного корня по модулю числа $n \in \mathbb{Z}^{(2)}$ при знании разложения $n = pq$ осуществляется за полиномиальное время. В общем случае проблема так же трудна, как и проблема разложения n на множители.

4. **Дискретный логарифм в простом конечном поле.** Пусть p — простое число, тогда $\mathbb{Z}_p$ — простое конечное поле характеристики p. Мультипликативная группа $\mathbb{Z}_p^*$ циклическая. Пусть g — порождающий элемент этой группы. *Дискретным логарифмом* элемента $f \in \mathbb{Z}_p^*$ называется число x, для которого $g^x = f(\mathrm{mod} p)$.

Число x определяется по модулю $(p-1)$ — порядка группы $\mathbb{Z}_p^*$. *Проблемой дискретного логарифма* в поле $\mathbb{Z}_p$ называется вопрос о вычислении x по случайно выбранному элементу f; g считается известным. Пишут $x = \log_g(f)$ и называют его *дискретным логарифмом* элемента f по основанию g. Для однозначности вычисления x накладывается дополнительное ограничение $0 \leqslant x \leqslant p-2$. Проблема дискретного логарифма в простом конечном поле $\mathbb{Z}_p$ равносильна разрешимости *экспоненциального диофантова уравнения*

$$g^x = f + py. \tag{8}$$

Проблема дискретного логарифма может рассматриваться для любого конечного поля, где также может быть записана эквивалентным экспоненциальным диофантовым уравнением. Здесь мы не говорим об этом более подробно.

Из результатов Ю. В. Матиясевича [14, 15] следует, что множество E всех решений x, y уравнения (8) является диофантовым. В общем случае *диофантовым* называется множество наборов $\bar{a} = (a_1, \ldots, a_k)$ целых чисел, для которого существует диофантов многочлен $d(\zeta_1, \ldots, \zeta_k, \varkappa_1, \ldots, \varkappa_n)$, такой, что набор целых чисел $\bar{a} = (a_1, \ldots, a_k)$ принадлежит множеству E в том и только в том случае, если найдутся целые значения $b_1, \ldots, b_n$ для $\varkappa_1, \ldots, \varkappa_n$, такие, что $d(a_1, \ldots, a_k, b_1, \ldots, b_n) = 0$, то есть соответствующее диофантово уравнение разрешимо в целых числах. По теореме Матиясевича любое рекурсивно перечислимое множество E наборов из k целых чисел является диофантовым множеством. Существование такой характеризации рекурсивно перечислимых множеств даёт ещё большее основание говорить о диофантовом языке как об универсальном и рассматривать его в качестве средства построения криптографических систем и протоколов. О явном виде диофантова уравнения, равносильного уравнению вида (8), см. в [55, 56].

Трудность вычисления дискретного логарифма в произвольном случае лежит в основе многочисленного семейства систем шифрования и протоколов, таких, как система ЭльГамаля, протоколы Масси — Омуры и Диффи — Хеллмана, стандарты цифровой подписи DSS и ГОСТ Р 34.10-94, основанные на базовом протоколе ЭльГамаля, и т. д.

Есть ещё одно важное обстоятельство, говорящее в пользу использования неразрешимости 10-й Проблемы Гильберта в качестве основы для построения криптографических примитивов, систем и протоколов. Как недавно показал А. Н. Рыбалов [59], 10-я Проблема Гильберта остаётся неразрешимой на любом строго генерическом множестве диофантовых уравнений.

Каждый диофантов многочлен $d(\zeta_1, \ldots, \zeta_k)$ может рассматриваться как функция из $\mathbb{Z}^k$ в $\mathbb{Z}$. Ю. В. Матиясевич [14, 15] доказал, что существует такой диофантов многочлен $d_0(\zeta_1, \ldots, \zeta_k)$, что не существует алгоритма нахождения решения в целых числах уже в классе уравнений вида $d_0(\zeta_1, \ldots, \zeta_k) = c$, где $c \in \mathbb{Z}$. Таким образом можно определить функцию $\mathbb{Z}^k \to \mathbb{Z}$, которая может рассматриваться в качестве кандидата на одностороннюю функцию. Действительно, значение данного диофантова многочлена вычисляется за полиномиальное время, в то время как не существует полиномиального ограничения на нахождение аргумента по значению функции $d_0(\zeta_1, \ldots, \zeta_k)$.

Односторонней называется функция, эффективно вычислимая за полиномиальное время на детерминированной машине Тьюринга, для которой не существует вероятностной машины Тьюринга, вычисляющей за полиномиальное время по значению функции один из соответствующих этому значению аргументов с существенной вероятностью. Формального определения здесь не приводим, тем более что часто в определении присутствуют дополнительные требования (см. по этому поводу [57]).

Односторонние функции являются неотъемлемой частью криптографических систем и протоколов. Теоретически их существование ещё не доказано. В то же время ряд функций, которые претендуют на то, чтобы считаться односторонними, широко используются в криптографии. Нам представляется, что диофантовы функции дают широкие возможности для построения возможно односторонних функций, тем более что, как показано выше, ряд кандидатов на роль односторонних функций могут трактоваться как диофантовы.

С. Ю. Ерофеев в работе [58] рассмотрел различные варианты построения не только возможно односторонних, но и возможно двушагово односторонних функций. *Двушагово односторонней* называется композиция двух односторонних функций, которая сама является односторонней. Более того, по значению композиции и известному аргументу второй из функций аргумент самой композиции не является эффективно вычислимым. Необходимость построения таких функций объясняется тем, что в ряде предлагаемых протоколов, например в протоколе аутентификации с нулевым разглашением из [13], наличия обычных односторонних функций недостаточно.

5. Свободные метабелевы группы и проблема эндоморфной сводимости

Этот раздел связан с базовыми понятиями теории групп (о них см., например, [32, 33] и другие книги, излагающие основы теории групп). Элементы теории групповых многообразий см., например, в [10].

5.1. Свободные метабелевы группы

Напомним, что для произвольного натурального числа n через F_n обозначается свободная группа ранга n. Её фактор-группа по коммутанту $A_n = F_n/F_n'$ является свободной абелевой группой ранга n, а фактор-группа по второму коммутанту $M_n = F_n/F_n''$ — свободной метабелевой группой ранга n. При этом второй коммутант G'' определяется как коммутант от коммутанта $(G')'$. Он также является нормальной подгруппой группы G. Фактор-группа G/G'' по второму коммутанту является метабелевой группой. В общем случае *метабелевой* называется группа, в которой существует цепочка

нормальных подгрупп

$$1 \leqslant A \leqslant G \tag{9}$$

с абелевыми факторами. Другими словами, в группе G есть абелева нормальная подгруппа A, фактор-группа по которой G/A также абелева. Легко проверяется, что группа G метабелева в том и только в том случае, если её коммутант G' абелев. В определении (9) коммутант G' играет роль A.

Заметим, что фактор-группа M_n/M_n' также изоморфна свободной абелевой группе A_n.

Зафиксируем канонические гомоморфизмы $\pi_n' : F_n \to A_n$, $\pi_n'' : F_n \to M_n$, $\pi_n : M_n \to A_n$. Если $(f_1, \ldots, f_n)$ — *базис*, то есть *множество свободных порождающих* группы F_n, то $(a_1, \ldots, a_n) = (f_1F_n', \ldots, f_nF_n')$ — соответствующий базис группы A_n и $(x_1, \ldots, x_n) = (f_1F_n'', \ldots, f_nF_n'')$ — базис группы M_n. Имеем также $(a_1, \ldots, a_n) = (\pi_n(x_1), \ldots, \pi_n(x_n))$.

Группы A_n и M_n являются свободными группами многообразия $\mathcal{A}$ всех абелевых групп и многообразия $\mathcal{A}^2$ всех метабелевых групп соответственно. Любое отображение базиса группы A_n в произвольную абелеву группу A и любое отображение базиса группы M_n в произвольную метабелеву группу M однозначно продолжается до гомоморфизма $A_n \to A$ и $M_n \to M$ соответственно.

Перейдём к описанию структуры свободной метабелевой группы M_n. Как уже отмечалось, фактор-группа M_n/M_n' изоморфна свободной абелевой группе A_n. Это означает, что любой элемент группы M_n однозначно представим в виде

$$g = \prod_{i=1}^{n} x_i^{k_i} u, \tag{10}$$

где $k_i \in \mathbb{Z}$ для $i = 1, \ldots, n$; элемент $u = u(g)$ принадлежит коммутанту M_n'. Чтобы получить из (10) нормальную форму записи элемента g, достаточно построить такую форму для элемента u.

Так как M_n' — нормальная абелева подгруппа группы M_n, её можно рассматривать как модуль над групповым кольцом $\mathbb{Z}A_n$. Групповая операция в этом модуле — это умножение в группе M_n. Действие элемента $a \in A_n$ на элемент $v \in M_n'$ определяется следующим образом. Берём произвольный прообраз $\bar{a}$ элемента a в группе M_n относительно канонического гомоморфизма π_n и полагаем

$$v^a = v^{\bar{a}}. \tag{11}$$

Так как все возможные прообразы $\bar{a}$ отличаются друг от друга на элементы из M_n', сопряжение в (11) не зависит от выбора $\bar{a}$. Следовательно, приведённое определение корректно. Продолжение действия на групповое кольцо $\mathbb{Z}A_n$ осуществляется по линейности, а именно: для любого набора элементов $b_j \in A_n$ и любого набора целых чисел $l_j \in \mathbb{Z}$ $(j = 1, \ldots, p)$ полагаем

$$v^{\sum\limits_{j=1}^{p} l_j b_j} = \prod_{j=1}^{p} (v^{b_j})^{l_j}, \tag{12}$$

причём правая часть в (12) не зависит от порядка сомножителей, что обеспечивает корректность определения.

Коммутант M_n' более естественно рассматривать как модуль над $\mathbb{Z}A_n$ по следующим причинам. Как подгруппа, M_n' является свободной абелевой группой, ранг которой бесконечен. Следовательно, такое представление не является конечным. Как

модуль, M'_n конечно порождён. В качестве его порождающих элементов можно взять набор коммутаторов вида

$$e_{ij} = [x_i, x_j] \text{ для } i > j;\ i, j = 1, \ldots, n. \tag{13}$$

Покажем, как произвольное слово $v = v(x_1, \ldots, x_n)$, записывающее элемент коммутанта M'_n, представляется через порождающие модуля (13). Сначала переставляем влево все вхождения $x_1^{\pm 1}$, пользуясь формулами

$$x_i x_1 = [x_i, x_1] x_1 x_i, \quad x_i^{-1} x_1 = [x_i^{-1}, x_1] x_1 x_i^{-1} = [x_i, x_1]^{-a_i^{-1}} x_1 x_i^{-1}, \quad x_i x_1^{-1} = [x_i, x_1^{-1}] x_1^{-1} x_i =$$
$$= [x_i, x_1]^{-a_1^{-1}} x_1^{-1} x_i, \quad x_i^{-1} x_1^{-1} = [x_i^{-1}, x_1^{-1}] x_1^{-1} x_i^{-1} = [x_i, x_1]^{a_1^{-1} a_i^{-1}} x_1^{-1} x_i^{-1}.$$

Возникающие при этом коммутаторы $e_{ij} = [x_i, x_1]$ передвигаются вправо согласно формуле $[x_i, x_1] f = f [x_i, x_1]^{f^{-1}}$, справедливой при любом $i = 2, \ldots, n$ и любом $f \in M_n$. После того как будут переставлены все вхождения $x_1^{\pm 1}$, произойдёт сокращение этих степеней и таких вхождений уже не будет. Продолжим процесс переписки, переводя влево $x_2^{\pm 1}$, и т. д. В результате получим выражение вида

$$v = \prod_{\substack{i>j,\\ i,j=1,\ldots,n}} e_{ij}^{\alpha_{ij}} \tag{14}$$

для некоторых элементов α_{ij} группового кольца $\mathbb{Z}A_n$.

При $l < t$ считаем, что e_{lt} обозначает коммутатор $[x_l, x_t] = [x_t, x_l]^{-1} = e_{tl}^{-1}$. Модуль M'_n не является свободным. Относительно порождающих (13) все его определяющие соотношения следуют из следующих соотношений Якоби:

$$e_{ij}^{a_k - 1} e_{jk}^{a_i - 1} e_{ki}^{a_j - 1} = 1. \tag{15}$$

Ввиду этих соотношений форма (14) записи элемента v не является однозначной. Для получения однозначной (нормальной) формы записи элемента $v \in M'_n$ воспользуемся следующими соображениями. Для любых $m < n$ будем считать группу A_m естественно вложенной подгруппой группы A_n.

Утверждение 1. Любой элемент коммутанта M'_n однозначно представим в виде

$$v = \prod_{\substack{i>j,\\ i,j=1,\ldots,n}} e_{ij}^{\alpha_{ij}}, \tag{16}$$

где $\alpha_{ij} \in \mathbb{Z}A_i$ для $i > j; i, j = 1, \ldots, n$.

Доказательство. Пусть элемент v записан в форме (14). Покажем сначала, как можно исключить в этой записи элементы $a_i^{\pm 1}$ для $i > 2$ из показателя модульного порождающего e_{21}. Начинаем с исключения $a_3^{\pm 1}$. Достаточно рассмотреть случай, когда в показателе стоит элемент группы A_n вида $a_3^k h$, где h не зависит от a_3. Пусть $k > 0$. Тогда $a_3^k h = (a_3 - 1) a_3^{k-1} h + a_3^{k-1} h$. Отсюда и из соотношений (15) получаем равенство

$$e_{21}^{a_3^k h} = e_{21}^{a_3^{k-1} h} e_{31}^{(a_2 - 1) a_3^{k-1} h} e_{32}^{-(a_3 - 1) a_3^{k-1} h}.$$

Далее продолжаем процесс указанным способом до полного исключения a_3^k.

Пусть $k < 0$. Равенства (15) остаются справедливыми, если в них заменить x_3 и a_3 соответственно на x_3^{-1} и на a_3^{-1}. Следовательно, можем исключить из рассматриваемого показателя a_3^k, как это делалось выше, а затем использовать равенства

$$[x_3^{-1}, x_i] = [x_3, x_i]^{-a_3^{-1}} \text{ для } i = 1, 2.$$

Подобным образом исключим из показателя элемента e_{21} все элементы вида $a_i^{\pm 1}$ для $i = 3, \ldots, n$. Оставшийся показатель принадлежит групповому кольцу $\mathbb{Z}A_2$. Далее исключаем подобным образом $a_i^{\pm 1}$ для $i \geqslant 4$ из показателей степеней при e_{31} и e_{32}. В конце концов получим запись элемента v в форме (16). Докажем, что полученная запись единственная. Сначала применим к (16) гомоморфизм специализации группы M_n, определённый на базисных элементах как $x_i \mapsto x_i$ для $i = 1, 2$ и $x_j \mapsto 1$ для $j \geqslant 3$. Образом элемента v будет $e_{21}^{\alpha_{21}}$. Так как все соотношения в модуле M_n' следуют из соотношений Якоби, подмодуль, порождённый в M_n' любым из элементов e_{ij}, свободен. Значит, показатель α_{21} определяется однозначно.

Далее рассматриваем элемент $v' = e_{21}^{-\alpha_{21}} v$ и применяем к нему гомоморфизм специализации, определенный отображением $x_i \mapsto x_i$ для $i = 1, 2, 3$, и $x_j \mapsto 1$ для $j \geqslant 4$. Образом элемента v' будет $e_{31}^{\alpha_{31}} e_{32}^{\alpha_{32}}$. Так как все соотношения в модуле M_n' следуют из соотношений Якоби, подмодуль, порождённый в M_n' набором элементов $e_{i1}, \ldots, e_{ii-1}$, является свободным на этих порождающих. Значит, показатели α_{31} и α_{32} определяются по элементу v однозначно. Продолжая доказательство подобным образом, установим однозначность записи (16). ■

Группа M_n допускает также точное представление матрицами над полем. Оно получается из следующего знаменитого точного матричного представления, известного как *вложение Магнуса*. Относительно этого представления см., например, монографию [60].

Пусть T_n обозначает свободный модуль ранга n над групповым кольцом $\mathbb{Z}A_n$ с базисом $t_1, \ldots, t_n$. Рассмотрим группу матриц $M(A_n, T_n)$ вида

$$\begin{pmatrix} a & \sum\limits_{i=1}^{n} \alpha_i t_i \\ 0 & 1 \end{pmatrix}, \tag{17}$$

где $a \in A_n, \alpha_i \in \mathbb{Z}A_n$ для $i = 1, \ldots, n$.

Группа $M(A_n, T_n)$ является прямым сплетением группы A_n на себя, то есть $M(A_n, T_n) = A_n \wr A_n$. Относительно определения и свойств конструкции сплетения групп см., например, [32]. Легко проверяется, что группа $M(A_n, T_n)$ метабелева. Все матрицы вида (17) с 1 в левом верхнем углу образуют в ней абелеву нормальную подгруппу N, фактор-группа по которой изоморфна группе A_n. Группа N является модулем над групповым кольцом $\mathbb{Z}A_n$ с базисом $t_1, \ldots, t_n$. Можно заметить, что модульная операция индуцируется сопряжениями элементами группы $M(A_n, T_n)$ аналогично тому, как это объяснялось выше относительно модуля M_n'.

Вложение Магнуса группы M_n в группу $M(A_n, T_n)$ определяется следующим отображением базиса:

$$\mu : x_i \mapsto \begin{pmatrix} a_i & t_i \\ 0 & 1 \end{pmatrix} \text{ для } i = 1, \ldots, n. \tag{18}$$

Вложение Магнуса также позволяет ввести нормальную форму элементов группы M_n как матриц вида (18). Важно отметить для этого, что матрица вида (17) принадлежит образу $\mu(M_n)$ тогда и только тогда, когда выполнено равенство

$$a - 1 = \sum_{i=1}^{n} \alpha_i (a_i - 1). \tag{19}$$

Для того чтобы считать группу $M(A_n, T_n)$ матричной над полем, возьмем поле частных $\mathbb{F}$ группового кольца $\mathbb{Z}A_n$ и его чисто трансцендентное расширение

$\bar{\mathbb{F}} = \mathbb{F}(t_1, \ldots, t_n)$. Тогда группа $M(A_n, T_n)$ оказывается подгруппой полной матричной группы $GL_2(\bar{\mathbb{F}})$.

Вложение Магнуса и его обобщения широко используются в теории групп для доказательства важных утверждений не только о свободных метабелевых группах, но и о группах из широкого класса групп вида F/R', то есть фактор-групп по коммутантам нормальных подгрупп свободных групп F. Имеется прямая связь с другим важным понятием теории групп — свободными дифференцированиями Фокса (см., например, монографию [60]).

Например, с помощью вложения Магнуса легко доказать, что моноид X_n^*, порождённый в группе M_n множеством свободных порождающих $X_n = \{x_1, \ldots, x_n\}$, свободен. Это позволяет, например, записывать элементами этого моноида слова в произвольном алфавите из n букв. Можно использовать вместо X_n^* его автоморфную копию или произвести еще какие-нибудь операции, позволяющие скрыть вид слов. Это даёт возможности для построения криптографических примитивов, а затем на их основе систем и протоколов.

Есть ещё ряд обстоятельств, говорящих в пользу групп M_n как возможных платформ для криптографических систем. Во-первых, в группе M_n при любом n проблема равенства разрешима за полиномиальное время. Более точно, в [61] показано, что проблема равенства в группе M_n решается за время $\mathrm{O}(nm \log_2 m)$, где m — длина слова. Там же указан соответствующий алгоритм. В то же время близкая по постановке алгоритмическая проблема вычисления геодезической длины элемента, по которой для данного слова группы M_n нужно найти длину его кратчайшей записи от элементов базиса, является NP-полной. В [62] установлено, что проблема сопряжённости в группе M_n решается за время $\mathrm{O}(nm^8)$, где m обозначает сумму длин двух слов, для которых проверяется сопряжённость записываемых ими элементов группы M_n. Доказательство в [62] конструктивно, что позволяет дать точно такую же оценку времени решения соответствующей проблемы поиска сопряжённого элемента. Приведённые здесь результаты говорят о том, что можно эффективно работать с элементами групп M_n, их нормальными формами и сопряжёнными элементами. Известны также [63] эффективные алгоритмы, решающие в группах M_n проблему вхождения.

Важно также отметить, что группа M_n при $n \geqslant 2$ имеет экспоненциальный рост. Это означает, что функция роста количества элементов длины $\leqslant r$ относительно словарной метрики группы M_n экспоненциальна. Значит, если рассматривать группу M_n при $n \geqslant 2$ в качестве источника параметров, ключей и т. п., соответствующее пространство будет достаточно обширно, чтобы его нельзя было атаковать методом полного перебора.

В заключение отметим, что классические алгоритмические проблемы равенства, сопряжённости и вхождения разрешимы в любой конечно порождённой метабелевой группе. Проблема равенства решена Е. И. Тимошенко [64]. Разработанный им алгоритм, сводящий проблему к решению системы линейных уравнений над групповым кольцом $\mathbb{Z}A_n$ свободной абелевой группы, вполне пригоден для практического использования. Проблема сопряжённости решена Г. А. Носковым [65], но представленный им алгоритм довольно сложен. Он опирается на структурную теорию коммутативных колец и, по-видимому, в такой форме вряд ли может использоваться практически. В работе [66] описан алгоритм, решающий в конечно порождённой метабелевой группе более общую, чем проблема сопряжённости, проблему скрученной сопряжённости. По представлению автора, такой более общий подход даёт возможность его практического использования, по крайней мере, на генерическом множестве. Проблема вхож-

дения решена Н. С. Романовским [63]. На практичность она не исследована, но, по-видимому, может быть реализована для такой цели. Разрешимы и многие другие алгоритмические проблемы [67] (см. соответствующий обзор в [25]). Правда, с точки зрения теории сложности общий случай ещё исследован недостаточно. В классе всех конечно порождённых метабелевых групп разрешима проблема изоморфизма данной свободной метабелевой группе M_n [68]. Разрешимость проблемы изоморфизма в этом классе остается открытым вопросом (см. по этому поводу [69]).

5.2. Уравнения в группах

Итак, классические алгоритмические проблемы в свободных метабелевых группах разрешимы. Однако некоторые другие естественные по своей постановке алгоритмические проблемы в этих группах неразрешимы. Первые такие примеры указаны автором в [11, 12]. Это алгоритмические проблемы разрешимости произвольного уравнения в группе M_n при $n \geqslant 2$ и разрешимость проблемы эндоморфной сводимости в группе M_n достаточно большого ранга $n \geqslant n_0$. Для постановки этих проблем и объяснения их неразрешимости необходимо провести специальную подготовку, к которой мы сейчас переходим.

Пусть G — группа. *Нижним центральным рядом* группы G называется убывающая последовательность нормальных подгрупп

$$G = \gamma_1 G \geqslant \gamma_2 G \geqslant \dots \gamma_k G \geqslant \dots, \tag{20}$$

в которой $\gamma_{i+1}G = [\gamma_i G, G]$ — подгруппа, порождённая всеми коммутаторами вида $[g, f]$, где $g \in \gamma_i G, f \in G$. Ряд (20) называется *центральным*, так как любой его фактор $\gamma_i G/\gamma_{i+1}G$ лежит в центре фактора $G/\gamma_{i+1}G$. Группа G называется *нильпотентной*, если для некоторого i в ней $\gamma_{i+1}G = 1$. Наименьшее число i с этим свойством называется *ступенью нильпотентности* группы G. Считается, что тривиальная группа имеет ступень нильпотентности 0, нетривиальная абелева группа — ступень нильпотентности 1 и т. д.

Выпишем известные (см., например, [32]) коммутаторные тождества, справедливые в любой группе G:

$$\begin{gathered}[xy, z] = [y, z]^x [x, z] = [[y, z], x]^{-1} [y, z][x, z], \\ [x^{-1}, z] = [x, z]^{-1} [[x, z], x^{-1}], \\ [z, x^{-1}] = [[x, z], x^{-1}]^{-1} [x, z].\end{gathered} \tag{21}$$

Одним из следствий тождеств (21) является следующая относительная дистрибутивность:

$$[g_1^{k_1}, \dots, g_l^{k_l}] = [g_1, \dots, g_l]^{\prod_{i=1}^{l} k_i} (\mathrm{mod}\, \gamma_{l+1} G), \tag{22}$$

где $g_1, \dots, g_l$ — произвольные элементы группы G, а $k_1, \dots, k_l$ — целые числа.

Предполагаем, что в левой части стоит *простой* коммутатор, т. е. коммутатор вида $[\dots[[a_1, a_2], a_3], \dots, a_l]$, в котором скобки стоят слева направо. Такие коммутаторы ещё называют *левонормированными*. Однако равенство (22) остаётся верным при любой расстановке скобок, важно только, чтобы все операции с символами были коммутаторными.

Известно [10, 32], что в метабелевых группах выполняется тождество

$$[f, h, g_1, g_2, \dots, g_l] = [f, h, g_{\sigma(1)}, \dots, g_{\sigma(l)}],$$

где σ — произвольная перестановка символов $1, \ldots, l$.

Для свободных порождающих $x_1, \ldots, x_n$ группы M_n определяются *базисные коммутаторы* — простые коммутаторы от элементов базиса $x_1, \ldots, x_n$ вида

$$[x_{i_1}, x_{i_2}, x_{i_3}, \ldots, x_{i_l}], \tag{23}$$

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. Известно [70, 71], что образы базисных коммутаторов веса l относительно канонического гомоморфизма $M_n \to G/\gamma_{i+1}M_n$ образуют базис свободной абелевой группы $\gamma_i M_n/\gamma_{i+1}M_n$.

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

$$g = \prod_{j=1}^{t} c_j^{k_j} (\mathrm{mod} \gamma_{i+1}M_n) \text{ для некоторых } k_j \in \mathbb{Z}. \tag{24}$$

Таким образом, по модулю $\gamma_{i+1}M_n$ элементы группы M_n кодируются наборами целых чисел $(k_1, \ldots, k_t)$, $t = t(i)$. 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.

Любое отображение группы M_n на себя, рассматриваемое по модулю $\gamma_{i+1}M_n$, определяет отображение $\mathbb{Z}^t \to \mathbb{Z}^t$, и наоборот. Можно ввести в рассмотрение свободную метабелеву нильпотентную ступени $i+1$ группу $M_{n,i} = M_n/\gamma_{i+1}M_n$ и говорить о нормальной форме её элементов, соответствующей (24), её отображениях и т. п. Группа $M_{n,i}$ является свободной группой ранга n многообразия всех метабелевых нильпотентных ступени $\leqslant i$ групп, которое есть пересечение многообразия $\mathcal{A}^2$ всех метабелевых групп и многообразия $\mathcal{N}_i$ всех нильпотентных групп ступени $\leqslant i$.

Пусть два элемента g и f группы M_n записаны в виде (24), причем элемент g имеет координаты $(k_1, \ldots, k_t)$, а элемент f — координаты $(q_1, \ldots, q_t)$. Тогда существуют многочлены $p_j = p_j(\zeta_1, \ldots, \zeta_{t(j)}, \varkappa_1, \ldots, \varkappa_{t(j)})$ для $j = 1, \ldots, t$, такие, что координаты $(r_1, \ldots, r_t)$ произведения $h = gf$ вычисляются по формулам

$$r_j = p_j(k_1, \ldots, k_{t(j)}, q_1, \ldots, q_{t(j)}). \tag{25}$$

Напомним, что $t(j)$ обозначает количество всех базисных коммутаторов веса не больше чем j.

Аналогично, существуют многочлены $u_j(\zeta_1, \ldots, \zeta_t)$ для $j = 1, \ldots, t$, вычисляющие по координатам элемента g координаты обратного к нему элемента g^{-1}. Теория базисных коммутаторов введена в рассмотрение Ф. Холлом более 50 лет назад и получила широкое применение в теории групп (см. лекции Ф. Холла [70] и монографию [71]).

Важно отметить, что в рассматриваемом случае групповые операции переписываются через диофантовы функции. Это позволяет переходить от групповых уравнений к диофантовым. Вопрос о разрешимости группового уравнения таким образом сводится к решению соответствующего диофантова уравнения. Здесь также проявляется универсальность диофантова языка. Рассмотрим этот вопрос более подробно.

Уравнением в группе G (ещё говорят «над группой G»), или *групповым уравнением*, называется выражение вида

$$w = w(z_1, \ldots, z_r) = 1, \tag{26}$$

где w — групповое слово от неизвестных $z_1, \ldots, z_r$ и элементов группы G. Если ввести в рассмотрение свободную группу F с базисом $\{z_1, \ldots, z_r, \ldots\}$, то w может рассматриваться как элемент свободного произведения $G[z_1, \ldots, z_r, \ldots] = F * G$. *Решением* уравнения (26) называется набор элементов $g_1, \ldots, g_r$ группы G, для которого $w(g_1, \ldots, g_r) = 1$. Решению $g_1, \ldots, g_r$ соответствует гомоморфизм $\varphi : G[z_1, \ldots, z_r, \ldots] \to G$, при котором элементы группы G отображаются сами на себя, на группе F гомоморфизм определяется своими значениями $z_i \mapsto g_i$ при $i = 1, \ldots, r$, и произвольными значениями остальных порождающих z_j для $j \geqslant r+1$. Наоборот, каждому гомоморфизму φ группы $G[z_1, \ldots, z_r, \ldots]$ в группу G, тождественному на элементах группы G, отвечает решение $g_i = \varphi(z_i)$, $(i = 1, \ldots, r)$. Уравнение (26) называется *разрешимым*, если для него существует хотя бы одно решение, и *неразрешимым* в противном случае. Соответственно ставится следующая алгоритмическая проблема.

Проблема разрешимости уравнений. Разрешимо ли произвольное уравнение (26) в данной группе G.

Проблема разрешимости уравнений может ставиться также для класса групп $\mathcal{L}$ — вопрос о существовании алгоритма, который по произвольной группе G из данного класса $\mathcal{L}$ и произвольному уравнению (26) определяет его разрешимость в G. Можно рассматривать более широкую проблему *разрешимости систем уравнений* в группе или в классе групп. Можно, напротив, ограничивать класс рассматриваемых уравнений. Например, брать уравнения от ограниченного числа переменных или уравнения специального вида. Важным классом являются так называемые *бескоэффициентные* уравнения вида

$$w(z_1, \ldots, z_r) = f, \tag{27}$$

где левая часть не зависит от элементов группы G (*коэффициентов*), а в правой части стоит элемент f группы G.

Для любого натурального числа i сопоставим уравнению (26) *относительное уравнение*

$$w(z_1, \ldots, z_r) = 1 (\mathrm{mod} \gamma_{i+1} G), \tag{28}$$

для которого естественно определяется понятие *разрешимости*. Ясно, что разрешимость уравнения (26) влечет разрешимость уравнения (28) для любого i. Обратное утверждение в общем случае неверно. Разрешимость уравнения (28) в группе G равносильно разрешимости его гомоморфного образа в группе $G/\gamma_{i+1}G$. Под *гомоморфным образом* понимается уравнение, полученное из исходного уравнения заменой всех вхождений элементов из G на их канонические гомоморфные образы в фактор-группе $G/\gamma_{i+1}G$.

Итак, разрешимость относительных уравнений в группе равносильна разрешимости уравнений в фактор-группе. Выше рассмотрены относительные уравнения по модулю членов нижнего центрального ряда $\gamma_{i+1}G$ группы G. Однако ясно, что можно брать относительные уравнения по модулю любой нормальной подгруппы N группы G и связывать с ними уравнения в фактор-группе G/N.

Свободные метабелевы группы обладают так называемым свойством *эллиптичности*, или *конечности ширины* вербальных подгрупп, которое позволяет, в частности, относительным уравнениям (28) в группе $G = M_n$ сопоставлять равносильные им

уравнения в самой группе M_n. Напомним, что *вербальной* подгруппой $v(G)$ группы G, соответствующей групповому слову $v = v(z_1, \ldots, z_r)$, называется подгруппа, порождённая всеми *значениями* $v(g_1, \ldots, g_r)$ слова v в группе G. Подгруппа $v(G)$ имеет *конечную ширину* $l = \mathrm{width}(v(G))$, если любой элемент $u \in v(G)$ представим как произведение не более l значений слова v или обратного к нему v^{-1} в группе G, и l — минимальное число с этим свойством. Если такого числа l не существует, то говорят, что подгруппа $v(G)$ имеет *бесконечную ширину*.

Известно [72] (доказательство можно найти также в [73]), что любая вербальная подгруппа свободной метабелевой группы M_n при любом n имеет конечную ширину. Следовательно, любой член нижнего центрального ряда $\gamma_i M_n$ имеет конечную ширину $l_{n,i} = \mathrm{width}(\gamma_i M_n)$ относительно слова $v_i = v_i(z_1, \ldots, z_i) = [z_1, z_2, \ldots, z_i]$. Более точно, в работе [74] показано, что $l_{n,2} = [n/2]$ при $n \geqslant 2$ и $l_{n,i} = n$ при $i \geqslant 3$.

Это означает, что если взять слово

$$V_{n,i} = \prod_{j=1}^{l_{n,i}} [z_{j,1}^{(1)}, z_{j,2}^{(1)}, \ldots, z_{j,i}^{(1)}][z_{j,1}^{(2)}, z_{j,2}^{(2)}, \ldots, z_{j,i}^{(2)}]^{-1}$$

от независимых переменных $z_{j,k}^{(t)}$ $(j = 1, \ldots, l_{n,i};\ k = 1, \ldots, i;\ t = 1, 2)$, то любой элемент $u \in \gamma_i M_n$ представляется как значение этого слова в группе M_n. Значит, уравнение

$$u = \prod_{j=1}^{l_{n,i}} [z_{j,1}^{(1)}, z_{j,2}^{(1)}, \ldots, z_{j,i}^{(1)}][z_{j,1}^{(2)}, z_{j,2}^{(2)}, \ldots, z_{j,i}^{(2)}]$$

разрешимо в группе M_n тогда и только тогда, когда элемент u принадлежит подгруппе $\gamma_i M_n$. Отсюда получаем, что относительное уравнение (28) разрешимо в группе M_n тогда и только тогда, когда в M_n разрешимо уравнение

$$w(z_1, \ldots, z_r) V_{n,i} = 1.$$

Разрешимость относительного бескоэффициентного уравнения (27) равносильна разрешимости бескоэффициентного уравнения

$$w(z_1, \ldots, z_r) V_{n,i} = f.$$

Рассмотрим относительное уравнение

$$w(z_1, \ldots, z_r) = 1 (\mathrm{mod}\, \gamma_{i+1} G). \tag{29}$$

Перепишем в нормальной форме (24) все константы, входящие в запись (29), и все неизвестные $z_1, \ldots, z_r$, полагая $z_k = \prod_{j=1}^{t} c_j^{\zeta_{k,j}} (\mathrm{mod}\, \gamma_{i+1})$, с неизвестными показателями степеней $\zeta_{k,j}$ $(k = 1, \ldots, r;\ j = 1, \ldots, t)$, где $t = t(i)$. Другими словами, запишем константы и неизвестные в координатной форме. Затем приведём левую часть уравнения к нормальному виду (24), используя многочлены (25). Решению уравнения (29) соответствует тривиальная нормальная форма. Значит, все показатели полученной нормальной формы должны равняться нулю. Разрешимость уравнения (29) сводится таким образом к разрешимости системы из $t = t(i)$ диофантовых уравнений. В свою очередь, любая конечная система диофантовых уравнений равносильна одному диофантову уравнению.

Равносильность относительных и обычных уравнений в группе M_n позволяет получать те же системы диофантовых уравнений и для уравнений в группе M_n.

Остаётся установить, что класс получающихся диофантовых уравнений достаточно широк с точки зрения его алгоритмической разрешимости, а именно, что этот класс алгоритмически неразрешим. Это сделано в работах автора [11, 12]. А именно, в [12] показано, что по любому диофантову уравнению (7) можно явно указать такое групповое слово $w(z_1, \ldots, z_r)$, не зависящее от констант, и такой элемент f группы M_n для произвольного $n \geqslant 2$, что уравнение (27) разрешимо в группе M_n тогда и только тогда, когда диофантово уравнение (7) разрешимо в целых числах. Более того, можно зафиксировать левую часть уравнения (27), а элемент f выбирать из фиксированного смежного класса по циклической подгруппе $\mathrm{гр}(h)$ группы M_n. Отсюда и из неразрешимости 10-й Проблемы Гильберта следует неразрешимость проблемы разрешимости уравнений в любой свободной метабелевой нециклической группе. Более того, эта проблема неразрешима уже для класса бескоэффициентных уравнений с фиксированной левой частью, правая часть которых берется из фиксированного смежного класса по циклической подгруппе, как это объяснено выше.

Перейдем теперь к проблеме эндоморфной сводимости. Для произвольной группы G она ставится следующим образом.

Проблема эндоморфной сводимости. Определить по произвольным элементам g и f группы G, является ли элемент f эндоморфным образом элемента g при каком-нибудь эндоморфизме группы G.

Если рассмотреть свободную метабелеву группу M бесконечного счётного ранга с базисом $\{x_1, \ldots, x_r, \ldots\}$, то неразрешимость проблемы эндоморфной сводимости в ней вытекает из неразрешимости проблемы разрешимости бескоэффициентных уравнений в M_2. Действительно, для произвольных элементов $g = g(x_1, \ldots, x_r)$ и $f = f(x_1, \ldots, x_r)$ группы M элемент f является эндоморфным образом элемента g тогда и только тогда, когда он является таковым, если рассматривать группу M_r с базисом $\{x_1, \ldots, x_r\}$. В свою очередь, это равносильно разрешимости в M_r уравнения

$$g(z_1, \ldots, z_r) = f.$$

Как отмечено выше, эта проблема неразрешима уже в группе M_2. Число неизвестных также можно ограничить, поскольку известно [75], что 10-я Проблема Гильберта неразрешима уже для класса диофантовых уравнений от 9 переменных. Значит, для достаточно большого r проблема эндоморфной сводимости в группе M_r алгоритмически неразрешима.

Есть несколько возможностей построения диофантовых функций на свободных метабелевых группах. Произвольный эндоморфизм μ группы M_n однозначно определяется своими значениями на элементах базиса. Можно вести рассуждения по модулю $\gamma_{i+1}M_n$. Тогда этим значениям $\mu(x_i)$ для $i = 1, \ldots, n$ взаимно однозначно соответствуют наборы целых чисел из (24). Наоборот, любой набор из n таких наборов определяет некоторый эндоморфизм группы M_n, рассматриваемый по модулю $\gamma_{i+1}M_n$. Эндоморфизм, в свою очередь, является, с одной стороны, отображением группы M_n в себя, с другой стороны, если его рассматривать по модулю $\gamma_{i+1}M_n$, может считаться отображением множества $\mathbb{Z}^t$ в себя. Это отображение в свете существования диофантовых функций (25) является диофантовым отображением. Семейство таких отображений, среди которых, как известно, есть такие, что проблема нахождения для них прообразов по данному значению алгоритмически неразрешима, даёт богатую возможность

построения функций, претендующих на роль односторонних. Другие возможности связаны с рассмотрением других нормальных форм элементов группы M_n, о которых говорилось выше. В следующей работе мы приведём детали подобных построений.

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. `www.grouptheory.info/PersonalPages/Shpilrain,Vladimir/CryptologyePrintArchive`
4. *Anshel I., Anshel M., and Goldfeld D.* An algebraic method for public-key cryptography // Math. Res. Lett. 1999. V. 6. P. 287–291.
5. *Марков А. А.* Основы алгебраической теории кос // Труды Матем. ин-та АН СССР. 1945. Т. 16. С. 3–54.
6. *Dehornoy P.* Braids and self-distributivity. (Progress in Math. 192). Basel, Berlin, New York: Birkhäuser Verlag, 2000. 623 p.
7. *Лин В. Я.* Косы Артина и связанные с ними группы и пространства // Итоги науки и техн. Алгебра. Геометрия. Топология. Т. 17. М.: ВИНИТИ, 1983. С. 159–227.
8. *Dehornoy P.* Braid-based cryptography // Group theory, statistics and cryptography. Contemp. Math. V. 360. Providence, RI: Amer. Math. Soc., 2004. P. 5–33.
9. *Mahlburg K.* An overview of braid group cryptography. 2004. `www.math.wisc.edu/~boston/mahlburg.pdf`
10. *Нейман Х.* Многообразия групп. М.: Мир, 1974. 264 с.
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. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сиб. матем. ж. 1979. Т. 40. № 3. С. 671–673.
13. *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.
14. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Докл. АН СССР. 1970. Т. 191. № 2. С. 279–282.
15. *Матиясевич Ю. В.* Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. матем. 1971. Т. 35. № 1. С. 3–30.
16. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Наука, 1993. 223 с.
17. *Shpilrain V. and Zapata G.* Using decision problems in public key cryptography // Groups. Complexity. Cryptology. 2009. V. 1. P. 33–40.
18. *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.
19. *Shpilrain V. and Zapata G.* Combinatorial group theory and public key cryptography // Applicable Algebra in Engineering Communication and Computing. 2006. V. 17. P. 291–302.
20. *Kurt Y.* A new key exchange primitive based on the triple decomposition problem // Preprint: `http://eprint.iacr.org/2006/378`
21. *Birget J.-C., Magliveras S., and Sramka M.* On public-key cryptosystems based on combinatorial group theory // Tatra Mountains Math. Publ. 2006. V. 33. P. 137–148.

22. *Новиков П. С.* Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Труды Матем. ин-та АН СССР. 1955. Т. 44. С. 3–143.
23. *Новиков П. С.* Неразрешимость проблемы сопряженности в теории групп // Изв. АН СССР. Сер. матем. 1954. Т. 18. № 6. С. 485–524.
24. *Адян С. И.* Неразрешимость некоторых алгоритмических проблем в теории групп // Труды Моск. матем. общества. 1957. Т. 6. С. 231–298.
25. *Ремесленников В. Н., Романьков В. А.* Теоретико-модельные и алгоритмические вопросы теории групп // Итоги науки и техн. Алгебра. Геометрия. Топология. Т. 21. М.: ВИНИТИ, 1983. С. 3–79.
26. *Адян С. И., Дурнев В. Г.* Алгоритмические проблемы для групп и полугрупп // Успехи матем. наук. 2000. Т. 55. С. 3–94.
27. *Miller III C. F.* Decision problems for groups — survey and reflections // Algorithms and Classification in Combinatorial Group Theory. Berlin, Heidelberg, New York: Springer Verlag, 1992. P. 1–60.
28. *Sims C. C.* Computation with finitely presented groups. Cambridge: Cambridge Univ. Press, 1994. 604 p.
29. *Holt D. F., Eick B., and O'Brien E. A.* Handbook of computational group theory. London: Chapman & Hall/CRC, 2005. 414 p.
30. *Detinko A., Eick B., and Flannery D.* Computing with matrix groups // London Math. Soc. Lect. Notes Ser. 2011. V. 387. P. 256–270.
31. *Михайлова К. А.* Проблема вхождения для прямых произведений групп // Докл. АН СССР. 1958. Т. 119. С. 1103–1105.
32. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Лань, 2009. 288 с.
33. *Курош А. Г.* Теория групп. М.: Физматгиз, 2008. 808 с.
34. *Garside F. A.* The braid group and other groups // Quart. J. Math. 1969. V. 20. No. 78. P. 235–254.
35. *Gebhardt V.* Conjugacy search in braid groups from a braid-based cryptography point of view // Applicable Algebra in Engineering Communication and Computing. 2006. V. 17. P. 219–238.
36. *Gebhardt V.* A new approach to the conjugacy problem in Garside groups // J. Algebra. 2005. V. 292. P. 282–302.
37. *Petrides G.* Cryptoanalisis of the public key cryptosystem based on the word problem on the Grigorchuk groups // LNCS. 2003. V. 2898. P. 234–244.
38. *Magyarik M. R. and Wagner N. P.* A public key cryptosystem based on the word problem // LNCS. 1985. V. 196. P. 19–36.
39. *Fine B., Habeeb M., Kahrobaei D., and Rosenberger G.* Survey and open problems in non-commutative cryptography // JP J. Algebra, Number Theory and Applications. 2011. V. 21. P. 1–40.
40. *Papadimitriou C.* Computation complexity. Boston: Addison-Wesley, 1994. 523 p.
41. Computational complexity theory / eds. S. Rudich and A. Wigderson. Amer. Math. Soc. Institute for Advanced Study, IAS/Park City Math. Series. V. 10. Providence, RI: Amer. Math. Soc., 2004. 389 p.
42. *Gurevich Y.* Average case comleteness // J. Comput. Syst. Sci. 1991. V. 42. P. 346–398.
43. *Levin L.* Average case complete problems // SIAM J. Comput. 1986. V. 15. P. 285–286.
44. *Kapovich I., Myasnikov A., Shupp P., and Shpilrain V.* Average-case complexity and decision problems in group theory // Adv. Math. 2005. V. 190. P. 343–359.

45. *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.
46. *Celler F., Leedham-Green C. R., Murray S. H., et al.* Generating random elements of a finite group // Comm. Algebra. 1995. V. 23. No. 3. P. 4931–4948.
47. *Borovik A., Myasnikov A., and Shpilrain V.* Measuring sets in infinite groups // Contemp. Math. V. 298. Providence, RI: Amer. Math. Soc., 2002. P. 21–42.
48. *Klee V. and Minty G.* How good is the simplex algorithm? // Inequalities. Proc. Third. Symp., Univ. California. California: Academic Press, 1972. P. 159–175.
49. *Хачиян Л. А.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. № 5. С. 1093–1096.
50. *Вершик А. М., Спорышев П. В.* Ограничение среднего числа шагов в симплекс-методе и проблемы асимптотической интегральной геометрии // Докл. АН СССР. Т. 271. № 5. С. 1044–1048.
51. *Smale S.* On the average number of steps of the simplex method of linear programming // Math. Programming. 1983. V. 27. P. 241–262.
52. *Gilman R., Myasnikov A. G., Miasnikov A. D., and Ushakov A.* Report on generic case complexity // Вестник Омского университета. Спец. вып.: Комбинаторные методы алгебры и сложность вычислений. 2007. С. 103–110.
53. *Cook S. A. and Mitchell D. G.* Finding hard instances of the satisfiability problem: A survey // Satisfiability problem: Theory and Applications. V. 35. Providence, RI: Amer. Math. Soc., 1997. P. 1–17.
54. *Kellerer H., Pferschy U., and Pisinger D.* Knapsack Problems. Berlin, New York: Springer Verlag, 2004. 546 p.
55. *Ерофеев С. Ю.* Диофантовость дискретного логарифма // Прикладная дискретная математика. Приложение. 2011. № 4. С. 31–32.
56. *Ерофеев С. Ю.* Диофантовость дискретного логарифма // Вестник Омского университета. 2010. № 4. С. 13–15.
57. *Goldreich O.* Foundations of cryptography. Cambridge: Cambridge Univ. Press., 2001. V 1. 451 p.; 2004. V. 2. 798 p.
58. *Ерофеев С. Ю.* Схемы построения двушагово односторонних функций // Вестник Омского университета. 2011. № 4. С. 15–18.
59. *Рыбалов А. Н.* О генерической неразрешимости десятой проблемы Гильберта // Вестник Омского университета. 2011. № 4. С. 19–22.
60. *Тимошенко Е. И.* Эндоморфизмы и универсальные теории разрешимых групп. Новосибирск: Изд-во НГТУ, 2011. 327 с.
61. *Myasnikov A., Roman'kov V., Ushakov A., and Vershik A.* The word and geodesic problems in free solvable groups // Trans. Amer. Math. Soc. 2010. V. 362. P. 4655–4682.
62. *Vassileva S.* Polynomial time conjugacy in wreath products and free solvable groups // Groups. Complexity. Cryptology. 2011. V. 3. P. 105–120.
63. *Романовский Н. С.* О некоторых алгоритмических проблемах для разрешимых групп // Алгебра и логика. 1974. Т. 13. № 1. С. 26–34.
64. *Тимошенко Е. И.* Алгоритмические проблемы для метабелевых групп // Алгебра и логика. 1973. Т. 12. № 2. С. 232–240.
65. *Носков Г. А.* О сопряженности в метабелевых группах // Математические заметки. 1982. Т. 31. № 4. С. 495–507.
66. *Вентура Э., Романьков В. А.* Проблема скрученной сопряженности для эндоморфизмов метабелевых групп // Алгебра и логика. 2009. Т. 48. № 2. С. 157–173.

67. *Baumslag G., Cannonito F., and Robinson D. J. S.* The algorithmic theory of finitely generated metabelian groups // Trans. Amer. Math. Soc. 1994. V. 344. P. 629–648.
68. *Groves J. R. J. and Miller III C. F.* Recognizing free metabelian groups // Illinois J. Math. 1986. V. 30. No. 2. P. 246–254.
69. *Baumslag G., Mikhailov R., and Orr K. E.* A new look at finitely generated metabelian groups // arXiv math. Group Theory. 2012. No. 1203.5431. 17 p.
70. *Hall P.* Nilpotent groups // Canad. Math. Cong. Summer Sem. Vankuver: University of Alberta, 1957. P. 12–30.
71. *Холл М.* Теория групп. М.: ИЛ, 1962. 467 с.
72. *Stroud P.* Ph. D. Thesis. Cambridge, 1966. 121 p.
73. *Segal D.* Words: notes on verbal width in groups // London Math. Soc. Lect. Notes. V. 361. Cambridge: Cambridge Univ. Press, 2009. 215 p.
74. *Алламбергенов Х. С., Романьков В. А.* Произведения коммутаторов в группах // Докл. АН Уз. ССР. 1984. Т. 4. С. 14–15.
75. *Jones J.* Universal diophantine equation // J. Symbolic Logic. 1982. V. 47. No. 3. P. 549–571.