Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение
высшего профессионального образования
Омский государственный университет
им. Ф.М. Достоевского

В.А. РОМАНЬКОВ

АЛГЕБРАИЧЕСКАЯ КРИПТОГРАФИЯ

Монография

ИЗДАТЕЛЬСТВО
ОМСКОГО ГОСУДАРСТВЕННОГО
УНИВЕРСИТЕТА

2013

УДК 519.725
ББК 22.14+32.811.4
Р698

Рекомендовано к изданию
редакционно-издательским советом ОмГУ
Рецензенты:
д-р физ.-мат. наук, проф. А. Г. Мясников;
д-р техн. наук, проф. Р. Т. Файзуллин

Романьков В. А.

Р698 Алгебраическая криптография: монография. – Омск: Изд-во Ом. гос ун-та, 2013. – 136 с.

ISBN 978-5-7779-1600-6

Монография содержит авторское изложение одного из современных направлений исследований – криптографии, основанной на группах (в английской терминологии – *group-based cryptography*). Ее более общее название обусловлено тем, что за последнее время кроме теоретико-групповых платформ в криптографии стали широко использоваться другие алгебраические системы – алгебры, кольца, лупы и т. п. Объясняются основы теории, содержатся описания некоторых систем шифрования и криптографических протоколов. Ядро составляет криптографический анализ целого ряда известных криптографических схем. Анализ базируется на авторском методе атаки с использованием линейной разложимости, эффективной во многих случаях, когда платформа является частью конечномерной алгебры над конструктивным (в частности, конечным) полем. Отличительной чертой метода служит тот факт, что выработанный на его основе алгоритм не вычисляет секретные параметры (ключи), использованные при скрытии результата (разделенного ключа или передаваемого в зашифрованном виде текста), а восстанавливает сам результат. Представлена Диофантова криптография. Показана универсальность Диофантова языка, на котором можно записывать многие известные классические криптографические схемы, в том числе схемы, использующие дискретный логарифм и RSA. Намечены пути развития Диофантовой криптографии на группах. Приведены соотвествующие примеры протоколов.

Для специалистов в криптографии и алгебре, студентов, магистрантов и аспирантов, изучающих криптографию, преподавателей курсов криптографии и ее приложений в защите информации.

Издание монографии поддержано Министерством образования и науки Российской Федерации, проекты 14.B37.21: 0359 и 0859.

УДК 519.725
ББК 22.14+32.811.4

ISBN 978-5-7779-1600-6

Содержание

§ 4. Анализ схем криптографии, основанной на группах

§ 5. Анализ некоторых схем криптографии на алгебраических платформах

§ 6. Диофантова криптография

Предисловие

Понятие «криптография, основанная на группах» (английский вариант – «group-based cryptography») появилось сравнительно недавно – на рубеже 20-го и 21-го 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 [111], [112], а также множество статей, затрагивающих самые разные вопросы. Часть из этих статей представляет криптографические примитивы, другая описывает криптографические системы и протоколы, третья исследует вопросы сложности и т. д. Часть работ посвящена вскрытию слабостей представленных систем и протоколов. Также имеются практические разработки, в том числе компьютерные программы, для использования полученных результатов на практике. Обширный список работ по данному направлению можно найти по адресу [123].

В настоящей книге дается краткое представление о криптографии, основанной на группах, обсуждается возможность использования неразрешимых и трудноразрешимых алгоритмических проблем теории групп в качестве основы для построения криптографических систем и протоколов. Приводятся основные проблемы такого сорта и протоколы с их использованием.

Также в книге дается криптографический анализ целого ряда схем (систем или протоколов) криптографии, основанной на группах. Анализ базируется на оригинальном методе линейной разложимости. Условием применения метода является реализация схемы в конечномерной алгебре над полем. Поле предполагается конструктивным. Это означает, что его элементы допускают эффективную запись, а полевые операции над этими записями также выполняются эффективно. В этом смысле все конечные поля конструктивны. Заметим, что абсолютное большинство из

предлагаемых платформ в криптографии, основанной на группах, именно такие.

Атака с применением метода линейной разложимости проста и во многих случаях эффективна. Она позволяет эффективно за полиномиальное время находить секретные результаты криптографических схем. Это могут быть разделенные или переданные ключи, исходные тексты для данных зашифрованных текстов и т. п. Алгоритм в основном сводится к решению систем линейных уравнений, что можно осуществить методом исключения Гаусса. Для метода Гаусса существуют полиномиальные временные оценки, что вкупе с естественными предположениями относительно рассматриваемой криптографической схемы дает полиномиальные оценки времени работы всего алгоритма. Оценки таковы, что во многих случаях алгоритм можно считать реально осуществимым. Определяющей чертой алгоритма является то, что он не вычисляет секретные параметры, использованные в схеме, демонстрируя тем самым, что расшифровывать можно совсем не так, как было зашифровано.

По-видимому, это первый случай систематического нахождения результата (разделенного ключа, исходного текста и т. п.) без вычисления применяемых в протоколе ключей. Атака осуществляется как бы со стороны, обходя построенные защитные «редуты». В ряде случаев рассуждения авторов протоколов о стойкости протоколов становятся бесполезными, поскольку, как правило, основываются на сложности вычисления этих ключей.

Также в книге представляется новое оригинальное направление в криптографии, называемое автором «Диофантовой криптографией». Объясняется, что многие асимметричные криптографические схемы, среди которых схемы, основанные на дискретном логарифме и RSA, сводятся к Диофантовой проблеме. В этом смысле Диофантов язык можно рассматривать как универсальный язык криптографии с открытым ключом. Показано, как можно использовать алгоритмическую неразрешимость Диофантовой проблемы (10-й Проблемы Гильберта), установленную Ю.В. Ма-

тиясевичем ([20], [21], [22]), для построения криптографических протоколов на теоретико-групповой платформе. Перенос на группы осуществляется с использованием усовершенствованных старых результатов автора ([32], [33]) об интерпретации Диофантовых уравнений в группах. В основном это разрешимые группы: метабелевы или нильпотентные. Поэтому в книге обращается внимание на их структуру, приводятся некоторые необходимые факты и результаты. Даются некоторые примеры протоколов Диофантовой криптографии.

Для понимания материала достаточно знаний в объеме базовых университетских курсов по алгебре, дополненных основными понятиями криптографии.

Введение

Обычно зарождение современной криптографии с открытым ключом связывают с публикацией короткой заметки Диффи и Хеллмана [63]. В ней авторы не только впервые высказали замечательную идею открытой передачи секретных данных по незащищенным каналам связи без предварительного разделения между корреспондентами каких-либо секретов, но также представили соответствующий алгоритм, известный как *протокол Диффи-Хеллмана* разделения ключа. Протокол впоследствии сыграл не только теоретическую роль, но был реализован в различных практических схемах криптографии. Его популярность в настоящее время нисколько не убавилась. Справедливости ради следует сказать, что, по словам самого Хеллмана [79], идея подобного разделения ключа принадлежала Мерклю, поэтому сам протокол следует именовать *протокол Диффи-Хеллмана-Меркля*.

Протокол Диффи-Хеллмана-Меркля (для краткости – DHM) работает следующим образом:

- Двое корреспондентов, скажем, Алиса и Боб, выбирают конечную группу G и некоторый элемент g этой группы. При выборе Алиса и Боб пользуются незащищенным каналом связи, поэтому величины G и g считаются общеизвестными.

- Далее Алиса выбирает случайным образом натуральное число $k \in \mathbf{N}$, вычисляет элемент g^k и передает его по открытому каналу Бобу. Само число k считается секретным.

- Боб поступает аналогично: выбирает $l \in \mathbf{N}$, вычисляет и передает Алисе элемент g^l. Число l считается секретным.

- Получив элемент g^l, Алиса вычисляет элемент $(g^l)^k = g^{kl}$.

- Боб делает то же самое, получая g^k и вычисляя $(g^k)^l = g^{kl}$.

- Элемент g^{kl} считается разделенным секретным ключом.

Реализация DHM должна быть такой, чтобы вычисление по данным G, g^k, g^l разделенного ключа g^{kl} было трудной вычислительной задачей. Эту задачу называют *проблемой Диффи-Хеллмана* (DHP). Она тесно связана с проблемой дискретного логарифма (DLP): по фиксированному элементу g известной конечной группы G и его степени $f = g^t, t \in \mathbf{N}$, определить число t, которое называется *дискретным логарифмом* элемента f относительно базы g и обозначается $\log_g f$. При ограничении $0 \leq t \leq \mathrm{ord}(g)$, где $\mathrm{ord}(g)$ обозначает порядок элемента g (в дальнейшем через $\mathrm{ord}(G)$ мы обозачаем порядок группы (G)), дискретный логарифм $t = \log_g f$ определен однозначно. Обычно в качестве элемента g берется порождающий элемент конечной циклической группы $G = gp(g)$. Здесь и далее через $gp(g_1, ..., g_k)$ обозначается (под)группа, порожденная элементами $g_1, ..., g_k$. В этом случае $\log_g f$ существует для любого элемента f группы G. Если в протоколе DHM вычислить $k = log_g g^k$ или $l = log_g g^l$, то легко вычисляется и g^{kl}. Поэтому разрешимость DLP влечет разрешимость протокола DHM, то есть вычисление его конечного результата – разделенного ключа.

В оригинальной работе [63] и многих последующих работах в качестве платформ G для протокола DHM использовались мультипликативные группы $\mathbf{F}_p^*$ простых конечных полей $\mathbf{F}_p, p$ – простое, реализованных как кольца вычетов $\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$. Эти группы очень удобны для построения на них протокола DHM. Во-первых, они циклические, и поэтому при выборе в качестве g порождающего элемента группы $\mathbf{F}_p^*$ дискретный логарифм $\log_g f$ определен для любого элемента $f \in \mathbf{F}_p^*$. Во-вторых, их элементы можно записывать стандартными именами вычетов $1, 2, ..., p-1$, по которым трудно вычислять их дискретные логарифмы относительно g.

Также в качестве платформ для DHM и других протоколов, основанных на трудности разрешимости DLP, стали использоваться мультипликативные группы $\mathbf{F}_q^*$ произвольных конечных полей $\mathbf{F}_q$ порядка $q = p^r$ (p – простое) степени $r \in \mathbf{N}$ над простым конечным полем $\mathbf{F}_p$ характеристики p. Эти группы циклические, их

элементы однозначно записываются в виде многочленов из кольца $\mathbf{F}_p[x]$ степени не больше, чем $r-1$. Вычисления ведутся по модулю неприводимого многочлена $h(x) \in \mathbf{F}_p[x]$ степени r, по которому построено поле $\mathbf{F}_q \simeq \mathbf{F}_p[x]/ideal(h(x))$.

В дальнейшем в качестве платформ протоколов типа DHM стали предлагаться кроме циклических и другие конечные группы, среди которых выделились группы эллиптических кривых над конечными полями (см. [89], [90], [109]). Обозначились и бесконечные группы, прежде всего – матричные (линейные) группы над полями, кольцами, алгебрами, затем стали широко использоваться полициклические группы, группы кос Артина и т. д. Кроме групп стали предлагаться полугруппы, лупы и т. п.

Оказалось ([106], [107]), что обычная проблема дискретного логарифма в группах матриц над полями сводится к кратной проблеме дискретного логарифма в поле, содержащем все характеристические числа матрицы g, являющейся базой дискретного логарифма. Действительно, характеристические числа матрицы g^t являются t-степенями характеристических чисел матрицы g. Матрица g приводится к жордановой форме над полем $\mathbf{F}$, содержащем все эти характеристические числа. Теперь они стоят на главной диагонали. Тем же самым преобразованием матрица g^t приводится к треугольному виду с t-степенями характеристических чисел матрицы g на соответствующих местах главной диагонали. Если жорданова форма матрицы g диагональна, то становится очевидной равносильность двух обсуждаемых проблем. Если нет, то из разрешимости проблемы дискретного логарифма для матриц следует разрешимость кратной проблемы дискретного логарифма в мультипликативной группе $\mathbf{F}^*$. В данном случае две задачи не равносильны. Тем не менее, решив кратную задачу, уже не так трудно решить и матричную.

С самого начала использования некоммутативных групп появились аналоги дискретного логарифма. Наболее популярным стало употребление вместо возведения в степень сопряжения, в дальнейшем стали применяться правые и левые умножения и т. п.

На этом строится целый ряд известных протоколов. См. по этому поводу монографии [111], [112]. Базовые протоколы, основанные на трудности решения так называемых проблем поиска, в большинстве своем имитировали классические криптографические схемы Диффи-Хеллмана-Меркля, ЭльГамаля, Масси-Омуры, Фиата-Шамира и т. д., относительно которых см., например, [34], [64], [90], [105].

Автор предлагает универсальный подход к криптоанализу схем, криптостойкость которых базируется на сложности решения проблем поиска для различных алгоритмических проблем. Оказалось, что в ряде случаев, в том числе для некоторых хорошо известных протоколов, среди которых протоколы разделения ключа Ко, Ли и др. (сопряжение) [88], протокол Стикелса (двустороннее домножение) [137], другие протоколы, относительно которых см. [111], [112], итоговый секретный результат протокола (разделенный ключ или сообщение) можно получить, не решая соответствующих проблем поиска. При этом подходе применяются обычные методы линейной алгебры. Правда, такие атаки возможны, если соответствующий протокол может быть записан на платформе, представляющей из себя кольцо матриц над конечномерной алгеброй над конструктивным полем. В конечном случае это не является ограничением, поскольку можно все перевести на платформу матриц над конечным полем. Но это часто можно сделать и в бесконечном случае. Например, в случае групп кос Артина, которые, как известно [91], линейны. Группы кос Артина – один из наиболее популярных объектов в криптографии. См. обзоры [61], [66] и [100]. Также линейны (см., например, [12] или [93]) конечно порожденные нильпотентные или, более общо, полициклические группы, которые все чаще предлагаются в качестве платформ криптографических протоколов. Почти всегда предлагаемые для платформ алгебраические системы так или иначе представляются матрицами, что позволяет проводить атаку данным методом.

Дается криптографический анализ ряда других протоколов, отличительной особенностью большинства из которых служит применение в них автоморфизмов в качестве как преобразований, так и ключей. Анализ также использует обычные методы линейной алгебры. Соответствующая атака проводится без вычисления параметров криптографической схемы, результат получается совсем другим способом.

Структура книги следующая.

В § 1 кратко излагаются основные элементы криптографии, основанной на группах. Приведены необходимые требования к платформам, на которых реализуются системы шифрования и криптографические протоколы. Обсуждаются алгоритмические проблемы и способы их использования для построения криптографических примитивов. Вводятся возникающие при этом проблемы поиска. Говорится об основных типах сложности возникающих проблем.

В § 2 дается общее представление об алгебраическом шифровании.

В § 3 приводится основная идея оригинального метода линейной разложимости. Метод позволяет находить шифрованное сообщение или разделенный ключ. Соответствующий алгоритм использует обычный аппарат линейной алгебры. Метод применим при условии, что платформа, на которой строится криптографическая схема, может быть выбрана как конечномерная алгебра, например, как матричная алгебра над полем. Метод не предполагает нахождения секретных параметров, фигурирующих в схеме. Теоретические основы метода и ряд атак на его основе схем шифрования и разделения ключа, базирующихся на различных обобщениях задачи дискретного логарифма и идей Диффи-Хеллмана-Меркля на некоммутативные группы, изложены в работе автора [118]. В [36] дается развитие метода, которому находятся новые применения.

В § 4 метод используется для криптографического анализа ряда известных протоколов криптографии, основанной на группах.

Среди них протоколы Ко, Ли и др. [88], Шпильрайна и др. [125], [126], [127], Альвареса, Мартинеса и др. [45], [46], [47], а также Стикельса [137].

Следующий § 5 посвящен криптографическому анализу схем шифрования и разделения ключа, базирующихся на групповых (луповых) алгебрах и градуированных алгебрах с мультипликативным базисом, предложенных в работах Росошека [37], [38], Михалева и др. [7], [19], Махалонобиса [99] и др. Объединяет эти схемы (кроме схемы из [7]) использование в них автоморфизмов. Также приводится криптографический анализ протокола разделения ключа Мегрелишвили и Джинджихадзе [23]. Анализ использует метод линейной разложимости.

Заключительный § 6 представляет Диофантову криптографию. Даются сведения о Диофантовых уравнениях и функциях, в том числе связанные с алгоритмической неразрешимостью проблемы существования решений у Диофантовых уравнений (Диофантовой проблемой). Показывается, что многие схемы шифрования с открытым ключом, включая схемы, использующие дискретные логарифмы и схему шифрования Ривеста-Шамира-Адлемана (RSA), записываются на Диофантовом языке и тем самым сводятся к решению Диофантовой проблемы для уравнений определенного вида. Показано, как с помощью интерпретации Диофантовых уравнений в группах (в частности, в свободных метабелевых группах) переносить неразрешимость Диофантовой проблемы на теоретико-групповые платформы. В этой связи дается описание структуры свободной метабелевой группы произвольного конечного ранга. Определяется проблема эндоморфной сводимости, обсуждается ее алгоритмическая неразрешимость в некоторых разрешимых группах. Это дает основание для построения криптографических систем и протоколов на платформах разрешимых групп. Приводится пример такого протокола аутентификации. Обсуждаются детали его построения.

§ 1. Криптография, основанная на группах

1.1. Платформы шифрования

В данном разделе криптографии в качестве платформ для систем шифрования и криптографических протоколов используются группы. Они могут быть конечными или бесконечными, могут задаваться разными способами. В то же время они не могут быть произвольными и должны удовлетворять некоторым естественным требованиям общего характера. Для обоснования возможности использования группы в качестве платформы шифрования или криптографического протокола обратим 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. [48], в которой была 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 [48] в качестве платформы бралась группа кос Артина B_n на n нитях для достаточно большого n.

В качестве алгоритмической в ней рассматривалась проблема сопряженности в группе B_n двух наборов элементов $\bar{g} = (g_1, ..., g_k)$ и $\bar{f} = (f_1, ..., f_k)$. Алгоритм может быть представлен в любой группе. Конкретный ее 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 говорится более подробно в дальнейшем. Здесь мы опишем сам алгоритм в его общем виде.

Пусть G – конечно порожденная группа с множеством порождающих элементов $\{x_1, ..., x_n\}$, которое можно считать фиксированным. Любой элемент группы G записывается в виде группового слова от порождающих элементов. *Групповым* называется слово, записанное от букв $x_1, ..., x_n$ и формальных обратных $x_1^{-1}, ..., x_n^{-1}$. 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 $\{x_1, ..., x_n\}$, 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 ее элементов. Это означает, что любой элемент может быть однозначно записан в виде канонического слова от порождающих элементов. Переход от произвольной записи элемента $g = g(x_1, ..., x_n)$ 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 $\{x_1, ..., x_n\}$ – это обычный процесс сокращения подслов вида $x_i^{\varepsilon} x_i^{-\varepsilon}$, о которых говорилось выше. Известно, что результат – несократимое слово – не зависит от выбора порядка сокращения.

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

Предполагается, что в группе G вычисление по опубликованным нормальным формам сопрягающих наборы элементов u и v – трудная задача. На этом основывается криптостойкость протокола. После выхода статьи [48] появилось множество статей с анализом этой криптостойкости. Подчеркивалась важность выбора параметров, ключей и т. п. Появились соответствующие рекомендации и т. п.

На выходе протокола корреспонденты получают секретный ключ. Делается это следующим образом. Алиса вычисляет элемент

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

Боб вычисляет тот же самый элемент $[v, u]$ из равенства

$$v \cdot v(\text{нф}(f_1^u), ..., \text{нф}(f_k^u))^{-1} = [v, u]. \qquad (2)$$

Таким образом Алиса и Боб 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 [48] в качестве платформы своего протокола. Относительно этих свойств см. классическую работу А.А. Маркова [18], монографию Дехорноя [60],

обзор В.Я. Лина [16] и иные монографии, посвященные группам кос Артина.

О криптографии на группах кос Артина, включая подробное описание протокола Аншель-Аншеля-Голдфельда, см. обзоры Дехорноя [61], Гарбера [66] и Мальбурга [99].

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

- Группы B_n при любом n являются конечно определенными, 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 B_n нахождение сопрягающего элемента u по элементу g и нормальной форме $\text{нф}(g^u)$ сопряженного к нему элемента является трудноразрешимой задачей. Более того, она остается трудноразрешимой при замене одного элемента на набор элементов.

Отмеченные свойства так или иначе присутствуют в большинстве работ такого сорта. Хочется еще заметить, что в работе [48] 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.

Выбор платформ в некотором классе $\mathcal{K}$ групп и соответствующей алгоритмической проблемы $\mathcal{A}$ является важной задачей. И прежде всего необходимо предложить класс $\mathcal{K}$. Также важен способ случайного выбора элемента в классе $\mathcal{K}$. Отметим, что в

настоящее время наиболее популярными для $\mathcal{K}$ являются классы конечных групп, конечных p-групп (p – простое), а также полициклических, метабелевых и матричных групп. В качестве $\mathcal{A}$ рассматривают проблемы равенства, сопряженности, вхождения, эндоморфной сводимости.

Например, в совместной с С.Ю. Ерофеевым работе автора [11] даны конкретные предложения. В качестве платформы для построения криптографических примитивов, систем и протоколов выбираются свободные метабелевы группы. *Свободная метабелева группа* M_n ранга n, где n – натуральное число, определяется как фактор группа F_n/F_n'' свободной группы F_n ранга n по второму коммутанту F_n''. Напомним, что коммутантом G' произвольной группы G называется ее подгруппа, порожденная 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 фактор группы G/G'. Отсюда ее название.

Группа M_n называется *свободной метабелевой группой ранга* n, потому что в ней есть *базис* $X_n = \{x_1, ..., x_n\}$, состоящий из n элементов, такой, что любое отображение этого базиса $X_n \to G$ в произвольную метабелеву группу G однозначно продолжается до гомоморфизма $M_n \to G$. Также говорят, что группа M_n – *свободная группа ранга* n *многообразия всех метабелевых групп* $\mathcal{A}^2$. Базис X_n еще называют *множеством свободных порождающих* группы M_n. О многообразиях групп см. монографию Х. Нейман [26].

В качестве алгоритмической проблемы мы в данном случае возьмем проблему $E(M_n)$ эндоморфной сводимости в группе M_n. Известно ([32], [33]), что она алгоритмически неразрешима при достаточно большом $n \geq n_0$. Основываясь на алгоритмической неразрешимости проблемы $E(M_n)$ при $n \geq n_0$, мы 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, мы предложим протокол аутентификации с нулевым разглашением пользователя в системе. Подобный протокол уже предлагался в [73], причем также со ссылкой на работу автора [33]. Однако, так просто воспользоваться группами и функциями из [33] в данном случае нельзя. Далее 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 $n \geq n_0$, установленная в [33], базируется на алгоритмической неразрешимости 10-й Проблемы Гильберта о существовании алгоритма, определяющего по произвольному уравнению вида $d(\zeta_1, ..., \zeta_k) = 0$, где $d(\zeta_1, ..., \zeta_k)$ – многочлен с целыми коэффициентами, имеет ли это уравнение решение в целых числах. Алгоритмическая неразрешимость 10-й Проблемы Гильберта установлена Ю.В. Матиясевичем в [20] (полное доказательство в [21], см. также [22]).

В § 6 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 конечных полей. Диофантов язык позволяет объединять эти системы и протоколы в единое целое, что позволяет нам 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 [111] и [112], обзор [61], статьи ([53], [92], [130], [132], [131]).

1.2. Бесконечные группы и алгоритмические проблемы

Мы будем рассматривать 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. Классические алгоритмические проблемы равенства, сопряженности, изоморфизма впервые были поставлены М. Деном в начале 20-го столетия. Дальнейшее развитие теории групп и теории вычислимости выработало множество алгоритмических проблем. Были получены ставшие классическими результаты об их алгоритмической разрешимости и неразрешимости. Отметим работы П.С. Новикова [27], [28], где впервые были получены примеры конечно определенных групп с неразрешимой проблемой равенства, а также работу С.И. Адяна [1], в которой был указан большой спектр алгоритмических проблем, неразрешимых в классе всех конечно определенных групп. Относительно этих и других результатов в данной области см., например, обзоры [2], [30], [108], [119].

1.2.1. Постановка алгоритмических проблем

В самых общих чертах алгоритмическая проблема выглядит следующим образом. Пусть 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, или нет. 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, ее элементы, подгруппы, подмножества, словом, объекты, для которых ставится проблема, заданы каким-либо эффективным образом. Способов эффективного задания существует довольно много. Далее мы опишем некоторые из них.

Как уже отмечалось выше, классические алгоритмические проблемы теории групп сформулированы в начале 20-го столетия Максом Деном. Они ставились им для класса конечно определенных групп.

Это означает, что группа G, для которой ставится проблема, задана своим *конечным представлением* вида

$$\mathcal{P}(G) =< x_1, ..., x_n | r_1, ..., r_m > . \tag{3}$$

Иначе говоря, группа G является фактор группой F_n/R свободной группы F_n с базисом (множеством свободных порождающих элементов) $\{x_1, ..., x_n\}$ относительно *нормального замыкания* $R = \text{нз}(r_1, ..., r_m)$, то есть минимальной нормальной подгруппы группы F_n, содержащей элементы $r_1, ..., r_m$. Элементы $r_1, ..., r_m$ записываются в виде групповых слов от порождающих $x_1, ..., x_n$. Напомним, что групповое слово записывается как слово от элементов $x^{\pm 1}, ..., x_n^{\pm 1}$. Элементы $r_1, ..., r_m$ называются *определяющими словами*. Иногда представление (3) записывают в виде

$$\mathcal{P}(G) =< x_1, ..., x_n | r_1 = 1, ..., r_m = 1 > . \tag{4}$$

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

Элементы нормального замыкания множества определяющих слов $R = \text{нз}(r_1, ..., r_m)$ допускают описание в виде групповых слов следующего вида:

$$u = \prod_{j=1}^{k} (r_{i_j}^{g_j})^{\varepsilon_j}, \tag{5}$$

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

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 $i = 1, ..., n$. Любой элемент g группы G можно поэтому записать в виде группового слова $g = g(y_1, ..., y_n)$. Однако, часто порождающие y_i группы G обозначают теми же буквами x_i, что и их прообразы. Элемент g тогда записывается в виде $g(x_1, ..., x_n)$.

Классические алгоритмические проблемы Дена формулируются следующим образом.

- **Проблема равенства.** Определить по двум групповым словам от порождающих элементов $g = g(x_1, ..., x_n)$ и $f = = f(x_1, ..., x_n)$, записывают ли они один и тот же элемент группы G, заданной своим конечным представлением (3) (или (4)). 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 $gf^{-1} =_G 1$. Также оно может быть перенесено в группу F_n, поскольку равенство $g =_G 1$ равносильно тому, что слово $g = g(x_1, ..., x_n)$ как элемент группы F_n принадлежит нормальной подгруппе R.

Как уже отмечалось, первые примеры конечно определенных групп с неразрешимой проблемой равенства были построены в 50-е годы 20-го столетия П.С. Новиковым в [27], [28]. Впоследствии таких примеров стало достаточно много. См. [108].

- **Проблема сопряженности.** Определить, задают ли два групповых слова $g = g(x_1, ..., x_n)$ и $f = f(x_1, ..., x_n)$ сопряженные элементы группы G. Другими словами, существует ли элемент h группы G такой, что $g^h =_G f$.

Разрешимость проблемы сопряженности в группе G, очевидно, влечет разрешимость в G проблемы равенства. Действительно, элемент g группы G равен 1 тогда и только тогда, когда g сопряжен с 1. Обратное утверждение в общем случае неверно. Существуют конечно определенные группы, в которых проблема равенства разрешима, а проблема сопряженности неразрешима. Первые примеры групп с неразрешимой проблемой сопряженности, некоторые из которых имеют разрешимую проблему равенства, построены в [28]. Более подробно об этом см. в [30], [108].

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

Неразрешимость проблемы изоморфизма в классе конечно определенных групп установлена С.И. Адяном [1].

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

- **Проблема вхождения.** Определить для произвольного элемента g данной конечно определенной группы G и произвольной ее конечно порожденной подгруппы H, принадлежит g подгруппе H, или нет.

Проблему вхождения еще часто называют *обобщенной проблемой равенства*. Очевидно, что ее разрешимость влечет разрешимость проблемы равенства, равносильной проблеме вхождения в тривиальную подгруппу. Выделяют также проблему вхождения в фиксированную конечно порожденную подгруппу.

Известные результаты и открытые проблемы алгоритмического характера в теории групп освещены в обзорах [2], [30], [108].

В некоторых важных классах групп классические алгоритмические проблемы разрешимы. Например, все они разрешимы в классах свободных и конечно порожденных 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 [80], [133] и обзорную статью [62].

Мы видим, что первоначально при постановке алгоритмических проблем рассматривались только конечно определенные группы, элементы которых записывались в виде групповых слов. Впоследствии класс групп, для которых стали ставиться алгоритмические проблемы, был расширен как за счет включения в него *рекурсивно определенных* групп, в которых множество порождающих элементов конечно, а множество определяющих соотношений может быть бесконечным рекурсивно перечислимым множеством. Этот класс расширился также и за счет конечно порожденных 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 – кольцом. Группа может также быть задана как конструктивный объект в смысле теории моделей. Может она определяться и другими эффективными способами.

Класс конечно порожденных матричных групп над конструктивными кольцами представляет особый интерес. Очевидно, что проблема равенства в таких группах разрешима. Однако другие проблемы даже в достаточно просто устроенных матричных группах могут быть неразрешимыми.

Одним из самых известных является пример Михайловой матричной группы с неразрешимой проблемой вхождения, описанный в работе [25]. 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 $\mathbf{Z}$. Опишем одно из возможных таких представлений. Хорошо известно (см., например, [12] или [14]), что представление (оно называется *представлением Санова*) группы F_2 матрицами порядка 2 над $\mathbf{Z}$, заданное на порождающих элементах x_1, x_2 группы F_2 следующим отображением, точное:

$$x_1 \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, x_2 \mapsto \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}. \tag{6}$$

Точное представление группы G матрицами 4−го порядка соответствует схеме

$$\begin{pmatrix} F_2 & 0 \\ 0 & F_2 \end{pmatrix}, \tag{7}$$

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−порожденной конечно определенной группы с неразрешимой проблемой равенства. Пусть такая группа K задана представлением $\mathcal{P}(K) =< x_1, x_2 | r_1, ..., r_m >$. Рассмотрим в группе G подгруппу H, порожденную элементами вида $f_1 = (x_1, x_1), f_2 = (x_2, x_2), h_i = (r_i, 1)$, для $i = 1, ..., m$. Легко показать, что элемент $g = (g', 1)$ принадлежит H тогда и только тогда, когда g' принадлежит нормальной подгруппе $R = \text{нз}(r_1, ..., r_m)$ группы F_2. Неразрешимость проблемы равенства в группе $K = F_2/R$ влечет неразрешимость проблемы вхождения в подгруппу H группы G.

Развитие алгебраической криптографии заставляет по-новому взглянуть на алгоритмические проблемы в алгебре с точки зрения их возможного применения как основы для построения криптографических схем. С одной стороны, разрешимость проблемы

еще не означает, что эта разрешимость может быть реализована практически. Многочисленные эксперименты, проведенные в 90-е годы 20-го столетия в рамках программы MAGNUS Городского университета Нью-Йорка, показали, что абсолютное большинство известных алгоритмов в комбинаторной теории групп практически не реализуемо. Для исправления ситуации нужны или их модификации, или новые алгоритмы.

1.3. Неразрешимые и трудноразрешимые алгоритмические проблемы как основа для построения криптографических схем

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 сопряженности. В уже упоминавшейся выше работе М. Аншеля и др. [48] основой криптостойкости протокола служит трудноразрешимость проблемы сопряженности в группах кос Артина. Заметим, что проблема сопряженности в них разрешима. Это установлено в работе Гарсайда [67]. Тем не менее, так как эффективный алгоритм для ее решения до сих пор не найден, эта задача продолжает считаться трудноразрешимой. См. публикации [68], [69], [131]. Проблема равенства фигурирует в работах [65], [98], [115]. Проблема вхождения – в работе [130]. Этот список – только малая часть работ, обсуждающих использование алгоритмических проблем в криптографии.

1.3.1. Проблемы поиска

Абсолютное большинство работ в криптографии, основанной на группах, в которых рассматриваются трудноразрешимые и неразрешимые проблемы, связано с решением так называемых *проблем поиска* (английский вариант – *search problems*). Например,

если в основе криптографического примитива лежит проблема сопряженности, то обычно, как это происходит, например, в протоколе Аншель-Аншеля-Голдфельда, известно, что данные элементы или наборы элементов, если речь идет 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 еще говорят – *свидетельство* этого, справедливость которого легко проверить. Например, если известно, что элемент f группы G принадлежит подгруппе H, порожденной элементами $h_1, ..., h_k$, то требуется найти запись f в виде группового слова от этих элементов. Для проблемы равенства, аналогично, требуется найти выражение слова $u = u(x_1, ..., x_n)$ от порождающих элементов $x_1, ..., x_n$ свободной группы F_n, записывающего тривиальный элемент группы $G = F_n/R$, где $R = \text{нз}(r_1, ..., r_m)$, его выражения в виде (5). Это, конечно, можно сделать простым перебором, но сейчас речь идет 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 выхода, который мы наблюдаем, значит, мы не можем организовать полиномиальный перебор возможных входов, основываясь на такой оценке. Ели же основная алгоритмическая проблема неразрешима, то мы не можем 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 [112].

1.4. О сложности алгоритмических проблем и соответствующих им проблем поиска

1.4.1. Виды сложности

Современная теория сложности зародилась в 70-е годы 20-го столетия. Для нас особую важность 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 мы должны обратить внимание на то, что при практическом использовании разрабатываемых протоколов различные входящие в них параметры, в том числе ключи, будут выбираться случайным образом. Значит, нам 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 понятия *сложности в среднем* и понятия *генерической сложности*. Перейдем к общему схематическому описанию, отсылая за деталями к монографиям [111], [112], [114], сборнику [57] и статьям [76], [84], [85], [94].

Итак, мы рассматриваем три основных вида сложности.

- Сложность по худшему случаю.
- Сложность в среднем.
- Генерическая сложность.

Относительно классического понятия сложности по худшему случаю см., например, монографию [114]. Класс сложности $\mathcal{C}$ определяется спецификацией модели вычислений (для нас это многоленточная машина Тьюринга), типом вычислений (то есть ис-

пользованием либо детерминированной, либо вероятностной машины Тьюринга), а также ресурсами, объем 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 объем 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 ее определения необходимо, чтобы на пространстве всех возможных входов была задана функция распределения вероятностей, или хотя бы какая-нибудь аддитивная неотрицательная функция. При ее задании сложность в среднем чаще всего оценивается математическим ожиданием объема 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 путем. Уже давно стало понятным, что при учете алгебраической структуры группы ее элементы как бы становятся «неравноправными». См. по этому поводу [56].

В работе [55] предложен следующий возможный общий подход к построению обсуждаемого распределения на бесконечной конечно порожденной группе. Пусть группа G наделена функцией натуральнозначной длины $l : G \to \mathbf{N}$ такой, что множество $\mathbf{S}_r$ всех

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

Обычно в качестве значения $l(g)$ функции длины l на элементе g конечно порожденной группы G с фиксированным конечным множеством X порождающих элементов берется 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 этой метрики 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 $f : \mathbf{N} \cup \{0\} \to [0, 1]$. Во-вторых, алгоритм может оказаться таким, что он работает чрезвычайно долго только на малой доле возможных входов, а на остальных входах он достаточно быстр. Усредненное 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 [87] 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 [43] имеет в основном теоретическое значение. Более точно, А.М. Вершик и П.В. Спорышев в [6] и независимо С. Смейл в [135] показали, что симплекс-алгоритм работает с линейной сложностью на множестве полной меры.

1.4.2. Асимптотическая плотность

По описанным выше причинам для нас 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 [85] представляет точное определение генерической сложности. В ней же установлено, что для широкого класса конечно порожденных групп классические алгоритмические проблемы равенства, сопряженности и вхождения имеют линейную сложность при их ограничении на некоторое генерическое подмножество. См. также работу [70].

Перейдем 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, мы можем ввести для любого неотрицательного целого числа r понятия сферы $\mathbf{S}_r$ и шара $\mathbf{B}_r$ 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* $\mathbf{S}_r$ называется отношение

$$\rho_{\mathbf{S}_r}(V) = \frac{|V \cap \mathbf{S}_r|}{|\mathbf{S}_r|}, \tag{8}$$

где $|\cdot|$ означает число элементов.

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

$$\rho_{\mathbf{B}_r}(V) = \frac{|V \cap \mathbf{B}_r|}{|\mathbf{B}_r|}, \tag{9}$$

Мы будем использовать для определения асимптотической плотности функцию (9), хотя совершенно аналогично можно дать определение, основываясь на функции (8).

Определение 1.1. *Асимптотической плотностью подмножества V моноида Σ^* называется верхний предел*

$$\rho(V) = \overline{\lim}_{r\to\infty} \rho_{\mathbf{B}_r}(V). \tag{10}$$

Если в (10) 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 $\{\rho_{B_r}(V)\}_{r\in\mathbf{N}}$. Будем говорить, что сходимость последовательности *экспоненциально быстрая*, если существуют числа $0 \le \sigma < 1$ и $C \ge 0$ такие, что для любого r имеет место оценка

$$|\tilde{\rho}(V) - \rho_{B_r}(V)| \le C\sigma^r. \tag{11}$$

Определение 1.2. *Подмножество V множества Σ^* называется генерическим, если $\tilde{\rho}(V) = 1$, и строго генерическим, если сходимость $\rho_{B_r}(V) \to_{r\to\infty} \tilde{\rho}(V)$ экспоненциально быстрая.*

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

Определения 1.1. и 1.2. легко распространяются на случай, когда вместо множества Σ^* мы рассматриваем множество $(\Sigma^*)^k$ наборов из k элементов этого множества для $k \geq 2$. *Длиной* набора $\bar{g} = (g_1, ..., g_k)$ мы считаем сумму длин

$$l(\bar{g}) = \sum_{i=1}^{k} l(g_i) \tag{12}$$

его компонент.

Можно использовать также другое определение, согласно которому

$$l(\bar{g}) = max\{l(g_i)|i = 1, ..., k\}. \tag{13}$$

Часто алгоритмические проблемы в группах трактуют как подмножества вида

$$D \subseteq (\Sigma^*)^k \tag{14}$$

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 сопряженности 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, порожденной элементами $h_1, ..., h_{k-1}$, имеет вид:

$$D_H(G) \subseteq (\Sigma^*)^k, D_H = \{(u, h_1, ..., h_{k-1})\}, \tag{15}$$

где u определяет элемент подгруппы H.

При этом подгруппа H считается фиксированной. Можно считать также, что фиксировано множество $\{h_1, ..., h_{k-1}\}$ порождающих ее элементов. В этом случае на вход работы алгоритма должно подаваться слово u. Если рассматривать проблему вхождения в группе G, то элементы $h_1, ..., h_{k-1}$ 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 порожденных групп.

Определение 1.3. *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 определенным, то есть он может оказаться неопределенным на некоторых входах, которые можно включить в дополнение V' генерического множества V из Определения 1.3. 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 [58], [86]. 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 будет применим и будет достаточно быстр. Такой алгоритм может быть использован в практических приложениях.

§ 2. Алгебраическое шифрование

2.1. Новое направление в криптографии

Итак, сравнительно недавно появилось новое направление в криптографии, отличительной особенностью которого является использование в качестве платформ бесконечных некоммутативных групп. Основы этого направления изложены в монографиях А. Мясникова, В. Шпильрайна и А. Ушакова [111], [112]. Часто используют термин *криптография, базирующаяся на группах* (*group based cryptography*). Я предпочитаю применять термин *алгебраическая криптография*, имея в виду, что в настоящее время не только группы, но и другие алгебраические системы все чаще используются в качестве платформ криптографических схем.

Новое направление открывает новые возможности и ставит новые задачи.

Очень важен выбор класса абстрактных групп, используемых в качестве платформы. Интуитивно ясно, что эти группы должны быть наделены каноническими формами записи их элементов. По-видимому, процесс переписки произвольного элемента, записанного в виде группового слова от порождающих элементов, в каноническую форму должен быть эффективным. Криптостойкость должна основываться на каких-то трудноразрешимых задачах в этих группах.

Вернемся к представлению схемы Аншель-Аншеля-Голдфельда [48]. Теперь мы обращаем внимание на предложенный в [48] класс платформ, а именно группы кос Артина. В настоящее время это весьма популярная тема. Группы кос Артина достаточно хорошо изучены, в них можно эффективно выполнять вычисления разного толка. В то же время существуют трудноразрешимые проблемы, дающие возможность построения стойких криптосистем.

2.2. Группы кос Артина

Группы, о которых идет речь, определяются своими конечными представлениями вида

$$\mathbf{B}_n =< \sigma_1, \ldots, \sigma_{n-1} : \sigma_j\sigma_i = \sigma_i\sigma_j \qquad \text{при } |i-j| \geq 2,$$

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \qquad \text{при } |i-j| = 1 >,\ n \geq 2.$$

Очевидно, что естественное отображение группы $\mathbf{B}_n$ в группу $\mathbf{B}_{n+1}$, сопоставляющее порождающим элементам $\sigma_1, \ldots \sigma_{n-1}$ точно так же обозначенные порождающие элементы группы $\mathbf{B}_{n+1}$, является вложением. Таким образом, группы $\mathbf{B}_2, \ldots, \mathbf{B}_n, \ldots$ образуют индуктивную возрастающую систему. В ней группа $\mathbf{B}_2$ – бесконечная циклическая, группы $\mathbf{B}_n$ при $n \geq 3$ уже некоммутативны.

Существуют также геометрические определения групп кос, о которых мы здесь подробно не говорим. Из литературы о группах кос упомянем монографии [8], [18].

В группах кос можно указать однозначные формы записи их элементов. Для этого вначале индуктивно определим элементы:

$$\Delta_1 = 1, \Delta_{m+1} = \Delta_m\sigma_m\sigma_{m-1}\ldots\sigma_1.$$

Назовем косу (то есть элемент группы кос) *положительной*, если ее можно записать в качестве полугруппового слова от порождающих элементов (не включающего в запись обратных к порождающим). Пусть $\mathbf{B}_n^+$ означает полугруппу положительных кос. Оказывается, что любую косу $b \in \mathbf{B}_n$ можно однозначно записать в виде $b = \Delta_n^k \cdot c$, где $k \in \mathbf{Z}$ – максимально возможный показатель, а элемент c принадлежит $\mathbf{B}_n^+$. Существует очевидный гомоморфизм группы $\mathbf{B}_n$ в группу подстановок $\mathbf{S}_n$. Оказывается, что можно выбрать такие элементы $b_1, ..., b_l$ полугруппы $\mathbf{B}_n^+$, $l = n!$, образы которых взаимно однозначно соответствуют элементам группы $\mathbf{S}_n$. Такие косы называются *простыми*. Каждая коса $b \in \mathbf{B}_n$ допускает единственное разложение вида $b = \Delta_n^k b_{i_1} \ldots b_{i_t}$, где $k \in \mathbf{Z}$ максимально, $b_{i_1}, \ldots, b_{i_t}$ – простые косы. Значит, *канонической формой*

элемента b можно считать набор $(k, b_{i_1}, \dots b_{i_t})$. Важно отметить, что геометрическая структура, связанная с каноническими формами, является автоматной. Это, в частности, означает, что процесс переписки в каноническую форму не более, чем квадратичен.

2.3. Схема Аншель-Аншеля-Голдфельда [48] (см. также [49])

В работе [48] предложена следующая схема генерации ключа.

Установка.

Корреспонденты Алиса и Боб выбирают (открыто) группу $\mathbf{B}_n$. Кроме этого они выбирают (также открыто) два набора элементов:

$$a_1, \dots, a_k \in \mathbf{B}_n, c_1, \dots, c_l \in \mathbf{B}_n.$$

Алгоритм

Вначале Алиса выбирает секретный случайный элемент $u = u(a_1, \dots, a_k)$ и вычисляет набор элементов $c_1' = uc_1u^{-1}, \dots, c_l' = uc_lu^{-1}$. При этом Алиса публикует (открыто посылает Бобу) нормальные формы элементов $c_1', \dots, c_l'$.

Боб аналогичным образом выбирает секретный элемент $v = v(c_1, \dots, c_l)$, вычисляет нормальные формы элементов $a_1' = va_1v^{-1}, \dots, a_k' = va_kv^{-1}$ и посылает их в открытом виде Алисе.

Далее Алиса вычисляет нормальную форму элемента

$$w_A = uu(a_1', \dots, a_k')^{-1} = uvu^{-1}v^{-1} = [u, v].$$

В свою очередь, Боб вычисляет нормальную форму элемента

$$w_c = vv(c_1', \dots, c_l')^{-1} = vuv^{-1}u^{-1} = [v, u] = [u, v]^{-1}.$$

Секретный ключ, известный теперь обоим корреспондентам, есть элемент $[u, v]$.

Криптостойкость системы основана на трудноразрешимой задаче нахождения по нормальной форме элемента вида xdx^{-1} и

элементу d сопрягающего элемента x. Иногда такую проблему называют «проблемой сопряженности». Но это не совсем точно. Классическая проблема сопряженности для группы G есть поиск ответа на вопрос: сопряжены ли два произвольных элемента $g, f \in G$? В данном случае мы заранее знаем, что элементы a_i' и a_i (c_j' и c_j) сопряжены ($i = 1, \ldots, k$; $j = 1, \ldots, l$). Необходимо найти сопрягающий элемент. То есть это одна из проблем поиска, о которых говорилось выше. О трудности данной проблемы поиска сопрягающего элемента можно говорить только при правильном выборе как элементов $a_1, \ldots a_k, c_1, \ldots, c_l$, так и элементов u, v. Ряд математиков считают, что эта проблема вычислительно трудна в общем случае. Автор скорее придерживается скептического взгляда на возможность использования групп кос в качестве платформ для шифрования, по крайней мере, в предложенных ранее вариантах. Более подходящими для этой цели он считает бесконечные нильпотентные и разрешимые группы с хорошими каноническими формами элементов (например, свободные нильпотентные и свободные разрешимые группы достаточно высоких степеней).

2.4. Другие схемы

Считается, что криптостойкость базового протокола DHM и целого ряда других протоколов, использующих дискретные логарифмы в конечных полях, базируется на трудности решения DLP в мультипликативных группах этих полей. Действительно, эффективное решение DLP влечет соответствующее решение в протоколе DHM. Это означает вычисление разделенного ключа. Но верно ли обратное утверждение? Многие убеждены, что это так. Тем не менее, это утверждение остается недоказанным.

Идеи Диффи-Хеллмана-Меркля нашли свое отражение в целом ряде других протоколов. Хорошо известные – система шифрования ЭльГамаля [64] и протокол Масси-Омуры, которые можно найти почти во всех книгах по криптографии. См., например, [34], [90], [105].

Некоторые другие (отличные от мультипликативных групп конечных полей) группы также предлагаются в качестве платформ для криптографических систем и протоколов типа DHM. Среди них группы невырожденных матриц над конечными полями [59], [113], или, более общо, над групповыми алгебрами [83], над полугруппами [73] и т. д. Широко используются группы точек эллиптических кривых [34], [89], [105], [109].

Отметим, что Менезес и Ву [107] (см. также [106]) нашли полиномиальную по времени сводимость протокола DHM на матричной платформе к стандартной кратной DLP над несколькими конечными полями. В целом это позволяет считать матричный протокол DHM даже менее эффективным, чем DHM над конечным полем. Заметим, правда, что предполагается решение через решение DLP.

Одним из возможных и наиболее популярных обобщений понятия дискретного логарифма на произвольную некоммутативную группу является *проблема поиска сопрягающего элемента* (английский вариант *conjugacy search problem* (CSP)). Напомним, что сопряжение g^f элемента g обратимым элементом f определяется как $g^f = fgf^{-1}$.

- Проблема поиска сопрягающего элемента для (полу)группы G следующая: по данной паре элементов $g, f \in G$ и информации, что $g^x = f$ для некоторого обратимого $x \in G$ найти по крайней мере один элемент x с этим свойством.

CSP играет особую роль в криптографии, основанной на группах. Большинство протоколов использует различные варианты этой проблемы.

Перечислим другие естественные и наиболее популярные аналоги DLP:

- *Проблема поиска разложения (the decomposition search problem* (DSP)) для (полу)группы (алгебры, кольца) G следующая: по данным подмножествам (часто подгруппам) $A, B \subseteq$

G и двум элементам $g, f \in G$, найти два других элемента $a \in A$ и $b \in B$, удовлетворяющих равенству $a \cdot g \cdot b = f$, в предположении, что по крайней мере одна такая пара существует.

- *Проблема поиска факторизации (factorization search problem* (FSP)) для (полу)группы (алгебры, кольца) G следующая: по данному элементу $f \in G$, данным двум подмножествам (часто – подгруппам) $A, B \subseteq G$, найти два элемента $a \in A$ и $b \in B$, удовлетворяющих равенству $a \cdot b = f$, в предположении, что по крайней мере одна такая пара существует.

- *Проблема поиска сопрягающего элемента и степени (power conjugacy search problem* (PCSP)) следующая: по данным двум элементам $g, f \in G$, информации, что $(g^k)^x = f$ для некоторого $k \in N$ и некоторого элемента $x \in G$ найти по крайней мере одну такую пару (k, x).

Очевидно, что FSP есть частный случай DSP для $g = 1$.

Существует масса криптографических систем и протоколов, базирующихся на перечисленных и некоторых других аналогах DLP. Перечислим некоторые статьи, содержащие описания таких систем и протоколов:

- [82], [88], [127], [142] используют CSP;

- [48], [49], [139] используют кратную CSP;

- [128] использует скрученный вариант CSP (TCSP);

- [40], [45], [46], [47], [117], [124], [125], [126], [137] используют DSP и FSP;

- [82], [120] используют PCSP в матричных группах;

- [73] использует CSP для построения протокола аутентификации;

- [11], [73], [99] используют версии DLP с автоморфизмами или эндоморфизмами.

Многие протоколы, использующие CSP, DSP, FSP и PCSP, описаны в монографиях [111], [112]. См. также [35], представляющую Диофантову криптографию, основанную на неразрешимости Диофантовой проблемы (этой теме посвящен § 6).

Криптостойкость многих протоколов криптографии, основанной на группах, базируется на трудности решения аналогов DLP в группах, моноидах или других алгебраических системах, выбираемых в качестве платформ. Во многих случаях для этой цели предлагаются матричные группы, моноиды или другие алгебраические системы над ассоциативными алгебрами конечной размерности. Это и матричные группы над полями, и группы, допускающие точные представления матрицами над полем. Все конечные группы могут рассматриваться как матричные. Любая группа кос Артина точно представима матрицами над полем [91]. См. обзоры [61], [66] и [100] о криптографии на группах кос. Матричные группы над групповыми алгебрами конечных групп [83] или колец усеченных многочленов [142] также являются матричными над конечномерными ассоциативными алгебрами. В [51] представлено несколько предложений о построении криптографических систем, симметрических и асимметрических, базирующихся на комбинаторной теории групп и теории матричных групп.

С этого момента предполагаем, что $\mathbf{A}$ обозначает ассоциативную алгебру над конструктивным полем $\mathbf{F}$ конечной размерности $m = \dim_{\mathbf{F}} \mathbf{A}$. Также $\mathrm{M}_n(\mathbf{A})$ обозначает матричную алгебру $\mathbf{A}$ размера $n \times n$. Следовательно, $\dim_{\mathbf{F}} \mathrm{M}_n(\mathbf{A}) = mn^2$ есть размерность $\mathrm{M}_n(\mathbf{A})$ над $\mathbf{F}$.

Наша основная цель – предложить эффективную процедуру (метод, линейную атаку), вычисляющую итоговый результат (разделенный или переданный ключ) или расшифровывающую зашифрованное сообщение в системах и протоколах, базирующихся на трудности решения аналогов CSP или других проблем типа DLP в случаях, когда платформой служит подмножество (обычно

подгруппа или подмоноид) матричной алгебры $\mathrm{M}_n(\mathbf{A})$. Основная идея метода заключается в получении результата без нахождения использованных для его скрытия ключей и без нахождения сопрягающего элемента в CSP, множителей в DSP или FSP. Следовательно, мы не пытаемся решать эти проблемы в попытке раскола протокола или системы. Мы ищем обходной маневр, тайную дверь для достижения своей цели. Для реализации этой идеи используется матричная структура платформы. Конечная размерность матричной алгебры позволяет оценить временную сложность атаки. Такой подход может также применяться и в бесконечномерном случае, но, скорее всего, без верхней оценки его временной сложности. Более того, в некоторых случаях такой подход может быть использован и в нематричном случае. Это предмет дальнейших разработок и публикаций.

§ 3. Метод линейной разложимости

> You cannot trust an encryption algorithm designed by someone who had not 'earned their bones' by first spending a lot of time cracking codes'
>
> Brian Snow

3.1. Построение базиса

Пусть V – конечномерное векторное пространство над полем $\mathbf{F}$ с базисом $\mathcal{B} = \{v_1, \ldots, v_r\}$. Пусть $\mathrm{End}(V)$ – полугруппа всех эндоморфизмов пространства V. Мы предполагаем, что элементы $v \in V$ записываются как векторы относительно $\mathcal{B}$, а эндоморфизмы $a \in \mathrm{End}(V)$ записываются матрицами относительно $\mathcal{B}$. Для эндоморфизма $a \in \mathrm{End}(V)$ и элемента $v \in V$ через v^a обозначается образ элемента v относительно a. Также для любого подмножества $W \subseteq V$ и $A \subseteq \mathrm{End}(V)$ полагаем $W^A = \{w^a | w \in W, a \in A\}$, и обозначаем через $Sp(W)$ подпространство пространства V, порожденное W, а через $\langle A \rangle$ – подмоноид, порожденный A в $\mathrm{End}(V)$.

Ниже мы обсуждаем понятия сложности некоторых алгоритмов. Всюду в дальнейшем предполагается, что элементы поля $\mathbf{F}$ даны в некоторой конструктивной форме и формально определен «размер» этой формы. Более того, мы предполагаем, что операции основного поля $\mathbf{F}$ эффективны, в частности, их результаты могут быть вычислены за полиномиальное время от размеров элементов. Предполагаем, что фигурирующие в дальнейшем поля $\mathbf{F}$ удовлетворяют этим условиям. Говорим, что они *конструктивны*.

Для элемента $\alpha \in \mathbf{F}$ пишем $\|\alpha\|$, обозначая так его размер. Полагаем также $\|v\| = \max \|\alpha_i\|$ для вектора $v = (\alpha_1, \ldots, \alpha_r) \in V$, и $\|a\| = \max\{\|\alpha_{ij}\|\}$ для матрицы $a = (\alpha_{ij}) \in \mathrm{End}(V)$.

Основная лемма. *Существует алгоритм, который по данным конечным подмножествам $W \subseteq V$ и $U \subseteq End(V)$ находит базис подпространства $Sp(W^{\langle U\rangle})$ в виде $w_1^{a_1}, \ldots, w_t^{a_t}$, где $w_i \in W$ и a_i – произведение элементов из U. Более того, число полевых операций, используемых алгоритмом, полиномиально от $r = \dim_{\mathbf{F}} V$ и мощностей подмножеств W и U.*

Доказательство. Используя метод Гаусса, можно эффективно найти максимальную линейно независимую подсистему L_0 подмножества W. Справедливо равенство $Sp(L_0^{\langle U\rangle}) = Sp(W^{\langle U\rangle})$. Добавляя к системе L_0 один за другим элементы v^a, где $v \in L_0, a \in U$, и проверяя каждый раз линейную независимость расширенного множества, можно эффективно построить максимальную линейно независимую подсистему L_1 множества $L_0 \cup L_0^U$, содержащего L_0. Заметим, что $Sp(L_0^{\langle U\rangle}) = Sp(L_1^{\langle U\rangle})$ и что элементы в L_1 имеют вид w или w^a, где $w \in W$ и $a \in U$. Отсюда следует, что если $L_0 = L_1$, то L_0 – базис пространства $Sp(W^{\langle U\rangle})$. Если $L_0 \neq L_1$, то мы повторяем процедуру для $L_1 \setminus L_0$ и находим максимальную линейно независимую подсистему L_2 множества $L_1 \cup (L_1 \setminus L_0)^U$, расширяющую L_1. Продолжая таким образом, строим строго возрастающую цепочку $L_0 < L_1 < \ldots < L_i$ линейно независимых систем. Так как размерность r пространства V конечна, цепочка закончится на шаге $i \leq r$. В этом случае L_i – базис подпространства $Sp(W^{\langle U\rangle})$. Его элементы имеют требуемую форму.

Для верхней оценки числа полевых операций, используемых алгоритмом, заметим сначала, что число операций в методе Гаусса относительно матрицы размера $n \times r$ равно $O(n^2 r)$. Следовательно, требуется $O(n^2 r)$ шагов для построения L_0 из W, где $n = |W|$– число элементов в W. Заметим, что $|L_j| \leq r$ для любого j. Поэтому для нахождения L_{j+1} достаточно рассмотреть процесс исключения Гаусса относительно матрицы, соответствующей $L_j \cup L_j^U$, имеющей размер не более, чем $r + r|U|$. Таким образом, верхняя оценка на это число есть $O(r^3|U|^2)$. Так как происходит не более r итераций процесса, общая оценка выглядит как $O(r^3|U|^2 + r|W|^2)$. Конечно, такая оценка весьма грубая.

Лемма доказана.

Следствие 3.1. *При сделанных ограничениях на поле* $\mathbf{F}$ *алгоритм из Основной леммы полиномиален относительно размера входа, т. е. относительно* $r = \dim_{\mathbf{F}} V$, $|W|$, $|U|$ *и* $\max\{\|w\|, \|u\| \mid w \in W, u \in U\}$.

Сейчас мы проиллюстрируем, как может проводиться атака методом линейного разложения.

3.2. Основная идея

3.2.1. Базовая модель

Пусть теперь U_1 и U_2 – два конечных подмножества в $\mathrm{End}(V)$ таких, что каждый элемент из U_1 перестановочен с любым элементом из U_2. Пусть A и B – подмоноиды в $\mathrm{End}(V)$, порожденные U_1 и U_2 соответственно. Пусть $a \in A, b \in B$ и $v \in V$. Мы предполагаем, что U_1, U_2 и векторы v, v^a, v^b открыты, в то время как эндоморфизмы a и b секретны.

Утверждение 3.1. *Для данных* U_1, U_2, v, v^a, v^b *вектор* $v^{ab} = v^{ba}$ *находится за полиномиальное время.*

Доказательство. По данным U и v Основная лемма (и ее Следствие 3.1.) позволяют сконструировать за полиномиальное время базис подпространства $Sp(v^A)$, где A – подмоноид, порожденный U, в виде $v^{a_1}, \ldots, v^{a_t}$, где $a_i \in A, i = 1, \ldots, t$, даны как некоторые произведения элементов из U. Используя процесс Гаусса, выразим v^a, как линейную комбинацию элементов этого базиса:

$$v^a = \Sigma_{i=1}^t \alpha_i v^{a_i}, \quad \alpha_i \in \mathbf{F}.$$

Это позволяет вычислить v^{ab} следующим образом:

$$v^{ab} = (v^a)^b = (\Sigma_{i=1}^t \alpha_i v^{a_i})^b =$$

$$\Sigma_{i=1}^t \alpha_i v^{a_i b} = \Sigma_{i=1}^t \alpha_i v^{b a_i} = \Sigma_{i=1}^t \alpha_i (v^b)^{a_i}. \qquad (16)$$

Действительно, поскольку вектор v^b, матрицы a_i и коэффициенты α_i известны, правая часть равенства 16 непосредственно вычислима.

Утверждение доказано.

В заключение отметим, что у нас не было необходимости вычислять ни a, ни b, чтобы вычислить вектор v^{ab}

Отметим также, что в Утверждении 3.1 не нужно знать U_2, достаточно знать только, что для $b \in \mathrm{End}(V)$ справедливо равенство $[b, U_1] = 1$, т. е. он перестановочен с любым элементом из U_1.

3.2.2. Линейная группа, действующая сопряжением

Пусть G – конечно порожденная группа, $\phi : G \to \mathrm{GL}_n(\mathbf{A})$ – вложение, где $\mathbf{A}$ – конечномерная ассоциативная алгебра над полем $\mathbf{F}$. Как обычно, предполагаем, что элементы $\mathbf{A}$ записываются в конструктивной форме, для которой определен размер. Более того, предполагаем, что основные алгебраические операции в $\mathbf{A}$ эффективны. Значит, они могут вычисляться за время, полиномиальное от размера элементов. В частности, матричное умножение в $\mathrm{M}_n(\mathbf{A})$ осуществляется за полиномиальное время. Все эти условия соблюдены, если $\mathbf{A}$ совпадает с полем $\mathbf{F}$.

Так как группа G конечно порождена и умножение в $\mathrm{GL}_n(\mathbf{A})$ эффективно, можно вычислить за полиномиальное время образ g^ϕ любого элемента $g \in G$, записанного групповым словом от порождающих группы G.

Заметим, что $V = \mathrm{M}_n(\mathbf{A})$ можно рассматривать как конечномерную алгебру над $\mathbf{F}$, где матрицы из $\mathrm{M}_n(\mathbf{A})$ представляются как наборы из n^2 элементов из $\mathbf{A}$, т. е. элементов из $\mathbf{A}^{n^2}$. Если $\mathbf{A}$ имеет размерность r над $\mathbf{F}$, то $\mathbf{A}^{n^2}$ может рассматриваться как векторное пространство над $\mathbf{F}$ размерности rn^2, в котором сложение соответствует сложению в $\mathrm{M}_n(\mathbf{A})$. Группа $\mathrm{GL}_n(\mathbf{A})$ действует на V как левым, так и правым умножением. В обоих случаях гомоморфизм ϕ дает точное представление $\phi : G \to \mathrm{End}(V)$. Значит, любые два элемента $g, h \in G$ определяют эндоморфизм

$E_{g,h} : \mathrm{M}_n(\mathbf{A}) \to \mathrm{M}_n(\mathbf{A})$, определенный, как $E_{g,h}(x) = \phi(g)x\phi(h)$. В частности, сопряжение элементом $g \in G$ в $\mathrm{M}_n(\mathbf{A})$ соответствует эндоморфизму $E_{g,g^{-1}}$.

Теперь предположим, что U_1 и U_2 – такие конечные подмножества в G, что любой элемент из U_1 перестановочен с любым элементом из U_2. Пусть A и B – подмоноиды в G, порожденные U_1 и U_2 соответственно. Пусть $a \in A$, $b \in B$ и $g \in G$. Положим $g^a = aga^{-1}, g^b = bgb^{-1}$.

Утверждение 3.2. *Для данных U_1, U_2, g, g^a, g^b можно найти за полиномиальное время элемент $g^{ab} = g^{ba}$.*

Доказательство. Аргументы, высказанные выше, показывают, что $\phi : G \to \mathrm{M}_n(\mathbf{A})$ дает вложение $\phi : G \to \mathrm{End}(V)$ такое, что сопряжение элементом $f \in G$ определяет эндоморфизм $E_{f,f^{-1}} \in \mathrm{End}(V)$. Теперь Утверждение 3.2 прямо следует из Утверждения 3.1.

Утверждение доказано.

Есть несколько возможных способов обобщить базовую схему, описанную в данном разделе. Приведем одну из них. Некоторые другие вариации появятся в следующих параграфах.

3.2.3. Линейная группа, действующая умножениями

Предположим теперь, что $a, a' \in A$ и $b, b' \in B$.

Утверждение 3.3. *Для данных $U_1, U_2, g, agb, a'gb'$ можно найти за полиномиальное время элемент $a'agbb' = aa'gb'b$.*

Доказательство. Аргументы, аналогичные приведенным выше, сводят проблему к базовой модели.

Утверждение доказано.

Заметим, что Утверждение 3.3 справедливо также, если заменить группу G на полугруппу. Работают те же самые аргументы.

3.2.4. Линейная группа с действием автоморфизмами

Рассмотрим следующую модель. Пусть, как выше, G – группа, снабженная биективным гомоморфизмом $G \to \mathrm{GL}_n(\mathbf{A})$, где $\mathbf{A}$ – конечномерная ассоциативная алгебра над полем $\mathbf{F}$. Предположим, что Φ и Ψ – два конечных подмножества группы автоморфизмов $\mathrm{Aut}(G)$ такие, что каждый элемент $\phi \in \Phi$ перестановочен с любым элементом $\psi \in \Psi$. Пусть A и B – два подмоноида группы $\mathrm{Aut}(G)$, порожденные Φ и Ψ соответственно. Рассмотрим аналог модели из Утверждения 3.2, в котором сопряжения заменены автоморфизмами. Возникает вопрос о существовании полиномиального по времени алгоритма, который по данным $\Phi \subseteq \mathrm{Aut}(G), \Psi \subseteq \mathrm{Aut}(G)$, $g \in G$, и образам $\alpha(g)$ и $\beta(g)$ для некоторых случайных автоморфизмов $\alpha \in A, \beta \in B$ вычисляет элемент $\alpha(\beta(g)) = \beta(\alpha(g))$ в G. Здесь нет прямых редукций к моделям из Утверждений 3.1 или 3.2, так как произвольный автоморфизм из $\mathrm{Aut}(G)$ в общем случае не расширяется до эндоморфизма из $\mathrm{End}(V)$. Такая редукция возможна, если все автоморфизмы из Φ и Ψ расширяются до некоторых линейных преобразований пространства V, как это происходит в случае модели из Утверждения 3.2. Обсудим одну теоретико-групповую конструкцию, которая может оказаться полезной в рассматриваемом случае.

Напомним, что *голоморф* $H(G)$ группы G есть полупрямое произведение $H(G) = \mathrm{Aut}(G) \ltimes G$ группы автоморфизмов $\mathrm{Aut}(G)$ и группы G, где умножение элементов из $\mathrm{Aut}(G) \ltimes G$ определено, как $(\alpha, g) \cdot (\beta, h) = (\alpha \cdot \beta, \beta(g) \cdot h)$. Группы $\mathrm{Aut}(G)$ G естественно вложены в $H(G)$ биекциями $\alpha \to (\alpha, 1)$ и $g \to (1, g)$, соответственно. Заметим, что каждый автоморфизм $\alpha \in \mathrm{Aut}(G)$ действует на G сопряжением в $H(G)$, так как $(\alpha^{-1}, 1) \cdot (1, h) \cdot (\alpha, 1) = (1, \alpha(h))$. Отсюда вытекает, что если голоморф – линейная группа над полем или если существует вложение $H(G) \to \mathrm{GL}_n(\mathbf{A})$ для некоторого n и $\mathbf{A}$, как выше, то в этом случае существует естественная редукция к модели из Утверждения 3.2. Например, справедливо следующее утверждение.

Утверждение 3.4. *Пусть $H(G)$ – линейная группа. Тогда при предположениях, сделанных выше относительно $\Phi, \Psi, g, \alpha(g), \beta(g)$, можно найти за полиномиальное время элемент $\alpha(\beta(g)) = \beta(\alpha(g))$.*

Доказательство очевидно.

Заметим, что голоморф $H(G)$ линеен, если группа G конечная (очевидно) или полициклическая [24] (см. также [93], [122]).

§ 4. Анализ схем криптографии, основанной на группах

4.1. Протоколы, базирующиеся на сопряжении

Напомним, что g^f означает fgf^{-1}.

4.1.1. Протокол разделения ключа Ко, Ли и др. [88]

Пусть G – группа, U_1, U_2 – два ее конечных подмножества, элементы которых перестановочны между собой, то есть для любых $g_1 \in G_1, g_2 \in G_2$ имеем $g_1 g_2 = g_2 g_1$. Обозначим через A и B подгруппы группы G, порожденные U_1 и U_2 соответственно. Тогда любой элемент $a \in A$ перестановочен с любым элементом $b \in B$. Зафиксируем элемент $g \in G$. Мы предполагаем, что все перечисленные данные открыты.

Алгоритм. Алиса выбирает случайный элемент $a \in A$, вычисляет и пересылает элемент g^a Бобу. Тот выбирает случайный элемент $b \in B$, вычисляет и пересылает элемент g^b Алисе.

Разделение ключа. Алиса вычисляет $K_1 = (g^b)^a = g^{ab}$. Боб вычисляет $K_2 = (g^a)^b = g^{ba} = g^{ab}$. Разделенный ключ: $K = K_1 = K_2 = g^{ab}$.

Криптографический анализ. Если группа G линейная, то, по Утверждению 3.2, существует алгоритм, который по открытым данным вычисляет разделенный ключ K за полиномиальное время.

В оригинальной версии [88] в качестве G было предложено использовать группу кос Артина B_n на n нитях. Заметим, что группа B_n линейна при любом n [91]. Следовательно, в этом случае ключ K находится полиномиальным по времени алгоритмом при любых открытых данных.

4.1.2. Протокол разделения ключа Ванга, Као и др. [142]

Пусть G – некоммутативный моноид. Зафиксируем элемент $g \in G$. Пусть x – обратимый элемент G. Предполагается, что G, g, x открыты.

Алгоритм. Алиса выбирает секретное случайное число $s \in \mathbf{N}$, вычисляет g^{x^s} и посылает результат Бобу. Боб выбирает секретное случайное число $t \in \mathbf{N}$, вычисляет g^{x^t} и посылает результат Алисе.

Разделение ключа. Алиса вычисляет $K_1 = (g^{x^t})^{x^s} = g^{x^{s+t}}$. Боб вычисляет $K_2 = (g^{x^s})^{x^t} = g^{x^{s+t}}$. Разделенный ключ: $K = K_1 = K_2 = g^{x^{s+t}}$.

Криптографический анализ. Если моноид G линейный, то, по Утверждению 3.2, существует алгоритм, вычисляющий по открытым данным разделенный ключ K за полиномиальное время.

В общем случае атака методом линейной разложимости применима к рассматриваемому протоколу, если моноид G вложен в конечномерную ассоциативную алгебру над полем. Справедливости ради следует заметить, что в [142] авторы предлагают использовать в качестве G полугруппу 3×3 матриц над кольцом многочленов, $\mathbf{Z}_m[z_1, ..., z_{10}]$ при $m = 12$, профакторизованному по идеалу, порожденному всеми мономами степени 1000, т. е. над кольцом *усеченных* многочленов. Поскольку кольцо коэффициентов в данном случае не является полем, Утверждение 3.2 напрямую не применимо. Если бы m было свободным от квадратов, то переход к полям очевиден, считаем по модулю каждого простого делителя числа m, а затем применяем Китайскую теорему об остатках.

4.2. Протоколы, базирующиеся на умножениях

4.2.1. Протокол разделения ключа Стикельса [137]

Пусть G – неабелева конечная группа, и пусть g и f – два перестановочных элемента из G. Пусть $k_0 = ord(g)$ и $l_0 = ord(f)$ –

порядки этих элементов. Предположим, что данные G, g, f, k_0, l_0 открыты.

Алгоритм. Алиса выбирает два секретных натуральных числа k и l, $1 < k < k_0, 1 < l < l_0$, вычисляет $g^k f^l$ и посылает результат Бобу. Тот выбирает два секретных натуральных числа r и s, $1 < r < k_0, 1 < s < l_0$, вычисляет $g^r f^s$ и посылает результат Алисе.

Разделение ключа. Алиса вычисляет элемент $K_1 = g^k(g^r f^s)f^l = g^{k+r} f^{l+s}$, Боб – элемент $K_2 = g^r(g^k f^l)f^s = g^{k+r} f^{l+s}$. Разделенный ключ: $K = K_1 = K_2 = g^{k+r} f^{l+s}$.

Криптографический анализ. Если $G \leq \mathrm{M}_n(\mathbf{A})$ (что предполагалось в [137]), то, по Утверждению 3.3, существует алгоритм, вычисляющий по открытым данным ключ K за полиномиальное время от $n, \dim_{\mathbf{F}}(\mathbf{A}), k_0, l_0$ и размеров g и f (поле $\mathbf{F}$ предполагается фиксированным).

Замечание. Аналогичный анализ имеет место, если G – произвольная (не обязательно конечная) линейная группа.

4.2.2. Протокол разделения ключа Альвареса, Мартинеса и др. [45], [46], [47]

По данному простому числу p и двум натуральным числам n, m корреспонденты Алиса и Боб выбирают матрицы

$$M_i = \begin{pmatrix} A_i & X_i \\ 0 & B_i \end{pmatrix}$$

для $i = 1, 2$ соответственно. Здесь $A_i \in \mathrm{GL}_n(\mathbf{F}_p)$, $B_i \in \mathrm{GL}_m(\mathbf{F}_p)$, $X_i \in \mathrm{M}_{n\times m}(\mathbf{F}_p)$. Пусть $|M_i| = m_i$ для $i = 1, 2$ – порядки этих матриц. Для натурального числа t имеем

$$M_i^t = \begin{pmatrix} A_i^t & X_i^{(t)} \\ 0 & B_i^t \end{pmatrix}, i = 1, 2.$$

Алгоритм. Алиса выбирает два случайных натуральных числа $k_i, 1 \le k_i \le m_i - 1, i = 1, 2$, вычисляет

$$C = M_1^{k_1} M_2^{k_2} = \begin{pmatrix} A_C & X_C \\ 0 & B_C \end{pmatrix}$$

и передает результат Бобу.

Боб выбирает два случайных натуральных числа l_i, $1 \le l_i \le m_i - 1, i = 1, 2$, вычисляет

$$D = M_1^{l_1} M_2^{l_2} = \begin{pmatrix} A_D & X_D \\ 0 & B_D \end{pmatrix},$$

и передает результат Алисе.

Разделение ключа. Алиса вычисляет

$$K_1 = A_1^{k_1} A_D X_2^{(k_2)} + A_1^{k_1} X_D B_2^{k_2} + X_1^{(k_1)} B_D B_2^{k_2}.$$

Боб вычисляет

$$K_2 = A_1^{l_1} A_C X_2^{(l_2)} + A_1^{l_1} X_C B_2^{l_2} + X_1^{(l_1)} B_C B_2^{l_2}.$$

Разделенный ключ: $K = K_1 = K_2$.

В [140] замечено, что K есть $(1, 2)$-вхождение матрицы $M_1^{k_1+l_1} M_2^{k_2+l_2}$.

Криптографический анализ. По Утверждению 3.3, существует алгоритм, который по открытым данным находит ключ K за полиномиальное от n, m, m_1, m_2 и размеров матриц M_1 и M_2 (в предположении, что поле $\mathbf{F}_p$ фиксировано) время.

4.2.3. Протокол разделения ключа Шпильрайна-Ушакова [125] (см. также [111])

Здесь мы описываем общую (не скрученную) версию протокола и показываем, что если в качестве платформы используется линейная группа, то существует эффективная процедура, вычисляющая разделенный ключ. К скрученной версии протокола (см.

[111]) данный криптографический анализ также применим. Разницы нет почти никакой, поэтому мы опускаем детали.

Заметим тем не менее, что в оригинальной статье [125] в качестве платформы предлагалась группа Томпсона. Эта группа не линейна, поэтому данный подход к решению протокола напрямую не применим.

Пусть $G \leq \mathrm{M}_n(\mathbf{A})$ – группа (или подмоноид), и пусть g – элемент из G. Пусть A и B – конечно порожденные подгруппы (или подмоноиды) из G, причем произвольный элемент из G_1 перестановочен с любым элементом из G_2.

Алгоритм. Алиса выбирает случайные секретные элементы $a, a' \in A$, затем вычисляет элемент aga' и передает его Бобу. Боб выбирает случайные секретные элементы $b, b' \in B$, вычисляет элемент bgb' и передает его Алисе.

Разделение ключа. Алиса вычисляет $K_1 = abgb'a'$. Боб вычисляет $K_2 = baga'b' = abgb'a'$.

Разделенный ключ: $K = K_1 = K_2 = abgb'a'$.

Криптографический анализ. По Утверждению 3.3, существует алгоритм, который по открытым данным вычисляет разделенный ключ K за полиномиальное от $n, \dim_{\mathbf{F}}(\mathbf{A})$, размеров порождающих множеств подгрупп (подмоноидов) A и B и размеров элементов g, aga' и bgb' время (в предположении, что поле $\mathbf{F}$ фиксировано).

4.2.4. Протокол разделения ключа Романчук-Устименко [117]

Пусть $G = \mathrm{GL}_n(\mathbf{F})$, где $\mathbf{F}$ – конечное поле. Предположим, что $C, D \in G$ – две перестановочные матрицы. Зафиксируем вектор $g \in \mathbf{F}^n$. Все эти данные считаем открытыми.

Алгоритм. Алиса выбирает случайный многочлен $P = P(C, D) \in \mathbf{F}[x, y]$, вычисляет вектор gP, затем передает его Бобу. Боб выбирает случайный многочлен $Q = Q(C, D) \in \mathbf{F}[x, y]$, вычисляет и передает Алисе вектор gQ.

Разделение ключа. Алиса вычисляет ключ $K_1 = (gQ)P = gQP$. Боб вычисляет ключ $K_2 = (gP)Q = gPQ$. Разделенный ключ: $K = K_1 = K_2$.

Криптографический анализ. По Утверждению 3.1 существует полиномиальный от n и размеров C, D, P и Q (в предположении, что поле $\mathbf{F}$ фиксировано) алгоритм, который по открытым данным вычисляет разделенный ключ K.

Замечание. Другая атака на этот протокол, также базирующаяся на линейной алгебре, была ранее предложена Блекберном и др. в [54]. Основная идея атаки следующая.

Предположим, что потенциальный взломщик Ева знает g, gP, gQ, C и D. Пусть X – матрица, перестановочная с C и D, такая, что $gQ = gX$. Для нахождения X достаточно решить соответствующую систему линейных уравнений. Затем Ева может вычислить разделенный ключ как $(gP)X = gXP = gQP = K$.

Заметим, что соответствующие системы линейных уравнений приходится решать в каждой сессии. Таких уравнений $2n^2 + n$. Если использовать метод линейной разложимости, то базис вычисляется один раз (offline). В каждой сессии решается система $\leq n$ линейных уравнений. Поэтому оценка сложности здесь на несколько порядков ниже.

4.3. Протоколы, использующие автоморфизмы

Если G – алгебраическая система (группа, полугруппа, кольцо и т. п.), $\mathrm{Aut}(G)$ – ее группа автоморфизмов, то через g^α будем обозначать образ элемента $g \in G$ относительно автоморфизма $\alpha \in \mathrm{Aut}(G)$. В других случаях мы используем обозначение $\alpha(g)$.

4.3.1. Протокол разделения ключа Махалонобиса [99]

Пусть G – группа и $g \in G$. Предположим, что Φ и Ψ – два конечных подмножества группы автоморфизмов $\mathrm{Aut}(G)$, причем элементы из Φ попарно перестановочны с элементами из Ψ. Пусть A и B – подгруппы группы $\mathrm{Aut}(G)$, порожденные множествами Φ и Ψ соответственно.

Алгоритм. Алиса выбирает случайный автоморфизм $\alpha \in A$, вычисляет g^α и передает результат Бобу. Боб выбирает случайный автоморфизм $\beta \in B$, вычисляет g^β и передает результат Алисе.

Разделение ключа. Алиса вычисляет $K_1 = (g^\beta)^\alpha = g^{\alpha\cdot\beta}$. Боб вычисляет $K_2 = (g^\alpha)^\beta = g^{\beta\cdot\alpha} = g^{\alpha\cdot\beta}$. Разделенный ключ: $K = K_1 = K_2 = g^{\alpha\cdot\beta}$.

Криптографический анализ. Пусть $G \leq \mathbf{A}$, где $\mathbf{A}$ – конечномерная ассоциативная алгебра над конструктивным полем $\mathbf{F}$. Если G такова, что все автоморфизмы из A (или из B) поднимаются до автоморфизмов линейного пространства алгебры $\mathbf{A}$, то, по Утверждению 3.4, существует алгоритм, вычисляющий по открытым данным разделенный ключ K за время, полиномиальное от $n, \dim_{\mathbf{F}}(\mathbf{A})$, размера элемента g и размеров элементов из Φ, Ψ (мы предполагаем, что поле $\mathbf{F}$ фиксировано).

Если голоморф $H(G)$ линеен (является подгруппой в $\mathrm{M}_n(\mathbf{A})$), то, по Утверждению 3.4, существует алгоритм, вычисляющий по открытым данным разделенный ключ K за время, полиномиальное от n, $\dim_{\mathbf{F}}(\mathbf{A})$, размера g и размеров элементов из Φ, Ψ.

В своей работе [99] автор предлагает использовать в качестве платформы конечно порожденную неабелеву нильпотентную группу G. Известно [24], что голоморф любой полициклической группы $H(G)$, в частности любой конечно порожденной нильпотентной группы, точно представим матрицами. Следовательно, в этом случае применим описанный выше криптографический анализ.

4.3.2. Протокол передачи ключа Махалонобиса [99]

Используем обозначения из 4.3.1.

Алгоритм. Алиса выбирает случайный автоморфизм $\alpha \in A$, вычисляет g^α, затем посылает результат Бобу. Боб выбирает случайный автоморфизм $\beta \in B$, вычисляет и посылает $(g^\alpha)^\beta$ Алисе. Алиса вычисляет α^{-1} и получает $((g^\alpha)^\beta)^{\alpha^{-1}} = g^\beta$. Затем она выбирает другой случайный автоморфизм $\gamma \in A$, вычисляет и посылает Бобу $(g^\beta)^\gamma$.

Получение ключа. Боб вычисляет β^{-1} и получает затем ключ $K = ((g^{\beta})^{\gamma})^{\beta^{-1}} = g^{\gamma}$.

Криптографический анализ. Предположим, что $G \leq \mathrm{M}_n(\mathbf{A})$. Полагаем $v = (g^{\alpha})^{\beta}$. Как в Утверждении 3.1, находим базис пространства $Sp(v^A)$, скажем, $v^{\alpha_1}, \ldots, v^{\alpha_t}$. Заметим, что $(g^{\beta})^{\gamma} = = (g^{\alpha\beta})^{\alpha^{-1}\gamma} \in Sp(v^A)$, поэтому справедливы равенства:

$$g^{\beta\cdot\gamma} = \sum_{i=1}^{t} \lambda_i v^{\alpha_i} = (\sum_{i=1}^{t} \lambda_i (g^{\alpha})^{\alpha_i})^{\beta},\ \lambda_i \in \mathbf{F}. \tag{17}$$

Здесь $(g^{\gamma})^{\beta} = (\sum_{i=1}^{t} \lambda_i (g^{\alpha})^{\alpha_i})^{\beta}$, откуда получаем разложение искомого ключа

$$K = g^{\gamma} = \sum_{i=1}^{t} \lambda_i (g^{\alpha})^{\alpha_i}. \tag{18}$$

4.3.3. Протокол разделения ключа Хабиба, Кахроби, Купариса и Шпильрайна [77]

Пусть G – (полу)группа и $H(G)$ – ее голоморф. Зафиксируем элемент $g \in G$ и автоморфизм $\phi \in \mathrm{Aut}(G)$. Эти данные считаем открытыми.

В этом разделе мы обозначаем образ элемента $g \in G$ относительно автоморфизма $\mu \in \mathrm{Aut}(G)$ через $\mu(g)$ (вместо g^{μ}).

Алгоритм. Алиса выбирает случайное натуральное число $m \in N$. Затем она вычисляет

$$(\phi, g)^m = (\phi^m, \phi^{m-1}(g) \cdot \ldots \cdot \phi^2(g) \cdot \phi(g) \cdot g)$$

и посылает только вторую компоненту $a_m = \phi^{m-1}(g) \cdot \ldots \cdot \phi^2(g) \cdot \phi(g) \cdot g$ полученной пары Бобу.

Боб выбирает случайное натуральное число $n \in N$. Затем он вычисляет $(\phi, g)^n = (\phi^n, \phi^{n-1}(g) \cdot \ldots \cdot \phi^2(g) \cdot \phi(g) \cdot g)$ и посылает только вторую компоненту $a_n = \phi^{n-1}(g) \cdot \ldots \cdot \phi^2(g) \cdot \phi(g) \cdot g$ этой пары Алисе.

Разделение ключа. Алиса вычисляет

$$(*, a_n) \cdot (\phi^m, a_m) = (* \cdot \phi^m, \phi^m(a_n) \cdot a_m) = (* \cdot \phi^m, K_1).$$

Заметим, что она на самом деле не имеет определенного значения для $* \cdot \phi^m$.

Боб вычисляет

$$(**, a_m) \cdot (\phi^n, a_n) = (** \cdot \phi^n, \phi^n(a_m) \cdot a_n) = (** \cdot \phi^n, K_2).$$

Также заметим, что для него выражение $** \cdot \phi^n$ остается неопределенным.

Разделенный ключ: $K = K_1 = K_2 = a_{m+n}$.

Криптографический анализ. Пусть $G \leq \mathbf{A}$, где $\mathbf{A}$ – конечномерная ассоциативная алгебра над конструктивным полем $\mathbf{F}$. Предположим, что автоморфизм ϕ расширяется до автоморфизма линейного пространства $\mathbf{A}$.

Методом Гаусса получаем максимальную линейно независимую систему L множества $\{a_0, a_1, ..., a_k, ...\}$, где $a_0 = g$ и $a_k = \phi^{k-1}(g) \cdot ... \cdot \phi(g) \cdot g$ для $k \geq 1$. Предположим, что $\{a_0, ..., a_k\}$ – линейно независимое множество, а a_{k+1} представляется в виде

$$a_{k+1} = \sum_{i=0}^{k} \lambda_i a_i, \quad \lambda_i \in \mathbb{F}.$$

По индукции предполагаем, что a_{k+j} допускает такое представление для всех $j \leq t-1$. В частности,

$$a_{k+t-1} = \sum_{i=0}^{k} \mu_i a_i, \quad \mu_i \in \mathbb{F}.$$

Тогда

$$a_{k+t} = \phi(a_{k+t-1}) \cdot g = \sum_{i=0}^{k} \mu_i \phi(a_i) \cdot g =$$

$$\sum_{i=0}^{k} \mu_i a_{i+1} = \mu_k \lambda_0 a_0 + \sum_{i=0}^{k-1} (\mu_i + \mu_k \lambda_{i+1}) a_{i+1}.$$

Значит, $L = \{a_0, ..., a_k\}$.

В частности, мы можем эффективно вычислить

$$a_n = \sum_{i=0}^{k} \eta_i a_i, \quad \eta_i \in \mathbb{F}.$$

Тогда

$$a_{m+n} = \phi^m(a_n) \cdot a_m = \sum_{i=0}^{k} \eta_i \phi^m(a_i) \cdot a_m =$$

$$= \sum_{i=0}^{k} \eta_i \phi^i(a_m) \cdot a_i.$$

Заметим, что все параметры правой части полностью известны. Это дает значение разделенного ключа $K = a_{m+n}$.

В оригинальной версии этого протокола [77] в качестве G предлагается полугруппа 3×3-матриц над групповой алгеброй $\mathbf{F}_7[\mathbb{A}_5]$, где $\mathbb{A}_5$ – группа четных подстановок на 5 символах. Авторы [77] использовали расширение полугруппы G с помощью внутреннего автоморфизма, соответствующего сопряжению матрицей $H \in \mathrm{GL}_3(\mathbf{F}_7[\mathbb{A}_5])$.

Следовательно, в этом случае существует полиномиальный по времени алгоритм, вычисляющий разделенный ключ K по открытым данным.

§ 5. Анализ некоторых схем криптографии на алгебраических платформах

Как уже говорилось выше, в настоящее время в качестве шифрования все чаще используются алгебраические системы, отличные от групп или полугрупп (или моноидов). Таким образом криптография, основанная на группах, постепенно вырастает в алгебраическую криптографию.

Переходим к рассмотрению и криптографическому анализу некоторых схем шифрования и разделения ключа, базирующихся на групповых (луповых) алгебрах и градуированных алгебрах с мультипликативным базисом, предложенных в работах Росошека [37], [38] Михалева и др. [7], [19] и др. Объединяет эти схемы (кроме схемы из [7]) использование в них автоморфизмов. Также приводится криптографический анализ протокола разделения ключа Мегрелишвили и Джинджихадзе [23]. Используется метод линейного разложения нахождения шифрованного сообщения или разделенного ключа, описанный выше в 3.2.1. Его конкретные реализации в данном случае имеют особенности. По этой причине некоторые общие рассуждения метода повторяются.

5.1. Протоколы на векторном пространстве и групповом кольце

5.1.1. Протокол разделения ключа Мегрелишвили-Джинджихадзе [23] (см. также [103], [104])

Корреспонденты Алиса и Боб договариваются о выборе векторного пространства $V = \mathbf{F}_2^n$ размерности n над полем $\mathbf{F}_2$. Далее фиксируется квадратная матрица A размера $n \times n$ и вектор $v \in V$. Эти данные открыты.

Алгоритм. Алиса выбирает случайным образом натуральное число k, вычисляет и пересылает Бобу вектор $u = vA^k$. В свою очередь Боб выбирает случайное натуральное число l, вычисляет и пересылает Алисе вектор $w = vA^l$.

Разделение ключа. Затем каждый из корреспондентов вычисляет разделяемый ключ

$$K = uA^l = wA^k = vA^{k+l}. \tag{19}$$

Криптографический анализ. Выпишем векторы $v = vA^0, vA, ..., vA^m$ до максимально возможной степени m с условием линейной независимости этого набора. Ясно, что $m \leq n$, поэтому процесс эффективен. Данный набор является базисом линейного пространства $\mathrm{Sp}_{\mathbf{F}_2}(vA^k, k \in \mathbf{N})$, порожденного всеми векторами вида $vA^k, k \in \mathbf{N}$. Для этого достаточно доказать, что любой вектор $vA^k, k \geq m+1$, линейно выражается через данный набор. Поскольку набор $v, vA, ..., vA^m, vA^{m+1}$ является первым линейно зависимым набором, вектор vA^{m+1} допускает разложение вида

$$vA^{m+1} = \sum_{i=0}^{m} \alpha_i vA^i, \ \alpha_i \in \mathbf{F}_2. \tag{20}$$

Пусть уже доказано, что вектор $vA^k, k \geq m+1$, представим в виде

$$vA^k = \sum_{i=0}^{m} \beta_i vA^i, \ \beta_i \in \mathbf{F}_2. \tag{21}$$

Умножим обе части (21) справа на матрицу A и проведем преобразование с использованием равенства (21):

$$vA^{k+1} = \sum_{i=0}^{m} \beta_i vA^{i+1} = \sum_{i=0}^{m-1} \beta_i vA^{i+1} + \beta_m \cdot \sum_{i=0}^{m} \beta_i vA^i =$$

$$\beta_m \cdot \beta_0 v + \sum_{i=1}^{m} (\beta_{i-1} + \beta_m \cdot \beta_i) vA^i. \tag{22}$$

Утверждение о базисе $v, vA, ..., vA^m$ пространства $\mathrm{Sp}_{\mathbf{F}_2}(vA^k, k \in \mathbf{N})$ следует по индукции.

Теперь можно получить разложение

$$u = vA^k = \alpha_0 v + \alpha_1 vA + ... + \alpha_m vA^m,\ \alpha_i \in \mathbf{F}_2. \qquad (23)$$

Заметим, что для получения разложения (23) не нужно знать k, а только u.

После этого подставим в правую часть полученного выражения (23), где все компоненты известны, вектор w вместо v и получим

$$\alpha_0 w + \alpha_1 wA + ... + \alpha_m wA^m =$$
$$(\alpha_0 v + \alpha_1 vA + ... + \alpha_m vA^m)A^l =$$
$$vA^{k+l} = K. \qquad (24)$$

Замечание. Авторы данного протокола, анализируя его криптостойкость, рассматривали возможность нахождения числа k по уравнению вида $vA^k = u$ или числа l по уравнению вида $vA^l = w$. Значительное внимание они уделили способам выбора матрицы A достаточно большого порядка, при котором подобные вычисления становятся трудными. Конечно, существуют способы выбора матрицы A порядка $2^n - 1$. Однако, при описанном выше подходе такой выбор не играет существенной роли. Данный пример достаточно хорошо иллюстрирует возможности метода линейного разложения.

5.1.2. Система Росошека [38]

Пусть K – конечное ассоциативное кольцо с единицей, группа автоморфизмов $\mathrm{Aut}(K)$ которого некоммутативна. Пусть G – конечная абелева группа с некоммутативной группой автоморфизмов $\mathrm{Aut}(G)$. Через KG обозначим групповое кольцо группы G с коэффициентами из K.

Алиса выбирает случайный автоморфизм σ кольца K большого порядка, а также случайный автоморфизм ν группы G также

большого порядка. Через $C(\sigma)$ обозначим централизатор элемента σ в группе $\mathrm{Aut}(K)$, а через $C(\nu)$ – централизатор автоморфизма ν в $\mathrm{Aut}(G)$. Считаем, что оба этих централизатора строго больше, чем подгруппы $\mathrm{gp}(\sigma)$ и $\mathrm{gp}(\nu)$, соответственно.

Установка. Алиса выбирает случайным образом автоморфизм $\tau \in C(\sigma)$, не принадлежащий $\mathrm{gp}(\sigma)$, и автоморфизм $\omega \in C(\nu)$, не принадлежащий $\mathrm{gp}(\nu)$. Затем она задает автоморфизм φ группового кольца KG следующим образом: для любого $h \in KG$ вида $h = a_{g_1}g_1 + ... + a_{g_n}g_n$, где $G = \{g_1, ..., g_n\}, a_{g_i} \in K, i = 1, ..., n$, она полагает

$$h^{\varphi} = (a_{g_1}^{\tau} g_1^{\omega} + ... + a_{g_n}^{\tau} g_n^{\omega})_{\mu}, \tag{25}$$

где μ – случайная подстановка на множестве номеров, слагаемых в записи элементов группового кольца, которая в силу коммутативности сложения не меняет сам элемент h, а только форму его записи. Секретным ключом Алисы служит автоморфизм φ.

Далее Алиса выбирает обратимый элемент $x \in KG$ и вычисляет $x^{\varphi} \in KG$.

Открытым ключом для А служит $(\sigma, \nu, x, x^{\varphi})$.

Алгоритм. Боб для шифрования своего сообщения, закодированного в виде элемента m группового кольца KG, выбирает упорядоченную пару случайных натуральных чисел (i, j), по которым определяет сессионный автоморфизм ψ группового кольца KG, полагая для любого элемента

$$h = a_{g_1}g_1 + ... + a_{g_n}g_n,$$

где $a_{g_1}, ..., a_{g_n} \in K$,

$$h^{\psi} = (a_{g_1}^{\sigma^i} g_1^{\nu^j} + ... + a_{g_n}^{\sigma^i} g_n^{\nu^j})_{\xi}, \tag{26}$$

где ξ – есть случайная подстановка на множестве номеров слагаемых. После этого Боб вычисляет $(x^{-1})^{\psi}$, используя открытый

ключ Алисы и автоморфизм ψ. Набор параметров (i, j, ψ) считается секретным сессионным ключом.

Зашифрованное сообщение m имеет вид

$$c = ((x^{-1})^{\psi}, m \cdot (x^{\varphi})^{\psi}). \tag{27}$$

Расшифрование. Алиса, получив зашифрованное сообщение (27), вычисляет, пользуясь перестановочностью автоморфизмов φ и ψ, очевидной из их построения, элемент $((x^{-1})^{\psi})^{\varphi} = ((x^{-1})^{\varphi})^{\psi}$. Затем, умножив его справа на второй элемент набора c, вычисляет m.

Криптографический анализ. Предположим, что K – алгебра над конечным полем $\mathbf{F}$ конечной размерности l. Обозначим через $\sigma^i \wedge \nu^j, i, j \geq 0$, автоморфизмы алгебры KG, задаваемые указанным выше способом (26). Также предполагаем, что любой автоморфизм кольца K будет автоморфизмом K как алгебры над $\mathbf{F}$. Это условие выполнено автоматически, если $\mathbf{F}$ – простое конечное поле. Поэтому достаточно требовать, чтобы K было алгеброй над простым конечным полем.

В этом случае KG также естественно является алгеброй над $\mathbf{F}$ конечной размерности $m = l \cdot \mathrm{ord}(G)$, где $\mathrm{ord}(G)$ означает порядок группы G. Любой автоморфизм вида $\eta = \lambda \wedge \mu, \lambda \in \mathrm{Aut}K$, $\mu \in \mathrm{Aut}G$, будет автоморфизмом KG как алгебры над $\mathbf{F}$.

Определим на группе Φ всех автоморфизмов вида $\sigma^i \wedge \nu^j$ для произвольного $r \geq 0$ *сферу* и *шар* радиуса r, полагая $\mathbf{S}_r = \{\sigma^i \wedge \nu^j | i + j = r\}$ и $\mathbf{B}_r = \cup_{t=0}^{r} \mathbf{S}_t$, соответственно. При этом $\mathbf{S}_0 = \mathbf{B}_0 = \{\sigma^0 \wedge \nu^0 = 1\}$.

Пусть x – фиксированный ненулевой элемент алгебры KG, выбранный Алисой. Обозначим через x^{Φ} множество всех элементов алгебры KG вида $x^{\eta}, \eta \in \Phi$, другими словами – Φ-орбиту элемента x. Через $V = Sp_{\mathbf{F}}(x^{\Phi})$ обозначим линейное подпространство алгебры KG над полем $\mathbf{F}$, порожденное множеством x^{Φ}.

Базис пространства V строим последовательно. Вначале полагаем $L_0 = \{x\}$. Затем расширяем L_0 до максимального линейно

независимого множества L_1 подпространства $V_1 = Sp_{\mathbf{F}}(x^{\mathbf{B}_1})$. Для этого мы рассматриваем последовательно в соответствии с лексикографическим порядком элементы $x^{\sigma^i \wedge \nu^j}, i+j=1$, включая в L_1 те из них, которые не выражаются линейно через уже включенные до них элементы. Пусть уже построен базис L_p подпространства $V_p = Sp_{\mathbf{F}}(x^{\mathbf{B}_p})$. Рассматриваем последовательно только те элементы вида $x^{\sigma^i \wedge \nu^j}, i+j=p+1$, множества $x^{\mathbf{S}_{p+1}}$, которые имеют предшественников, т. е. $x^{\sigma^{i-1} \wedge \nu^j}$ или $x^{\sigma^i \wedge \nu^{j-1}}$, в L_p. Если предшественники не включены в базис, значит, соответствующие им элементы линейно выражаются через уже рассмотренные элементы. Но тогда рассмотрение элемента $x^{\sigma^i \wedge \nu^j}, i+j=p+1$, не имеет смысла, так как он также линейно выражается через уже рассмотренные элементы. Перебираем элементы последовательно в соответствии с лексикографическим порядком, каждый раз проверяя, выражается ли элемент линейно через уже построенную часть базиса L_{p+1}. Если не выражается, то включаем его в L_{p+1}, если выражается, то нет. Так как размерность пространства V не превышает m, то через не более чем m включений возникнет ситуация, когда $L_p = L_{p+1}$, то есть на очередном $p+1$-м шаге базис не увеличится. Очевидно, что в этом случае $L_p = L$. Процесс построения L закончен.

Пусть $L = \{x^{\sigma^{q_i} \wedge \nu^{t_i}}, i = 1, ..., s\}$. Вычисляем соответствующее разложение

$$x^{\psi} = \sum_{i=1}^{s} \alpha_i x^{\sigma^{q_i} \wedge \nu^{t_i}}, \alpha_i \in \mathbf{F}, i = 1, ..., s. \tag{28}$$

Подставим в правую часть полученного выражения (28) вместо x элемент x^{φ}. Поскольку φ является автоморфизмом алгебры (достаточно даже – линейного пространства) KG над $\mathbf{F}$ и перестановочен с любым автоморфизмом из Φ, получаем

$$\sum_{i=1}^{s} \alpha_i (x^{\varphi})^{\sigma^{q_i} \wedge \nu^{t_i}} = (\sum_{i=1}^{s} \alpha_i x^{\sigma^{q_i} \wedge \nu^{t_i}})^{\varphi} = (x^{\psi})^{\varphi} = (x^{\phi})^{\psi}. \tag{29}$$

Элемента $(x^{\varphi})^{\psi}$ достаточно для получения m.

Замечание. В работе [38] есть примеры, в которых в качестве K выбирается кольцо матриц $\mathrm{M}_2(\mathbf{F}_p)$, где p – простое. Такое кольцо может рассматриваться как алгебра над $\mathbf{F}_p$ размерности 4. Если выбрать в нем произвольную матрицу a, а затем применить к этой матрице автоморфизм σ^i, то образ a^{σ^i} можно довольно легко записать в виде линейной комбинации над $\mathbf{F}_p$ единичной матрицы и матриц g^{σ^j} при $j = 1, 2, 3$. При этом i может быть очень большим. В общем случае предложенная атака будет эффективной, если кольцо K является алгеброй достаточно малой размерности над $\mathbf{F}_p$. При этом порядок группы G должен быть сравнительно небольшим. Эти требования выглядят достаточно естественными. Действительно, работа в групповых кольцах групп большого порядка, да еще с использованием автоморфизмов, затруднена уже при шифровании и расшифровании. Поэтому основные методы скрытия в подобных системах обычно связывают с достаточно большим кольцом коэффициентов.

Заметим, что в общем случае не обязательно пытаться получить базис L полностью. Можно организовать процесс параллельного построения базиса и проверки выразимости через уже построенную часть элемента x^{ψ}.

5.2. Протоколы на луповых кольцах

5.2.1. Протокол выработки общего ключа Маркова, Михалева и др. [19]

Предварительные сведения

Напомним вкратце некоторые определения, относительно которых см., например, [4], [116] или [136]

Группоид – непустое множество G с заданной бинарной операцией $\cdot$. *Квазигруппой* называется группоид, в котором для любой пары элементов $g, f \in G$ однозначно разрешимы уравнения

$xg = f$ и $gx = f$. *Лупой* называется квазигруппа с единицей. Лупа называется *лупой Муфанг*, если на ней выполняется тождество $(xy)(zx) = (x(yz))x$.

Приведем некоторые свойства лупы Муфанг, относительно которых см., например, [4], [116] или [136]:

1) в лупе Муфанг любые два элемента порождают подгруппу, в частности, лупа Муфанг является лупой с ассоциативными степенями;

2) если для элементов $a, b, c \in G$ выполнено равенство $a(bc) = (ab)c$, то эти элементы a, b, c порождают в G подгруппу.

Установка. Пусть G — лупа Муфанг, $a, b, c \in G$ – ее элементы. Эти данные считаются известными.

Алгоритм. Алиса выбирает тройку случайных натуральных чисел (m, k, n), затем вычисляет и посылает Бобу сообщение вида

$$(u_1, u_2) = (a^m b^k, b^k c^n).$$

Боб выбирает тройку случайных чисел (r, l, s), вычисляет и посылает Алисе сообщение

$$(v_1, v_2) = (a^r b^l, b^l c^s).$$

Получив сообщение от Боба, Алиса вычисляет элементы

$$(a^m v_1)b^k, (b^k v_2)c^n.$$

Подобным же образом Боб получает элементы

$$(a^r u_1)b^l, (b^l u_2)c^s.$$

Разделенный ключ. Общим ключом для Алисы и Боба служит

$$K = (a^{m+r} b^{k+l}) \cdot (b^{k+l} c^{n+s}). \tag{30}$$

Объяснение. Имеет место следующее утверждение.

Утверждение 5.1 [19]. *Если G – лупа Муфанг, $a, b \in G$, тогда для любых показателей $k, l, m, n, r, s \geq 0$ выполнено равенство*

$$(a^m(a^r b^s))b^n = a^m((a^r b^s)b^n) = (a^r(a^m b^n))b^s = a^r((a^m b^m)b^s) = a^{m+r}b^{n+s}. \quad (31)$$

Алиса получает ключ K с помощью следующих вычислений:

$$(a^m v_1)b^k = a^{m+r}b^{k+l}, (b^k v_2)c^s = b^{k+l}c^{n+s},$$
$$K = (a^{m+r}b^{k+l}) \cdot (b^{k+l}c^{n+s}). \quad (32)$$

Боб получает ключ K аналогично.

Криптографический анализ. Предположим, что лупа Муфанг G содержится в конечномерной алгебре размерности m над полем $\mathbf{F}$. В [19], например, в качестве возможных платформ для протокола рассматриваются неассоциативные, конечные и простые лупы Муфанг, которые называются лупами *Пейджа*. Они могут быть вложены в алгебры Цорна размерности 8 над конечным полем.

Возьмем элементы a, b, c – фигурирующие в протоколе. Пусть m, k, n, r, l, s – параметры из протокола. Достаточно по известным элементам $u_1 = a^m b^k$, $u_2 = b^k c^n, v_1 = a^r b^l, v_2 = b^l c^s$ вычислить $a^{m+r}b^{k+l}$ и $b^{k+l}c^{n+s}$.

Вначале определим базисы подпространств $V_1 = \mathrm{Sp}_{\mathbf{F}}(a^i b^j | i, j \geq 0)$ и $V_2 = \mathrm{Sp}_{\mathbf{F}}(b^p c^q | p, q \geq 0)$ соответственно. Опишем построение базиса пространства V_1. Базис пространства V_2 строится аналогично. Для этого на множестве $\{a^i b^j\}$ для произвольного $r \geq 0$ определим сферу радиуса r, полагая $\mathbf{S}_r = \{a^i b^j | i+j = r\}$ и шар радиуса r формулой $\mathbf{B}_r = \cup_{l=0}^{r} \mathbf{S}_t$. По определению, $\mathbf{S}_0 = \mathbf{B}_0 = \{1\}$. Пусть $L_0 = \{1\}$. Далее расширяем L_0 до $L_1 = \mathrm{Sp}_{\mathbf{F}}(\mathbf{B}_1)$, просматривая последовательно по лексикографическому порядку элементы из $\mathbf{S}_1$, включая в L_1 те из них, которые не выражаются линейно через уже включенные. Если базис L_i пространства $\mathrm{Sp}_{\mathbf{F}}(\mathbf{B}_i)$ уже

определен, просматриваем последовательно элементы $\mathbf{S}_{i+1}$, имеющие уже включенных в базис предшественников. У элемента $a^i b^j$ предшественниками считаются $a^{i-1}b^j$ (если $i \neq 0$) и $a^i b^{j-1}$ (если $j \neq 0$). Включаем в базис L_{i+1} те из них, которые не выражаются линейно через уже включенные. Если на некотором этапе $L_i = L_{i+1}$, то $L_i = L$.

Пусть $L = \{a^{p_i} b^{q_i}, i = 1, ..., t\}$. Вычисляем соответствующее разложение

$$a^m b^k = \sum_{i=1}^{t} \alpha_i a^{p_i} b^{q_i}, \alpha_i \in \mathbf{F}, i = 1, ..., t. \tag{33}$$

Используя правую часть (33), где все параметры известны, и элемент $a^r b^l$, получим

$$\sum_{i=1}^{t} \alpha_i (a^{p_i}(a^r b^l)) b^{q_i} = (a^r (\sum_{i=1}^{t} a^{p_i} b^{q_i})) b^l =$$

$$(a^r (a^m b^k)) b^l = a^{m+r} b^{k+l}. \tag{34}$$

Точно так же получаем элемент $b^{k+l} c^{n+s}$. Затем вычисляем искомое произведение

$$K = (a^{m+r} b^{k+l}) \cdot (b^{k+l} c^{n+s}).$$

5.2.2. Система Грибова, Золотых и Михалева [7]

Пусть K – ассоциативное кольцо с единицей 1, G – лупа, KG – луповое кольцо.

Установка. Алиса выбирает случайный автоморфизм σ кольца K большого порядка, а также случайный автоморфизм ν лупы G также большого порядка. Через $C(\sigma)$ обозначим централизатор элемента σ в группе $\mathrm{Aut}(K)$, а через $C(\nu)$ – централизатор автоморфизма ν в $\mathrm{Aut}(G)$. Считаем, что оба этих централизатора строго больше, чем подгруппы $\mathrm{gp}(\sigma)$ и $\mathrm{gp}(\nu)$ соответственно.

Генерация ключей. Алиса выбирает случайным образом автоморфизм $\tau \in C(\sigma)$, не принадлежащий $\mathrm{gp}(\sigma)$, и автоморфизм $\omega \in C(\nu)$, не принадлежащий $\mathrm{gp}(\nu)$. Затем она задаёт автоморфизм φ лупового кольца KG следующим образом: для любого $h \in KG$ вида $h = a_{g_1}g_1 + ... + a_{g_n}g_n$, где $g_i \in G, a_{g_i} \in K, i = 1, ..., n$, определяет значение h^φ формулой

$$h^\varphi = a_{g_1}^\tau g_1^\omega + ... + a_{g_n}^\tau g_n^\omega. \tag{35}$$

Далее Алиса выбирает элементы $x, a \in KG$ и вычисляет $x^\varphi, a^\varphi \in KG$.

Открытым ключом для Алисы служит

$$(\sigma, \nu, x, x^\varphi, a, a^\varphi).$$

Шифрование. Боб для шифрования своего сообщения, закодированного в виде элемента m групповой алгебры KG, выбирает две упорядоченных пары случайных натуральных чисел (i, j) и (k, l), по которым определяет сессионные автоморфизмы ψ и χ группового кольца KG, полагая для любого элемента $h = a_{g_1}g_1 + ... + a_{g_n}g_n$, где $g_i \in G, a_{g_i} \in K, i = 1, ..., n$,

$$h^\psi = a_{g_i}^{\sigma^i} g_1^{\nu^j} + ... + a_{g_n}^{\sigma^i} g_n^{\nu^j}, h^\chi = a_{g_i}^{\sigma^k} g_1^{\nu^l} + ... + a_{g_n}^{\sigma^k} g_n^{\nu^l}. \tag{36}$$

После этого Боб вычисляет x^ψ, a^χ, используя открытый ключ корреспондента А и автоморфизмы ψ и χ. Набор параметров (i, j, k, l, ψ, χ) считается секретным сессионным ключом.

Зашифрованное сообщение m имеет вид

$$c = (a^\chi \cdot x^\psi, m \cdot ((a^\varphi)^\chi \cdot (x^\varphi)^\psi)). \tag{37}$$

Также Боб вычисляет левый аннулятор $\mathrm{Ann}((a^\varphi)^\chi \cdot (x^\varphi)^\psi)$. Если полученный аннулятор ненулевой, то проводится новая сессия с выбором других элементов a и x, или же выбираются новые сессионные автоморфизмы ψ, χ.

Расшифрование. Алиса, получив зашифрованное сообщение (37), вычисляет, пользуясь перестановочностью автоморфизмов φ, ψ и χ, очевидной из их построения, элемент $(a^{\chi} \cdot x^{\psi})^{\varphi} = (a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi}$.

Для получения сообщения m Алисе достаточно решить систему линейных уравнений с коэффициентами из кольца K. Однозначность решения обеспечивается тривиальностью левого аннулятора элемента $(a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi}$.

Криптографичекий анализ. Предположим, что KG – алгебра над конечным полем $\mathbf{F}$ конечной размерности m. Обозначим через $\sigma^i \wedge \nu^j, i, j \geq 0$, автоморфизмы кольца KG, задаваемые указанным выше способом. Также предполагаем, что любой из рассматриваемых автоморфизм кольца K будет автоморфизмом K как алгебры над $\mathbf{F}$. Это условие выполнено автоматически, если $\mathbf{F}$ – простое конечное поле. Поэтому достаточно требовать, чтобы K было алгеброй над простым конечным полем. Определим на группе Φ всех автоморфизмов вида $\sigma^i \wedge \nu^j, i, j \geq 0$, для произвольного $r \geq 0$ сферу $\mathbf{S}_r$ и шар $\mathbf{B}_r$ радиуса r, как это было сделано в криптоанализе протокола Росошека, описанном выше.

Пусть z – некоторый фиксированный ненулевой элемент алгебры KG. Обозначим через z^{Φ} множество всех элементов алгебры KG вида $z^{\eta}, \eta \in \Phi$, другими словами – Φ-орбиту элемента z. Пусть теперь a, x – элементы из протокола, a^{Φ}, x^{Φ} – их Φ-орбиты, $a^{\Phi} \cdot x^{\Phi}$ – произведение Φ-орбит.Через $V = \mathrm{Sp}_{\mathbf{F}}(a^{\Phi} \cdot x^{\Phi})$ обозначим линейное подпространство алгебры KG над полем $\mathbf{F}$, порожденное множеством $a^{\Phi} \cdot x^{\Phi}$.

Базис L пространства V строим последовательно. Вначале полагаем $L_0 = \{a \cdot x\}$. Затем расширяем L_0 до максимального линейно независимого множества L_1 подпространства $V_1 = \mathrm{Sp}_{\mathbf{F}}(a \cdot x^{\mathbf{B}_1} \cup a^{\mathbf{B}_1} \cdot x)$. Для этого мы рассматриваем последовательно в соответствии с лексикографическим порядком элементы $a \cdot x^{\sigma^i \wedge \nu^j}$ и $a^{\sigma^i \wedge \nu^j} \cdot x$, где $i + j = 1$, включая в L_1 те из них, которые не выражаются линейно через уже включенные до них элементы. Пусть уже построен базис L_r подпространства $V_r = \mathrm{Sp}_{\mathbf{F}}(a^{\mathbf{B}_q} \cdot x^{\mathbf{B}_p} | p +$

$q = r$). Рассматриваем последовательно только те элементы вида $a^{\sigma^k \wedge \nu^l} \cdot x^{\sigma^i \wedge \nu^j}, k + l + i + j = r + 1$, которые имеют предшественников в L_r, т. е. элементы указанного вида, отвечающие наборам индексов $(k-1, l, i, j)$, $(k, l-1, i, j), (k, l, i-1, j)$ или $(k, l, i, j-1)$. Перебираем их последовательно в соответствии с лексикографическим порядком, каждый раз проверяя, выражается ли элемент линейно через уже построенную часть базиса L_{r+1}. Если не выражается, то включаем его в L_{r+1}, если выражается – то нет. Так как размерность пространства V не превышает m, то через не более чем m включений возникнет ситуация, когда $L_r = L_{r+1}$, то есть на очередном $r+1$-м шаге базис не увеличится. Очевидно, что в этом случае $L_r = L$. Процесс построения L закончен.

Пусть $L = \{a^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot x^{\sigma^{q_i} \wedge \nu^{t_i}} | i = 1, ..., s\}$. Вычисляем соответствующее разложение

$$a^{\chi} \cdot x^{\psi} = \sum_{i=1}^{s} \alpha_i a^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot x^{\sigma^{q_i} \wedge \nu^{t_i}}, \alpha_i \in \mathbf{F}, i = 1, ..., s. \qquad (38)$$

Подставим в правую часть полученного выражения (38) a^{φ} вместо a и x^{φ} вместо x. Поскольку φ перестановочен с любым автоморфизмом из Φ, получаем:

$$\sum_{i=1}^{s} \alpha_i (a^{\varphi})^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot (x^{\varphi})^{\sigma^{q_i} \wedge \nu^{t_i}} = (\sum_{i=1}^{s} \alpha_i a^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot x^{\sigma^{q_i} \wedge \nu^{t_i}})^{\varphi} =$$

$$(a^{\chi} \cdot x^{\psi})^{\varphi} = (a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi}. \qquad (39)$$

Остается, решив систему линейных уравнений, получить m.

Как отмечалось в [7], «это нетрудно сделать, если в качестве K взять конечномерную алгебру над полем. Можно в качестве K брать и другие кольца, главное, чтобы можно было решать систему линейных уравнений с коэффициентами из этого кольца».

5.3. Система на градуированном кольце с мультипликативным базисом

5.3.1. Система Маркова, Михалева и др. [19]

Предварительные сведения

Пусть R – ассоциативное кольцо с единицей $1 \in R$, G – группа в мультипликативной записи с нейтральным элементом (единицей) $e \in G$. Кольцо R называется *G-градуированным*, если существует такое семейство аддитивных подгрупп $\{R_\sigma, \sigma \in G\}$ аддитивной группы R, что $R = \oplus_{\sigma \in G} R_\sigma$, $R_\sigma R_\tau \subseteq R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. Ясно, что R_e – подкольцо R, а произвольная подгруппа R_σ – бимодуль над R_e для любого $\sigma \in G$.

Мультипликативным базисом конечномерной алгебры называется такой ее базис B, что $B \cup \{0\}$ замкнуто относительно умножения.

Установка. Алиса выбирает градуированное кольцо R относительно конечной группы G с конечным мультипликативным базисом $B = \{b_1, ..., b_n\}$. Предполагается, что группы автоморфизмов $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ достаточно богаты некоммутирующими элементами большого порядка с нетривиальными централизаторами большого порядка. Все эти величины R, G, B, а также градуировка открыты.

Алиса выбирает случайный автоморфизм σ кольца R_e большого порядка, а также случайный автоморфизм ν базиса B также большого порядка. Через $C(\sigma)$ обозначим централизатор элемента σ в группе $\mathrm{Aut}(R_e)$, а через $C(\nu)$ – централизатор автоморфизма ν в $\mathrm{Aut}(B)$. Считаем, что оба этих централизатора строго больше, чем подгруппы $\mathrm{gp}(\sigma)$ и $\mathrm{gp}(\nu)$ соответственно.

Генерация ключей. Алиса выбирает случайным образом автоморфизм $\tau \in C(\sigma)$, непринадлежащий $\mathrm{gp}(\sigma)$, и автоморфизм $\omega \in C(\nu)$, не принадлежащий $\mathrm{gp}(\nu)$. Затем она задаёт автоморфизм φ алгебры R следующим образом: для любого $h \in R$ вида $h = a_{b_1} b_1 + ... + a_{b_n} b_n$, где $a_{b_i} \in R_e, i = 1, ..., n$, определяет

$$h^{\varphi} = a_{b_1}^{\tau} b_1^{\omega} + ... + a_{b_n}^{\tau} b_n^{\omega}. \tag{40}$$

Далее Алиса выбирает элементы $x, a \in R$ с нулевыми левыми аннуляторами и вычисляет $x^{\varphi}, a^{\varphi} \in R$.

Открытым ключом для Алисы служит

$$(\sigma, \nu, x, x^{\varphi}, a, a^{\varphi}).$$

Шифрование. Боб для шифрования своего сообщения, закодированного в виде элемента m кольца R, выбирает две упорядоченные пары случайных натуральных чисел (i, j) и (k, l), по которым определяет сессионные автоморфизмы ψ и χ кольца R, полагая для любого элемента $h = a_{b_1} b_1 + ... + a_{b_n} b_n$, где $a_{b_i} \in R_e, i = 1, ..., n$,

$$h^{\psi} = a_{b_i}^{\sigma^i} b_1^{\nu^j} + ... + a_{b_n}^{\sigma^i} b_n^{\nu^j}, h^{\chi} = a_{b_i}^{\sigma^k} b_1^{\nu^l} + ... + a_{b_n}^{\sigma^k} b_n^{\nu^l}. \tag{41}$$

После этого Боб вычисляет x^{ψ}, a^{χ}, используя открытый ключ Алисы. Набор параметров (i, j, k, l, ψ, χ) считается секретным сессионным ключом.

Зашифрованное сообщение m имеет вид

$$c = (a^{\chi} \cdot x^{\psi}, m \cdot ((a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi})). \tag{42}$$

Расшифрование. Алиса, получив зашифрованное сообщение (42), вычисляет, пользуясь перестановочностью автоморфизмов φ, ψ и χ, очевидной из их построения, элемент

$$(a^{\chi} \cdot x^{\psi})^{\varphi} = (a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi}.$$

Для прочтения сообщения m Алисе достаточно решить систему линейных уравнений с коэффициентами из кольца R_e. Однозначность решения обеспечивается тривиальностью левого аннулятора элемента $(a^{\varphi})^{\chi} \cdot (x^{\varphi})^{\psi}$, вытекающей из тривиальности левых аннуляторов его сомножителей.

Криптографический анализ. Обозначим через $\sigma^i \wedge \nu^j, i, j \geq 0$, автоморфизмы кольца R, задаваемые указанным выше способом. Предположим, что R – алгебра над конечным полем $\mathbf{F}$ конечной размерности m. Также предполагаем, что любой автоморфизм R будет автоморфизмом R как алгебры над $\mathbf{F}$. Это условие выполнено автоматически, если $\mathbf{F}$ – простое конечное поле. Поэтому достаточно требовать, чтобы R было алгеброй над простым конечным полем.

Определим на группе Φ всех автоморфизмов вида $\sigma^i \wedge \nu^j, i, j \geq 0$, для произвольного $r \geq 0$ сферу и шар радиуса r, как это было сделано в криптографическом анализе протокола Росошека и системы Грибова, Золотых и Михалева, описанном выше.

Дальнейший анализ буквально повторяет рассуждения из криптоанализа системы Грибова, Золотых и Михалева. Для элементов $a, x \in R$ вычисляется базис подпространства $V = \mathrm{Sp}_{\mathbf{F}}(a^\Phi \cdot x^\Phi) : L = \{a^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot x^{\sigma^{q_i} \wedge \nu^{t_i}} | i = 1, ..., s\}$. Далее вычисляем соответствующее разложение вида (38). После подстановки в правую часть этого разложения элементов x^φ вместо x и a^φ вместо a и аналогичных вычислений получаем элемент $(a^\varphi)^\chi \cdot (x^\varphi)^\psi$. Затем решаем систему линейных уравнений, получая в итоге m.

§ 6. Диофантова криптография

6.1. 10-я Проблема Гильберта

Диофантовым уравнением от n переменных называется выражение вида

$$d(\zeta_1, ..., \zeta_n) = 0, \tag{43}$$

где $d(\zeta_1, ..., \zeta_n)$ – многочлен с целыми коэффициентами от обозначенных независимых коммутирующих переменных. Такой многочлен назовем *Диофантовым*. Множество всех Диофантовых многочленов от n переменных составляет кольцо $\Lambda_n = \mathbf{Z}[\zeta_1, ..., \zeta_n]$. Кольцо Λ_m при $m \leq n$ естественно вложено в кольцо Λ_n. Объединение всех таких колец обозначим через $\Lambda = \mathbf{Z}[\zeta_1, ..., \zeta_n, ...]$.

На Втором математическом конгрессе, состоявшемся в 1900 году в Париже, выдающийся математик Д. Гильберт изложил свои знаменитые 23 математические проблемы для математиков 20-го 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 (43) его разрешимость в целых числах.

Алгоритмическая неразрешимость 10-й Проблемы Гильберта установлена Ю.В. Матиясевичем в работах [20], [21] (см. также [22]). Было доказано, что алгоритма, определяющего для произвольного Диофантова уравнения, имеет ли оно решение в целых числах, не существует. Тем самым Матиясевичем были успешно завершены усилия многих математиков, из которых наиболее весомый вклад в решение проблемы внесли Д. Робинсон, М. Девис и Х. Путнам.

6.2. Универсальность Диофантова языка

Вернемся к криптографии. Почти всегда криптографическая система с открытым ключом основывается на трудноразрешимой математической проблеме, часто теоретико-числового характера. Мы приведем список наиболее популярных проблем такого типа. Также покажем, что с каждой из них можно связать Диофантово уравнение таким образом, что любое решение этого уравнения дает 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 (43): если взять квадраты этих левых частей и приравнять их сумму к 0, то мы можем эффективно сопоставлять любому конечному множеству проблем, о которых говорилось выше, одну равносильную им проблему – о разрешимости в целых числах полученного Диофантова уравнения.

Приведенное рассуждение показывает, что Диофантов язык является универсальным в определенном смысле. Он может быть применен 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.

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

Во многих приложениях p и q – различные нечетные простые числа. Пусть

$$\mathbf{Z}^{(2)} = \{n = pq | p, q \ - \text{различные нечетные простые числа}\}. \quad (44)$$

Приведем еще один вариант проблемы разложения на множители.

- Найти для случайно выбранного числа $n \in \mathbf{Z}^{(2)}$ его множители p и q.

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

$$(\zeta_1^2 + \zeta_2^2 + \zeta_3^2 + \zeta_4^2 + 3) \cdot (\zeta_5^2 + \zeta_6^2 + \zeta_7^2 + \zeta_8^2 + 3) = n. \qquad (45)$$

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, осуществленные с помощью мощных параллельных вычислений. Однако до сих пор не найден эффективный алгоритм для ее решения в целом. Это дает основание считать, что проблема действительно трудна.

- **Проблема расшифрования в RSA.** Пусть $n = pq \in \mathbf{Z}^{(2)}$. Кольцо вычетов $\mathbf{Z}_n$ используется в системе шифрования RSA в качестве платформы шифрования. Мультипликативная группа $\mathbf{Z}_n^*$ кольца $\mathbf{Z}_n$ 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 $x \in \mathbf{Z}_n$, кодирующего исходный текст, по его зашифрованному виду

$$c = x^e (\mathrm{mod} n). \qquad (46)$$

Эта проблема равносильна разрешимости Диофантова уравнения

$$x^e = c + ny \tag{47}$$

относительно неизвестных x и y.

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

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

$$x^2 = a(\mathrm{mod} n). \tag{48}$$

Проблема квадратичного вычета равносильна разрешимости Диофантова уравнения

$$x^2 = a + ny. \tag{49}$$

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

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

- **Дискретный логарифм в простом конечном поле.** Пусть p – простое число, тогда $\mathbf{Z}_p$ – простое конечное поле характеристики p. Мультипликативная группа $\mathbf{Z}_p^*$ циклическая. Пусть g – порождающий элемент этой группы. *Дискретным логарифмом* элемента $f \in \mathbf{Z}_p$ называется число x, для которого

$$g^x = f(\mathrm{mod} p). \tag{50}$$

Число x определяется по модулю числа $p-1$ – порядка группы $\mathbf{Z}_p^*$. *Проблемой дискретного логарифма* в поле $\mathbf{Z}_p$ называется вопрос о вычислении x по случайно выбранному элементу f. Элемент 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 $0 \leq x \leq p-2$. Проблема дискретного логарифма в простом конечном поле $\mathbf{Z}_p$ равносильна разрешимости *экспоненциального Диофантова уравнения*

$$g^x = f + py. \tag{51}$$

Проблема дискретного логарифма может рассматриваться также для любого конечного поля. Мы также можем записать эквивалентное ему экспоненциальное Диофантово уравнение. Здесь мы не говорим об этом более подробно.

Из результатов Ю.В. Матиясевича [20], [21] следует, что множество E всех решений x, y уравнения (51) является Диофантовым. В общем случае *Диофантовым* называется множество наборов $\bar{a} = (a_1, ..., a_k)$ целых чисел, для которого существует Диофантов многочлен $d(\zeta_1, ..., \zeta_k, \kappa_1, ..., \kappa_n)$ такой, что набор целых чисел $\bar{a} = (a_1, ..., a_k)$ принадлежит множеству E в том и только том случае, если найдутся целые значения $b_1, ..., b_n$ для $\kappa_1, ..., \kappa_n$ такие, что $d(a_1, ..., a_k, b_1, ..., b_n) = 0$, то есть соответствующее Диофантово уравнение разрешимо в целых числах. По теореме Матиясевича любое рекурсивно перечислимое (вычислимое) множество E наборов из k целых чисел является Диофантовым множеством. Существование такой характеризации рекурсивно перечислимых множеств дает еще 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 (51), см. [8], [9].

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, основанные на базовом протоколе ЭльГамаля стандарты цифровой подписи DSS и ГОСТ Р 34.10-94 и т. д.

Есть еще одно важное обстоятельство, говорящее в пользу использования алгоритмической неразрешимости 10-й Проблемы Гильберта в качестве основы для построения криптографических примитивов, систем и протоколов. Как недавно показал А.Н. Рыбалов [39], 10-я Проблема Гильберта остается неразрешимой на любом строго генерическом множестве Диофантовых уравнений.

Каждый Диофантов многочлен $d(\zeta_1, ..., \zeta_k)$ может рассматриваться как функция из $\mathbf{Z}^k$ в $\mathbf{Z}$. Ю.В. Матиясевич [20], [21] доказал, что существует такой Диофантов многочлен $d_0(\zeta_1, ..., \zeta_k)$, что не существует алгоритма нахождения решения в целых числах уже в классе уравнений вида $d_0(\zeta_1, ..., \zeta_k) = c$, где $c \in \mathbf{Z}$. Таким образом можно определить функцию $\mathbf{Z}^k \to \mathbf{Z}$, 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 $d_0(\zeta_1, ..., \zeta_k)$.

6.3. 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 $|y|$, вычис-

ляет x' с условием $y = f(x')$ с пренебрежимо малой вероятностью.

В первом томе монографии О. Голдрейха [71] даны следующие определения.

Определение 6.1. *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 (входу) x значение $y = f(x)$;

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

$$Prob(\mathcal{B}(f(U_n), 1^n) \in f^{-1}(f(U_n)) < \frac{1}{p(n)}, \tag{52}$$

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 [71] 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 6.1, 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 [96], [97], [121].

Определение 6.2. *Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется слабо односторонней, если выполнены следующие требования:*

а) = а) из Определения 6.1;

b) существует полином $p(\cdot)$ такой, что для любого вероятностного полиномиального по времени алгоритма $\mathcal{B}$, и всех до-

статочно больших натуральных чисел n выполняется неравенство

$$Prob(\mathcal{B}(f(U_n), 1^n) \notin f^{-1}(f(U_n)) > \frac{1}{p(n)}. \qquad (53)$$

В [71] доказано, что существование слабо односторонней функции влечет существование сильно односторонней функции.

Приведенные определения связаны с бинарным представлением аргументов и значений функций. Для задания возможно односторонней функции, определенной на группе, можно использовать следующие соображения. Во-первых, на конечно порожденной группе G с фиксированным множеством порождающих элементов можно задать словарную метрику, согласно которой расстояние $|g|$ от элемента g до 1 (его длина) равно 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 S_r и шары B_r радиуса r, которые дадут стратификацию множества элементов группы. Определения 6.1. и 6.2. переписываются следующим образом.

Определение 6.3. *Функция $\varphi : G \to G$ называется сильно односторонней, если выполнены следующие требования:*

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

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

$$Prob(\mathcal{B}(\varphi(U_n), B_n) \in \varphi^{-1}(\varphi(U_n)) < \frac{1}{p(n)}, \qquad (54)$$

где U_n означает случайную величину, равномерно распределенную на B_n. Как и раньше, алгоритму предписан размер его выхода.

Определение 6.4. *Функция $\varphi : G \to G$ называется слабо односторонней, если выполнены следующие требования.*

a) = a) из Определения 6.1;

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

$$Prob(\mathcal{B}(\varphi(U_n), B_n) \notin \varphi^{-1}(\varphi(U_n)) > \frac{1}{p(n)}. \tag{55}$$

Во многих случаях приведенные определения сводятся к Определениям 6.1. и 6.2. кодированием элементов группы бинарными последовательностями.

Известными кандидатами на роль односторонних являются следующие функции.

Степенная функция

$$f : x \longmapsto c = x^e \pmod{n}, \tag{56}$$

определенная на кольце Z_n вычетов по модулю n, где $n = pq$ – произведение больших различных (секретных) простых чисел. Для ее обратимости требуется взаимная простота показателя e со значением функции Эйлера $\varphi(n) = (p-1)(q-1)$.

Задача обращения функции (56) (см. [47]) равносильна нахождению решения Диофантова уравнения

$$c = \zeta_1^e + n\zeta_2 \tag{57}$$

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

$$d(\zeta_1, \zeta_2) = \zeta_1^e + n\zeta_2. \tag{58}$$

Функция (56) 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

$$g : x \longmapsto g^x, \tag{59}$$

определенная на кольце целых чисел Z со значениями в конечном поле F_q порядка q, где g – порождающий элемент мультипликативной (циклической) группы F_q^*. Криптостойкость ее основана на трудности вычисления дискретного логарифма в конечных полях.

Ее обращение равносильно обращению некоторой Диофантовой функции $d(\zeta_1, ..., \zeta_k)$. Это следует из результатов Ю.В. Матиясевича [20], [21].

В случае простого конечного поля $F_p = Z_p$ характеристики p явный вид полинома $d(\zeta_1, ..., \zeta_k)$ можно найти в [8], [9].

Функция (59) используется, например, в системе шифрования Эль Гамаля, протоколах Диффи-Хеллмана-Меркля, Масси-Омуры, базовом протоколе Эль Гамаля цифровой подписи и других схемах (см. по этому поводу [34], [105]).

Мы видим, что два приведенных выше примера криптографических функций являются частными случаями Диофантовых функций. Диофантова криптография 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.

С.Ю. Ерофеев в работе [10] рассмотрел различные возможности построения не только возможно односторонних, но также 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 композиции аргумент самой композиции также является эффективно невычислимым. Необходимость построения таких функций объясняется тем, что в ряде предлагаемых протоколов, например, в протоколе аутентификации с нулевым разглашением из [73], наличия обычных односторонних функций недостаточно.

6.4. Метабелевы группы

Настоящий раздел связан с базовыми понятиями теории групп, относительно которых см., например, [12] или [14]. Подходят и другие книги, излагающие основы теории групп. Элементы теории групповых многообразий см., например, в [26]. Сведения о разрешимых (в том числе нильпотентных и метабелевых) группах содержатся в [93].

6.4.1. Свободные метабелевы группы

Для произвольного натурального числа n через F_n обозначается свободная группа ранга n. Ее 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

$$1 \leq A \leq G \tag{60}$$

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 том случае, если ее коммутант G' абелев. В определении (60) 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 $(f_1, ..., f_n)$ – *базис*, т. е. *множество свободных порождающих* группы F_n, то $(a_1, ..., a_n) = (f_1F'_n, ..., f_nF'_n)$ соответствующий базис группы A_n. Аналогично определим базис $(x_1, ..., x_n) = (f_1F''_n, ..., f_nF''_n)$ группы M_n. Также мы имеем $(a_1, ..., a_n) = (\pi_n(x_1), ..., \pi_n(x_n)$.

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.

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

$$g = \prod_{i=1}^{n} x_i^{k_i} u, \tag{61}$$

где $k_i \in \mathbf{Z}$ для $i = 1, ..., n$; элемент $u = u(g)$ принадлежит коммутанту M'_n. Чтобы получить из (61) нормальную форму записи элемента g, достаточно построить такую форму для элемента u.

Так как M'_n нормальная абелева подгруппа группы M_n, ее можно рассматривать как модуль над групповым кольцом $\mathbf{Z}A_n$. 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. Мы берем произвольный прообраз $\bar{a}$ элемента a в группе M_n относительно канонического гомоморфизма π_n. Затем полагаем

$$v^a = v^{\bar{a}}. \tag{62}$$

Так как все возможные прообразы $\bar{a}$ отличаются друг от друга на элементы из M'_n, сопряжение в (62) не зависит от выбора $\bar{a}$. Следовательно, приведенное определение корректно. Продолжение действия на групповое кольцо $\mathbf{Z}A_n$ осуществляется по линейности, а именно для любого набора элементов $b_j \in A_n$ и любого набора целых чисел $l_j \in \mathbf{Z}$ $(j = 1, ..., p)$ полагаем

$$v^{\sum_{j=1}^{p} l_j b_j} = \prod_{j=1}^{p} (v^{b_j})^{l_j}, \tag{63}$$

причем правая часть в (63) не зависит от порядка сомножителей, что обеспечивает корректность определения.

Коммутант M'_n более естественно рассматривать как модуль над $\mathbf{Z}A_n$ 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 порожден. В качестве его порождающих элементов можно взять набор коммутаторов вида

$$e_{ij} = [x_i, x_j], \quad i > j, \ i, j = 1, ..., n. \tag{64}$$

Покажем, как произвольное слово $v = v(x_1, ..., x_n)$, записывающее элемент коммутанта M'_n, представляется через порождающие модуля (64). Вначале мы переставляем влево все вхождения $x_1^{\pm 1}$, пользуясь формулами:

$$x_i x_1 = [x_i, x_1] x_1 x_i, x_i^{-1} x_1 = [x_i^{-1}, x_1] x_1 x_i^{-1} =$$

$$= [x_i, x_1]^{-a_i^{-1}} x_1 x_i^{-1},$$

$$x_i x_1^{-1} = [x_i, x_1^{-1}] x_1^{-1} x_i = [x_i, x_1]^{-a_1^{-1}} x_1^{-1} x_i,$$

$$x_i^{-1} x_1^{-1} = [x_i^{-1}, x_1^{-1}] x_1^{-1} x_i^{-1} = [x_i, x_1]^{a_1^{-1} a_i^{-1}} x_1^{-1} x_i^{-1}. \tag{65}$$

Возникающие при этом коммутаторы $e_{ij} = [x_i, x_1]$ передвигаются вправо согласно формуле

$$[x_i, x_1]f = f[x_i, x_1]^{f^{-1}}, \tag{66}$$

справедливой при любом $i = 2, ..., n$ и любом $f \in M_n$. После того, как будут переставлены все вхождения $x_1^{\pm 1}$, произойдет сокращение этих степеней и таких вхождений уже не будет. Мы продолжим процесс переписки, переводя влево $x_2^{\pm 1}$, и т. д. В результате получим выражение вида

$$v = \prod_{i>j, i,j=1,...,n} e_{ij}^{\alpha_{ij}}, \tag{67}$$

где $\alpha_{ij} \in \mathbf{Z}A_n$. для $i > j, i, j = 1, ..., n$.

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 (64) все его определяющие соотношения следуют из следующих соотношений Якоби:

$$e_{ij}^{a_k - 1} e_{jk}^{a_i - 1} e_{ki}^{a_j - 1} = 1. \tag{68}$$

Ввиду этих соотношений форма (67) 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.

Предложение 6.1. *Любой элемент коммутанта M_n' однозначно представим в виде*

$$v = \prod_{i>j, i,j=1,...,n} e_{ij}^{\alpha_{ij}}, \tag{69}$$

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

Доказательство. Пусть элемент v записан в форме (67). Покажем вначале, 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 (68) получаем равенство

$$e_{21}^{a_3^k h} = e_{21}^{a_3^{k-1}h} e_{31}^{(a_2-1)a_3^{k-1}h} e_{32}^{-(a_3-1)a_3^{k-1}h}. \tag{70}$$

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

Пусть $k < 0$. Равенства (68) остаются справедливыми, если в них заменить x_3 и a_3 соответственно на x_3^{-1} и на a_3^{-1}. Следовательно, мы можем исключить из рассматриваемого показателя a_3^k, как это делалось выше, а затем использовать равенства

$$[x_3^{-1}, x_i] = [x_3, x_i]^{-a_3^{-1}} \text{ для } i = 1, 2. \tag{71}$$

Подобным образом мы исключим из показателя элемента e_{21} все элементы вида $a_i^{\pm 1}$ для $i = 3, ..., n$. Оставшийся показатель будет принадлежать групповому кольцу $\mathbf{Z}A_2$. Далее мы исключаем подобным образом $a_i^{\pm 1}$ для $i \geq 4$ из показателей степеней при e_{31} и e_{32}. В конце концов мы получим запись элемента v в форме (69). Докажем, что полученная запись единственная. Вначале применим к (69) гомоморфизм специализации группы M_n, определенный на базисных элементах как $x_i \mapsto x_i$ для $i = 1, 2$ и $x_j \mapsto 1$ для $j \geq 3$. Образом элемента v будет $e_{21}^{\alpha_{21}}$. Так как все соотношения в модуле M_n' следуют из соотношений Якоби, подмодуль, порожденный в M_n' любым из элементов e_{ij}, свободен. Значит, показатель α_{21} определяется однозначно.

Далее мы 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 $j \geq 4$. 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, порожденный в M_n' набором элементов $e_{i1}, ..., e_{ii-1}$, является свободным на этих порождающих. Значит, показатели α_{31} и α_{32} определяются по элементу v однозначно. Продолжая доказательство подобным образом, мы установим однозначность записи (69).

Предложение доказано.

Полученная форма записи элементов группы может рассматриваться как нормальная форма элементов группы M_n.

6.4.2. Базисные коммутаторы

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

$$G = \gamma_1 G \geq \gamma_2 G \geq ...\gamma_k G \geq ..., \tag{72}$$

в которой $\gamma_{i+1}G = [\gamma_i G, G]$ – подгруппа, порожденная всеми коммутаторами вида $[g, f]$, где $g \in \gamma_i G, f \in G$. Ряд (72) 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, [12]) коммутаторные тождества, справедливые в любой группе G.

$$\begin{gathered}[xy, z] = [y, z]^x [x, z] = [[y, z], x]^{-1} [y, z][x, z], \\ [x^{-1}, z] = [x, z]^{-1} [[x, z], x^{-1}], \\ [z, x^{-1}] = [[x, z], x^{-1}]^{-1} [x, z].\end{gathered} \tag{73}$$

Одним из следствий тождеств (73) является следующая относительная дистрибутивность:

$$[g_1^{k_1}, ..., g_l^{k_l}] = [g_1, ..., g_l]^{\prod_{i=1}^{l} k_i} (\mathrm{mod} \gamma_{l+1} G), \tag{74}$$

где $g_1, ..., g_l$ – произвольные элементы группы G, а $k_1, ..., k_l$ – целые числа.

Мы предполагаем, что в левой части стоит *простой* коммутатор, т. е. коммутатор вида

$$[...[[a_1, a_2], a_3], ..., a_l],$$

в котором скобки стоят слева направо. Такие коммутаторы еще называют *левонормированными*. Однако, равенство (74) остается верным при любой расстановке скобок, важно только, чтобы все операции с символами были коммутаторными.

Известно (см. [12], [26]), что в метабелевых группах выполняется тождество

$$[f, h, g_1, g_2, ..., g_l] = [f, h, g_{\sigma(1)}, ..., g_{\sigma(l)}], \tag{75}$$

где σ – произвольная перестановка символов $1, ..., l$.

Для свободных порождающих $x_1, ..., x_n$ группы M_n определяются *базисные коммутаторы* – простые коммутаторы от элементов базиса $x_1, ..., x_n$ вида

$$[x_{i_1}, x_{i_2}, x_{i_3}, ..., x_{i_l}], \tag{76}$$

где $l \geq 2$ называется *весом* коммутатора, и выполняются неравенства: $i_1 > i_2; i_2 \leq i_3 \leq ... \leq i_l$. Сами порождающие $x_1, ..., x_n$ также считаются базисными коммутаторами веса 1. Хорошо известно (см. [44], [78]), 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 $c_1, ...c_t (t = t(i))$ – полный список всех базисных коммутаторов веса не больше, чем i, в заданном порядке. Обычно считают, что $c_j = x_j$ для $j = 1, ..., n$, то есть что порядок на порождающих элементах как базисных коммутаторах веса 1 соответствует порядку на индексах. Тогда любой элемент

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

$$g = \prod_{j=1}^{t} c_j^{k_j} (\mathrm{mod} \gamma_{i+1} M_n), \quad k_j \in \mathbf{Z}. \tag{77}$$

Таким образом по модулю $\gamma_{i+1} M_n$ элементы группы M_n кодируются наборами целых чисел $(k_1, ..., k_t)$, $t = t(i)$. 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 $\mathbf{Z}^t \to \mathbf{Z}^t$, 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 ее элементов, соответствующей (77), ее отображениях и т. п. Группа $M_{n,i}$ является свободной группой ранга n многообразия всех метабелевых нильпотентных ступени $\leq i$ групп, которое есть пересечение многообразия $\mathcal{A}^2$ всех метабелевых групп и многообразия $\mathcal{N}_i$ всех нильпотентных групп ступени $\leq i$.

Пусть два элемента g и f группы M_n записаны в виде (77), причем элемент g имеет координаты $(k_1, ..., k_t)$, а элемент f – координаты $(q_1, ..., q_t)$. Тогда эффективно определяются многочлены $p_j = p_j(\zeta_1, ..., \zeta_{t(j)}, \kappa_1, ..., \kappa_{t(j)})$ для $j = 1, ..., t$, такие, что координаты $(r_1, ..., r_t)$ произведения $h = gf$ вычисляются по формулам:

$$r_j = p_j(k_1, ..., k_{t(j)}, q_1, ..., q_{t(j)}). \tag{78}$$

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

Аналогично, существуют многочлены $u_j(\zeta_1, ..., \zeta_t)$ для $j = 1, ..., t$, 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 [78], монографию [44].

Важно отметить, что в рассматриваемом случае групповые операции переписываются через Диофантовы функции. Это позволяет переходить от групповых уравнений к Диофантовым уравнениям. Вопрос о разрешимости группового уравнения таким образом сводится к решению соответствующего Диофантова уравнения. Здесь также проявляется универсальность Диофантова языка.

6.4.3. Вложение Магнуса

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 [42].

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

$$\begin{pmatrix} a & \sum_{i=1}^{n} \alpha_i t_i \\ 0 & 1 \end{pmatrix}, \tag{79}$$

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

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, [12]. Легко проверяется, что группа $M(A_n, T_n)$ метабелева. Все матрицы вида (79) 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 $\mathbf{Z}A_n$ с базисом $t_1, ..., t_n$. 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:

$$\mu : x_i \mapsto \begin{pmatrix} a_i & t_i \\ 0 & 1 \end{pmatrix}, \quad i = 1, ..., n. \tag{80}$$

Вложение Магнуса также позволяет ввести нормальную форму элементов группы M_n как матриц вида (80). Важно отметить для этого, что матрица вида (79) принадлежит образу $\mu(M_n)$ тогда и только тогда, когда выполнено равенство

$$a - 1 = \sum_{i=1}^{n} \alpha_i (a_i - 1). \tag{81}$$

Для того, чтобы считать группу $M(A_n, T_n)$ матричной над полем, возьмем поле частных $\mathbf{F}$ группового кольца $\mathbf{Z}A_n$ и его чисто трансцендентное расширение $\bar{\mathbf{F}} = \mathbf{F}(t_1, ..., t_n)$. Тогда группа $M(A_n, T_n)$ оказывается подгруппой полной матричной группы $GL_2(\bar{\mathbf{F}})$.

6.4.4. Свободные метабелевы группы как возможные платформы для шифрования

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 [42].

Например, с помощью вложения Магнуса легко доказать, что моноид X_n^*, порожденный в группе M_n множеством свободных порождающих $X_n = \{x_1, ..., x_n\}$, 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 дает возможности для построения

криптографических примитивов, а затем на их основе систем и протоколов.

Есть еще 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 [110] показано, что проблема равенства в группе M_n решается за время $O(nmlog_2m)$, 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 [141] установлено, что проблема сопряженности в группе M_n решается за время $O(nm^8)$, где m обозначает сумму длин двух слов, для которых проверяется сопряженность записываемых ими элементов группы M_n. Доказательство в [141] конструктивны, что позволяет дать точно такую же оценку времени решения соответствующей проблемы поиска сопряженного элемента. Приведенные здесь результаты говорят о том, что мы можем эффективно работать с элементами групп M_n, их нормальными формами и сопряженными элементами. Также известны [31] эффективные алгоритмы, решающие в группах M_n проблему вхождения.

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

В заключение этого пункта отметим, что классические алгоритмические проблемы равенства, сопряженности и вхождения разрешимы в любой конечно порожденной метабелевой группе. Проблема равенства решена Е.И. Тимошенко [41]. Разработанный им алгоритм, сводящий проблему к решению системы ли-

нейных уравнений над групповым кольцом $\mathbf{Z}A_n$ свободной абелевой группы вполне пригоден для его практического использования. Проблема сопряженности решена Г.А. Носковым [29], 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 [5] описан алгоритм, решающий в конечно порожденной метабелевой группе более общую, чем проблема сопряженности, проблему скрученной сопряженности. По представлению автора такой более общий подход дает возможность его практического использования по крайней мере на генерическом множестве. Проблема вхождения решена Н.С. Романовским [31]. На практичность она не исследована, но, по-видимому, может быть реализована для такой цели. Также разрешимы многие другие алгоритмические проблемы [50]. См. соответствующий обзор в [30]. Правда, с точки зрения теории сложности общий случай еще исследован недостаточно. В классе всех конечно порожденных метабелевых групп разрешима проблема изоморфизма данной свободной метабелевой группы M_n [75]. Разрешимость проблемы изоморфизма в этом классе остается открытым вопросом. См. по этому поводу [52].

6.5. Уравнения в группах

6.5.1. Основные понятия

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

$$w = w(z_1, ..., z_r) = 1, \tag{82}$$

где w – групповое слово от неизвестных $z_1, ..., z_r$ и элементов группы G. Если ввести в рассмотрение свободную группу F с базисом $\{z_1, ..., z_r, ...\}$, то w может рассматриваться как элемент свободного произведения

$$G[z_1, ..., z_r, ...] = F * G.$$

Решением уравнения (82) называется набор элементов $g_1, ..., g_r$ группы G, для которого $w(g_1, ..., g_r) = 1$. Решению $g_1, ..., g_r$ соответствует гомоморфизм

$$\varphi : G[z_1, ..., z_r, ...] \to G,$$

при котором элементы группы G отображаются сами на себя, на группе F гомоморфизм определяется своими значениями $z_i \mapsto g_i$, $i = 1, ..., r$, и произвольными значениями остальных порождающих z_j для $j \geq r+1$. Наоборот, каждому гомоморфизму φ группы $G[z_1, ..., z_r, ...]$ в группу G, тождественному на элементах группы G, отвечает решение $g_i = \varphi(z_i)$, $(i = 1, ..., r)$. Уравнение (82) называется *разрешимым*, если для него существует хотя бы одно решение, и *неразрешимым* в противном случае.

6.5.2. Алгоритмические проблемы, связанные с уравнениями

Мы заметили, что классические алгоритмические проблемы в свободных метабелевых группах разрешимы. См. обзор по уравнениям в группах [119]. Однако, оказалось, что некоторые другие естественные по своей постановке алгоритмические проблемы в этих группах неразрешимы. Первые такие примеры указаны автором в [32], [33]. Это алгоритмические проблемы разрешимости произвольного уравнения в группе M_n при $n \geq 2$ и разрешимость проблемы эндоморфной сводимости в группе M_n достаточно большого ранга $n \geq n_0$.

Соответственно ставится следующая алгоритмическая проблема:

- **Проблема разрешимости уравнений.** Разрешимо ли произвольное уравнение (82) в данной группе G.

Проблема разрешимости уравнений может ставится также для класса групп $\mathcal{L}$. Тогда это будет вопрос о существовании алгоритма, который по произвольной группе G из данного класса $\mathcal{L}$ и

произвольному уравнению (82) 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

$$w(z_1, ..., z_r) = f, \tag{83}$$

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 (82) *относительное уравнение*

$$w(z_1, ..., z_r) = 1(\mathrm{mod}\gamma_{i+1}G), \tag{84}$$

для которого естественно определяется понятие *разрешимости*. Ясно, что разрешимость уравнения (82) влечет разрешимость уравнения (84) для любого i. Обратное утверждение в общем случае неверно. Разрешимость уравнения (84) 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, мы видим, что разрешимость относительных уравнений в группе равносильна разрешимости уравнений в фактор группе. Выше мы рассматривали 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

(84) 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 $v = v(z_1, ..., z_r)$, называется подгруппа, порожденная всеми *значениями* $v(g_1, ..., g_r)$ слова v в группе G. Подгруппа $v(G)$ имеет *конечную ширину* $l = width(v(G))$, если любой элемент $u \in v(G)$ представим как произведение $\leq l$ 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 ([138], доказательство можно найти также в [122]), 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 $l_{n,i} = width(\gamma_i M_n)$ относительно слова $v_i = [z_1, ..., z_i]$. Более точно, в работе [3] показано, что при $n \geq 2$ $l_{n,2} = [n/2]$ и при $i \geq 3$ $l_{n,i} = n$.

Это означает, что если взять слово

$$V_{n,i} = \prod_{j=1}^{l_{n,i}} [z_{j,1}^{(1)}, z_{j,2}^{(1)}, ..., z_{j,i}^{(1)}][z_{j,1}^{(2)}, z_{j,2}^{(2)}, ..., z_{j,i}^{(2)}]^{-1} \tag{85}$$

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

$$u = \prod_{j=1}^{l_{n,i}} [z_{j,1}^{(1)}, z_{j,2}^{(1)}, ..., z_{j,i}^{(1)}][z_{j,1}^{(2)}, z_{j,2}^{(2)}, ..., z_{j,i}^{(2)}] \tag{86}$$

разрешимо в группе M_n тогда и только тогда, когда элемент u принадлежит подгруппе $\gamma_i M_n$. Отсюда получаем, что относительное уравнение (84) разрешимо в группе M_n тогда и только тогда, когда в M_n разрешимо уравнение

$$w(z_1, ..., z_r)V_{n,i} = 1. \tag{87}$$

Разрешимость относительного бескоэффициентного уравнения (83) равносильна разрешимости бескоэффициентного уравнения

$$w(z_1, ..., z_r)V_{n,i} = f. \tag{88}$$

Рассмотрим относительное уравнение

$$w(z_1, ..., z_r) = 1(\mathrm{mod}\gamma_{i+1}G). \tag{89}$$

Перепишем в нормальной форме (77) все константы, входящие в запись (89), и все неизвестные $z_1, ..., z_r$, полагая $z_k = \prod_{j=1}^{t} c_j^{\zeta_{k,j}}$ $(\mathrm{mod}\gamma_{i+1})$ с неизвестными показателями степеней $\zeta_{k,j}$ $(k = 1, ..., r; j = 1, ..., t)$, где $t = t(i)$. Другими словами, запишем константы и неизвестные в введенной выше координатной форме. Затем приведем левую часть уравнения к нормальному виду (77), используя многочлены (78). Решению уравнения (89) соответствует тривиальная нормальная форма. Значит, все показатели полученной нормальной формы должны равняться нулю. Разрешимость уравнения (89) 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 уравнений и обычных уравнений в группе M_n, отмеченная выше, позволяет получать те же системы Диофантовых уравнений и для уравнений в группе M_n.

Остается 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 [32] и [33]. А именно, в [33] показано, что по любому Диофантову уравнению (43) можно явно указать такое групповое слово $w(z_1, ..., z_r)$, не зависящее от констант, и такой элемент f группы M_n для произвольного $n \geq 2$, что уравнение (83) разрешимо в группе M_n тогда и только тогда, когда Диофантово уравнение (43) разрешимо в целых числах. Более того, мы можем зафиксировать левую часть уравнения (83), а

элемент f выбирать из фиксированного смежного класса по циклической подгруппе $\mathrm{gp}(h)$ 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 счетного ранга (или достаточно большого конечного ранга) с базисом $\{x_1, ..., x_r, ...\}$, то неразрешимость проблемы эндоморфной сводимости в ней вытекает из неразрешимости проблемы разрешимости бескоэффициентных уравнений в M_2. Действительно, для произвольных элементов $g = g(x_1, ..., x_r)$, и $f = f(x_1, ..., x_r)$ группы M элемент f является эндоморфным образом элемента g тогда и только тогда, когда он является таковым, если рассматривать группу M_r с базисом $\{x_1, ..., x_r\}$. В свою очередь, это равносильно разрешимости в M_r уравнения

$$g(z_1, ..., z_r) = f. \tag{90}$$

Как мы заметили выше, эта проблема неразрешима уже в группе M_2. Число неизвестных также можно ограничить, поскольку, как показано в [81], 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 $i = 1, ..., n$ взаимно однозначно соответствуют наборы целых чисел из (77). 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, если его рассматривать по модулю $\gamma_{i+1}M_n$, он может считаться отображением множества $\mathbf{Z}^t$ в себя. Это отображение в свете существования Диофантовых функций (78) является Диофантовым отображением. Семейство таких отображений, среди которых, как мы знаем, есть такие, что проблема нахождения для них прообразов по данному значению алгоритмически неразрешима, дает богатую возможность построения функций, претендующих на роль односторонних. Другие возможности связаны с рассмотрением других нормальных форм элементов группы M_n, о которых говорилось выше.

6.6. Протокол аутентификации

Далее предлагается новый кандидат на роль односторонней функции. В качестве платформы для нее 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 автора [33], 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 [33] была не только хорошо известна, но уже существовали вполне эффективные с практической точки зрения алгоритмы ее решения.

Более точно, автор [33], [118] ввел в рассмотрение интерпретацию Диофантовых уравнений в свободных нильпотентных группах ступени ≥ 9 и в свободных метабелевых группах достаточно большого ранга, позволяющую перенести алгоритмическую неразрешимость 10-й Проблемы Гильберта на алгоритмическую неразрешимость проблемы эндоморфной сводимости в рассматриваемых группах. Оценка на ранг следовала из результатов Матиясевича.

Впервые идея использования рассматриваемой схемы для построения протокола аутентификации на платформе группы с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости была высказана автором в докладе на семинаре в Graduate Center City University of New York в 2007 году. Впоследствии идея была описана в статье Д. Григорьева и В. Шпильрайна [73]. Авторы опирались на результаты автора из [32], [33].

В общих чертах протокол выглядит следующим образом.

Установка. Выбирается бесконечная эффективно заданная группа G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости. Алиса 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.

Алгоритм аутентификации.

1) В качестве сессионного ключа выбирается эндоморфизм (в работе [73] – автоморфизм) ψ, вычисляется элемент $v = \psi(f)$ и передается в систему $\mathbf{C}$, в которой осуществляется аутентификация Алисы.

2) Система $\mathbf{C}$ с равной вероятностью выбирает случайный бит и отсылает его Алисе.

3) Если Алиса получает 0, то она просто публикует ψ, а система $\mathbf{C}$ проверяет, что действительно v – образ f относительно ψ. Если Алиса получает 1, то она вычисляет композицию $\chi = \varphi\psi$, передает ее системе $\mathbf{C}$, которая проверяет справедливость равенства $v = \chi(g)$.

Схема выглядит как протокол аутентификации с нулевым разглашением, аналогичный известному протоколу Фиата-Шамира (см., например, [34] или [105]). Однако для ее криптостойкости необходимо выполнение ряда дополнительных условий. Во-первых, необходимо, чтобы существовал фигурирующий в протоколе элемент g, проблема вхождения в множество эндоморфных образов которого была алгоритмически неразрешимой. 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 $\mathrm{gp}(h)$, полагая $f = f(c)$ в соответствии с Диофантовым уравнением. Но далее аналогичные условия должны быть выполнены для пары элементов f, v. Результаты работы [33] уже не позволяют считать, что проблема вхождения в множество эндоморфных образов элемента f алгоритмически неразрешима. Но даже, если бы это было так, приведенных условий все равно оказалось бы недостаточно.

Для разрешения этой ситуации в подготовленной к печати книге автора и др. «Solvable Groups» используется понятие группы с неразрешимой двукратной проблемой эндоморфной сводимости. Доказывается, что в свободной метабелевой группе M_n достаточно большого ранга можно выбрать элемент g, элемент b, циклическую подгруппу $\mathrm{gp}(h)$, элемент u и конечно порожденную абелеву группу A таким образом, что для любой пары элементов (g, f), где $f \in b \cdot \mathrm{gp}(h)$, 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 приведенного алгоритма. Соответствующие построения проведены 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 [10]. 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 еще раз упомянуть понятие генерической сложности проблемы, возникшее, главным образом, при исследовании практических алгоритмов.

Список обозначений

$\mathbf{N}$ – натуральные числа, $\mathbf{Z}$ – кольцо целых чисел, $\mathbf{Q}$ – поле рациональных чисел, $\mathbf{Z}_n$ – кольцо вычетов по модулю n, $K[x_1, ..., x_n]$ – кольцо многочленов над кольцом (полем) K, $log_g f$ – дискретный логарифм элемента f относительно базы g - 10, $\mathrm{ord}(g)$ – порядок элемента g - 10, $\mathrm{ord}(G)$ – порядок группы G - 10, $\mathrm{gp}(g_1, ..., g_k)$ – (под)группа, порожденная элементами $g_1, ..., g_k$ - 10, $\mathbf{F}_p$ – простое конечное поле характеристики p - 10, $\mathbf{F}_p^*$ – мультипликативная группа простого конечного поля - 10, $\mathbf{F}_q^*$ – мультипликативная группа конечного поля - 10, $\mathbf{F}_q$ – конечное поле порядка $q, q = p^r, (p$ – простое число) - 10, $ideal(h(x))$ – идеал, порожденный многочленом $h(x)$ - 11, $\mathbf{F}_p[x]/ideal(h(x))$– фактор кольцо - 11, $\mathbf{F}$ - поле - 11, $\mathbf{F}^*$ – мультипликативная группа поля - 11, RSA - система Ривеста-Шамира-Адлемана - 14, $\mathrm{нф}(g)$ – нормальная форма элемента g - 16, $a^b = bab^{-1}$ – сопряжение элемента a элементом b - 17, $[a, b]$ – коммутатор элементов a и b - 17, B_n – группа кос Артина на n нитях - 18, 37, 38, F_n - свободная группа ранга n - 19, M_n – свободная метабелева группа ранга n - 19, G' – коммутант группы G -19, G'' – второй коммутант группы G - 19, $\mathcal{A}^2$ – многообразие всех метабелевых групп - 19, $E(M_n)$ – проблема эндоморфной сводимости в группе M_n - 19, $\mathcal{P}(G)$ – конечное представление (группы) - 22, $R = \mathrm{нз}(r_1, ..., r_m)$ - нормальное замыкание (множества) - 22, $l(g)$ – функция длины - 31, $\mathbf{S}_r$ – сфера радиуса r - 31, 65, $\mathbf{B}_r$ – шар радиуса r - 31, 65, $d(g, f)$ – расстояние между элементами g и f - 31, Σ – алфавит - 32, Σ^* – моноид - 32, $\rho_{\mathbf{S}_r}$ – относительная плотность (множества) по сферам - 33, $\rho_{\mathbf{B}_r}$ – относительная плотность (множества) по шарам - 33, $\rho(V)$ – асимптотическая плотность подмножества V - 33, $\tilde{\rho}(V)$ – строгая асимптотическая плотность подмножества V - 33, $\mathbf{B}_n^+$ - полугруппа положительных кос - 37, S_n – группа подстановок на n символах - 37, $\mathbf{A}$ - ассоциативная алгебра над конструктивным полем конечной размерности $\dim_{\mathbf{F}}\mathbf{A}$ - 42, $\mathrm{M}_n(\mathbf{A})$ матричная алгебра над $\mathbf{A}$ размера $n \times n$ размерности $\dim_{\mathbf{F}}(\ \mathrm{M}_n(\mathbf{A}))$ - 42, $\mathrm{End}(V)$ – полугруппа всех эндоморфизмов (линейных преобразо-

ваний) векторного пространства V - 44, v^a - образ вектора v при эндоморфизме (линейном преобразовании) a - 44, W^A – образ подмножества W-векторного пространства относительно множества эндоморфизмов (линейных преобразований) A - 44, $< A >$ – подмоноид, порожденный A - 44, $\mathrm{Sp}(W)$ - подпространство, порожденное W - 44, $||v||$ размер вектора v - 44, $||a||$ – размер матрицы a - 44, $\mathrm{GL}_n(\mathbf{A})$ – группа обратимых матриц размера $n \times n$ над $\mathbf{A}$ - 47, $E_{g,h}$ - линейное преобразование векторного пространства алгебры, соответствующее левому умножению на g и правому на h - 48, $\mathrm{Aut}(G)$ – группа автоморфизмов G - 49, $H(G)$ – голоморф группы G - 49, $\mathbb{A}_5$ – группа четных подстановок на 5 символах - 60, KG – групповое кольцо (алгебра) над K - 63, $C(\sigma)$ – централизатор элемента σ - 64, $\lambda \wedge \mu, \sigma^i \wedge \nu^j$ – автоморфизмы специального вида алгебры KG - 65, x^Φ – множество образов элемента x относительно автоморфизмов из множества Φ - 65, $\mathrm{Sp}_{\mathbf{F}}(x^\Phi)$ – линейное подпространство над полем $\mathbf{F}$, порожденное множеством x^Φ - 65, $\mathrm{Ann}(a)$ – левый аннулятор элемента a - 71, $\Lambda_n = \mathbf{Z}[\zeta_1, ..., \zeta_n]$ – кольцо Диофантовых многочленов от n переменных - 77, $\mathbf{Z}^{(2)}$ – множество произведений двух различных простых чисел - 78, A_n – (свободная) абелева группа ранга n - 87, $\mathcal{A}$ – многообразие всех абелевых групп - 88, $\gamma_i G$ – i-й член нижнего центрального ряда группы G - 92, $\mathcal{N}_i$ – многообразие всех нильпотентных групп ступени $\leq i$ - 94, $M_{n,i}$ – свободная метабелева нильпотентная ступени i группа ранга n - 94, T_n – свободный модуль (над групповым кольцом свободной абелевой группы A_n) - 95, $M(A_n, T_n)$ - матричная группа изоморфная прямому сплетению $A_n \wr A_n$ свободной абелевой группы A_n на себя - 95, $\bar{\mathbf{F}} = \mathbf{F}(t_1, ..., t_n)$ – поле частных кольца $\mathbf{Z}A_n$ - 96, X_n^* – (свободный) моноид от множества свободных порождающих X_n свободной метабелевой группы M_n - 96, $v(G)$ – вербальная подгруппа (группы G, соответствующая слову v) - 101, $width(v(G))$ – ширина вербальной подгруппы - 101.

Указатель терминов

Криптографические схемы (системы, протоколы) и проблемы

English Summary

This book is about «Group-based Cryptography» which is a modern direction in the subject. It is considered in a more general algebraic setting. Not only infinite abstract groups are used as platforms for different cryptographic schemes, but other algebraic structures, such as algebras, semi-groups and loops, are applied as well. Fundamentals of the theory are written, descriptions of some cryptographic systems and protocols are given.

The core of this book is an original method of a linear decomposition. A linear decomposition attack based on this method allows to get a hidden information without computing secret keys of a schema. A number of cryptographic schemes including systems and protocols by Ko, Lee et. al., Wang, Cao et. al., Kahrobaei, Spilrain et. al., Mahalonobis, Mikhalev et. al., are considered. We show that these schemes can be effectively compromised under assumption that their platforms are parts of finite dimensional algebras.

Also, a new direction «Diophantine Cryptography» is proposed. We show that Diophantine language can be considered as uniform in the classic cryptography. We can describe RSA, discrete logarithm and other tools in this language. A non-decidability of the Diophantine Problem can be used as a base for cryptographic schemes. An interpretation of Diophantine equations in solvable groups can transport these protocols to group-theoretic platforms. Some examples are given.

Список литературы

[1] Адян С. И.
Неразрешимость некоторых алгоритмических проблем в теории групп // Труды Моск. мат. общества. 1957. Т. 6. С. 231-298.

[2] Адян С. И., Дурнев В. Г.
Алгоритмические проблемы для групп и полугрупп // Успехи мат. наук. 2000. Т. 55. С. 3-94.

[3] Алламбергенов Х. С., Романьков В. А.
Произведения коммутаторов в группах// Докл. АН УзССР. 1984. Т. 4. С. 14-15.

[4] Белоусов В. Д.
Основы теории квазигрупп и луп. М.: Наука. 1967. 224 с.

[5] Вентура Э., Романьков В. А.
Проблема скрученной сопряженности для эндоморфизмов метабелевых групп // Алгебра и логика. 2009. Т. 48 №2. С. 157-173.

[6] Вершик А. М., Спорышев П. В.
Ограничение среднего числа шагов в симплекс методе и проблемы асимптотической интегральной геометрии // Докл. АН СССР. Сер. мат. Т. 271 №5. С. 1044-1048.

[7] Грибов А. В., Золотых П. А., Михалев А. В.
Построение алгебраической криптосистемы над квазигрупповым кольцом // Матем. вопросы криптографии. 2010. Т. 1 №4. С. 23-33.

[8] Ерофеев С. Ю.
Диофантовость дискретного логарифма // Вестник Омского университета. 2010. №4. С. 13-15.

[9] Ерофеев С. Ю.
Диофантовость дискретного логарифма // Прикл. дискр. мат. 2011. №4 (14). С. 31-32.

[10] Ерофеев С. Ю.
Схемы построения двушагово односторонних функций // Вестник Омского университета. 2011. №4. С. 15-18.

[11] Ерофеев С. Ю., Романьков В. А.
О построении возможно односторонних функций на основе алгоритмической неразрешимости проблемы эндоморфной сводимости в группах // Прикл. дискр. мат. 2012. №3 (17). С. 13-24.

[12] Каргаполов М. И., Мерзляков Ю. И.
Основы теории групп. М.: Лань, 2009. 288 с.

[13] Кожевников А. А., Николенко С. И.
О полных односторонних функциях // Проблемы передачи информации. 2009. Т. 45 №2. С. 101-118.

[14] Курош А. Г.
Теория групп. М.: ФИЗМАТГИЗ, 2008, 808 с.

[15] Левин Л. А.
Односторонние функции // Проблемы передачи информации. 2003. Т. 39 №1. С.103-117.

[16] 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.

[17] Маканин Г. С.
Уравнения в свободной группе // Изв. АН СССР. Сер. мат. 1982. Т. 46 №6. С. 1199-1273.

[18] Марков А. А.
Основы алгебраической теории кос // Труды мат. ин-та АН СССР. 1945. Т. 16. С. 3-54.

[19] Марков В. Т., Михалев А. В., Грибов А. В., Золотых П. А., Скаженик С. С.
Квазигруппы и кольца в кодировании и построении криптосхем // Прикл. дискр. мат. 2012. №4 (18). С. 32-52.

[20] Матиясевич Ю. В.
Диофантовость перечислимых множеств // Докл. АН СССР. Сер. мат. 1970. Т. 191 №2. С. 279-282.

[21] Матиясевич Ю. В.
Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. мат. 1971. Т. 35 №1. С. 3-30.

[22] Матиясевич Ю. В.
Десятая проблема Гильберта. М.: Наука (физ.-мат. лит-ра), 1993. 223 с.

[23] Мегрелишвили Р. П., Джинджихадзе М. В.
Однонаправленная матричная функция для обмена криптографическими ключами, метод генерации мультипликативных матричных групп // Proc. of Intern. Conf. SAIT 2011, May 23-28, Kyiv, Ukraine, P. 472.

[24] Мерзляков Ю. И.
Целочисленное представление голоморфов полициклических групп // Алгебра и логика. 1970. Т. 9 №5. С. 539-558.

[25] Михайлова К. А.
Проблема вхождения для прямых произведений групп // Докл. АН СССР. Сер. мат. 1958. Т. 119. С. 1103-1105.

[26] Нейман Х.
Многообразия групп. М.: Мир, 1974. 264 с.

[27] Новиков П. С.
Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Труды мат. ин-та АН СССР. 1955. Т. 44. С. 3-143.

[28] Новиков П. С.
Неразрешимость проблемы сопряженности в теории групп. // Изв. АН СССР. Сер. мат. 1954. Т. 18 №6. С. 485-524.

[29] Носков Г. А.
О сопряженности в метабелевых группах // Матем. заметки. 1982. Т. 31 №4. С. 495-507.

[30] 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.

[31] Романовский Н. С.
О некоторых алгоритмических проблемах для разрешимых групп // Алгебра и логика. Т. 13 №1. С. 26-34.

[32] 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.

[33] Романьков В. А.
Об уравнениях в свободных метабелевых группах // Сиб. матем. ж. 1979. Т. 40 №3. С. 671-673.

[34] Романьков В. А.
Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.

[35] Романьков В. А.
Диофантова криптография на бесконечных группах // Прикл. дискр. мат. 2012. №2 (16). С. 15-42.

[36] Романьков В. А.
Криптографический анализ некоторых схем шифрования использующих автоморфизмы // Прикл. дискр. мат. 2013. (сдано в печать).

[37] Росошек С. К.
Криптосистемы групповых колец // Вестник Томского государственного университета. 2003. №6. С. 57-62.

[38] Росошек С. К.
Криптосистемы в группах автоморфизмов групповых колец абелевых групп // Фунд. и прикл. мат. 2007. Т. 13 №3. С. 157-164.

[39] Рыбалов А. Н.
О генерической неразрешимости десятой проблемы Гильберта // Вестник Омского университета. 2011. №4. С. 19-22.

[40] Сидельников В. М., Черепнев М. А., Ященко В. Ю.
Системы открытого распределения ключей на базе некоммутативных полугрупп // Докл. РАН. Сер. мат. 1994. Т. 48 №2. С. 384-386.

[41] Тимошенко Е. И.
Алгоритмические проблемы для метабелевых групп // Алгебра и логика. 1973. Т. 12 №2. С. 232-240.

[42] Тимошенко Е. И.
Эндоморфизмы и универсальные теории разрешимых групп. Новосибирск: Изд-во НГТУ, 2011. 327 с.

[43] Хачиян Л. А.
Полиномиальный алгоритм в линейном программирова-

нии //Докл. АН СССР. Сер. мат. 1979. Т. 244 №5. С. 1093-1096.

[44] Холл М.
Теория групп. М.: Гос. изд-во ин. лит., 1962. 467 с.

[45] Alvarez R., Martinez F.-M., Vicent J. F., Zamora A.
A Matricial Public Key Cryptosystem with Digital Signature // WSEAS Trans. on Math. 2008. V. 4 №7. P. 195-204.

[46] Alvarez R., Tortosa L., Vicent J., Zamora A.
Analysis and design of a secure key exchange scheme // Information Sciences. 2009. V. 179. P. 2014-2021.

[47] Alvarez R., Tortosa L., Vicent J., Zamora A.
A non-abelian group based on block upper triangular matrices with cryptographic applications // AAECC-18 '09: Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Berlin-Heidelberg. 2009. Springer-Verlag. P. 117-126.

[48] Anshel I., Anshel M., Goldfeld D.
An algebraic method for public-key cryptography // Math. Res. Lett. 1999. V. 6. P. 287-291.

[49] Anshel I., Anshel M., Goldfeld D., Lemieux S.
Key agreement, the algebraic eraser, and lightweight cryptography // Algebraic Methods in Cryptography. V. 418 of Contemporary Mathematics, AMS, 2006. P. 1-34.

[50] Baumslag G., Cannonito F., Robinson D. J. S.
The algorithmic theory of finitely generated metabelian groups // Trans. Amer. Math. Soc. 1994. V. 344. P. 629-648.

[51] Baumslag G., Fine B., Xu X.
Cryptosystems using linear groups // Applicable Algebra in Engineering, Communication and Computing. 2006. V. 17 №3-4. P. 205-217.

[52] Baumslag G., Mikhailov R., Orr K. E.
A new look at finitely generated metabelian groups // Preprint: arXiv math. 1203.5431[ms.GT]. 2012. 17 p.

[53] Birget J.-C., Magliveras S., Sramka M.
On public-key cryptosystems based on combinatorial group theory // Tatra Mountains Math. Publ. 2006. V. 33. P. 137-148.

[54] Blackburn S. R., Cid C., Mullan C.
Cryptanalysis of three matrix-based key establishment protocols // J. Mathematical Cryptology. 2011. Vol. 5. P. 159-168.

[55] Borovik A., Myasnikov A., Shpilrain V.
Measuring sets in infinite groups // Contemp. Math. V. 298, Providence R.I.: Amer. Math. Soc., 2002. P. 21-42.

[56] Celler F., Leedham-Green C. R., Murray S. H., Niemeyer A. C., O'Brien E. A.
Generating random elements of a finite group // Comm. Algebra. 1995. V. 23 №3. P. 4931-4948.

[57] Computational complexity theory // S. Rudich, A. Wigderson – editors. Amer. Math. Soc. Institute for Advanced Study, IAS/Park City Math. Series. V. 10. Providence R.I.: Amer. Math. Soc., 2004. 389 p.

[58] Cook S. A., 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.

[59] Coppersmith D., Odlyzko A., Schroeppel R.
Discrete logarithms in GF(p) // Algorithmica. 1986. V. 1. P. 1-15.

[60] Dehornoy P.
Braids and self-distributivity // Progress in Math. V. 192. Basel-Berlin-New York: Birkhäuser Verlag. 2000. 623 p.

[61] Dehornoy P.
Braid-based cryptography // Group theory, statistics and cryptography. Contemp. Math. V. 360, Providence R.I.: Amer. Math. Soc., 2004. P. 5-33.

[62] Detinko A., Eick B., Flannery D.
Computing with matrix groups // London Math. Soc. Lect. Notes Ser. 2011. V. 387. P. 256-270.

[63] Diffie W., Hellman M. E.
New directions in cryptography // IEEE Transaction Information Theory. 1976. V. 22. P. 644–654.

[64] ElGamal T.
A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. V. IT-31 №4. P. 469-472.

[65] Fine B., Habeeb M., Kahrobaei D., Rosenberger G.
Survey and open problems in non-commutative cryptography // JP Journal of Algebra, Number Theory and Applications. 2011. V. 21. P. 1-40.

[66] Garber D.
Braid group cryptography. Lect. notes of Tutorials given at Braids PRIMA Summer School at Singapore, June 2007.
Preprint: arXiv math.:0711.3941v2[cs.CR] 27 Sep. 2008. P. 1-39.

[67] Garside F. A.
The braid group and other groups // Quart. J. Math. 1969. V. 20 №78. P. 235-254.

[68] Gebhardt V.
A new approach to the conjugacy problem in Garside groups // J. Algebra. 2005. V. 292. P. 282-302.

[69] 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.

[70] Gilman R., Myasnikov A. G., Miasnikov A. D., Ushakov A.
Report on generic case complexity // Вестник Омского университета. 2007. Специальный выпуск: Комбинаторные методы алгебры и сложность вычислений. С. 103-110.

[71] Goldreich O.
Foundations of cryptography. 1-2. Cambridge: Cambridge Univ. Press. 1, 2001. 451 p.; 2, 2004. 798 p.

[72] Goldwasser S., Bellare M.
Lecture Notes on Cryptography. Summer course on cryptography. MIT. 1996-2001.

[73] Grigoriev D., Shpilrain V.
Zero-knowledge autentification schemes from actions on graphs, groups and rings // Ann. Pure Appl. Logic. 2010. V. 162. P. 194-200.

[74] Grigoriev D., Shpilrain V.
Autentication from matrix conjugation // Groups. Complexity. Cryptology. 2009. V. 1. P. 199-206.

[75] Groves J. R. J., Miller III C. F.
Recognizing free metabelian groups // Illinois J. Math. 1986. V. 30 №2. P. 246-254.

[76] Gurevich Y.
Average case comleteness // J. Comput. Syst. Science. 1991. V. 42. P. 346-398.

[77] Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V.
Public key exchange using semidirect product of (semi)groups // Preprint: arXiv math.: 1304.6572v1[cs.CR] 24 Apr. 2013. P. 1-12.

[78] Hall P.
Nilpotent groups // Canad. Math. Cong. Summer Sem. Vankuver: University of Alberta, 1957. P. 12-30.

[79] Hellman M. E.
An Overview of Public Key Cryptography // IEEE Communication Magazine. 2002. P. 42–49.

[80] Holt D. F., Eick B., O'Brien E. A.
Handbook of computational group theory. London: Chapman & Hall/CRC. 2005. 414 p.

[81] Jones J.
Universal diophantine equation // J. Symbolic Logic. 1982. V. 47 №3. P. 549-571.

[82] Kahrobaei D., Khan B.
A Non-Commutative Generalization of ElGamal Key Exchange using Polycyclic Groups // Global Telecommunication Conference. 2006, GLOBECOM'06, IEEE. P. 1-5.

[83] Kahrobaei D., Koupparis C., Schpilrain V.
Public key exchange using matrices over group rings. Groups. Complexity. Cryptology. 2013. V. 5. P. 13-52.

[84] Kapovich I., Myasnikov A., Shupp P., Shpilrain V.
Average-case complexity and decision problems in group theory // Advances in Math. 2005. V. 190. P. 343-359.

[85] Kapovich I., Myasnikov A., Shupp P., Shpilrain V.
Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. P. 665-694.

[86] Kellerer H., Pferschy U., Pisinger D.
Knapsack Problems. Berlin-New York: Springer-Verlag, 2004. 546 p.

[87] Klee V., Minty G.
How good is the simplex algorithm? // Inequalities. Proc. Third. Symp., Univ. California. California: Academic Press, 1972. P. 159-175.

[88] Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C.
New public-key cryptosystem using braid groups // Advances in Cryptology - CRYPTO 2000. V. 1880 of Lecture Notes Comp. Sc., Berlin, 2000, Springer-Verlag. P. 166-183.

[89] Koblitz N.
Elliptic curve cryptosystems // Math. Comput. 1987. V. 48. P. 203-209.

[90] Koblitz N.
A Course in Number Theory and Cryptology. Springer-Verlag, New York - Heidelberg - Berlin. 1994. 235p.

[91] Krammer D.
Braid groups are linear // Ann. Math. 2002. V. 151. P. 131-156.

[92] Kurt Y.
A new key exchange primitive based on the triple decomposition problem // Preprint: http://eprint.iacr.org/2006/378.

[93] Lennox J. C., Robinson D. J. S.
The Theory of Infinite Soluble Groups. Oxford Math. Monographs, Oxford Science Publications, Clarendon Press. Oxford, 2004. 342p.

[94] Levin L.
Average case complete problems // SIAM J. Comput. 1986. V. 15. P. 285-286.

[95] Levin L. A.
One-way Functions and Pseudorandom Generators // Combinatorica. 1987. V. 7 №4. P. 357-363.

[96] Lohrey M.
Word problems on compressed words // Automata, Languages and Programming. Lect. Notes in Comput. Sci. V. 3142. Berlin-Heidelberg: Springer-Verlag. 2004. P. 906-918.

[97] Lohrey M., Schleimer S.
Efficient computation in groups via compression // Second International Symp. on Computer Science in Russia, CSR 2007. Ekaterinburg, Russia. 2007. Lect. Notes in Comput. Sci. V. 4649. Berlin-Heidelberg: Springer-Verlag. 2007. P. 249-258.

[98] Magyarik M. R., Wagner N. P.
A public key cryptosystem based on the word problem // Advances in Cryptology. CRYPTO 1084. Lect. Notes in Computer Science. V. 196. Berlin: Springer Verlag, 1985. P. 19-36.

[99] Mahalanobis A.
The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. 2008. Vol. 165. P. 161-187.

[100] Mahlburg K.
An overview of braid group cryptography. 2004. www.math.wisc.edu/ boston/mahlburg.pdf

[101] 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.

[102] Matijasevich Y. V., Robinson J.
Reduction of an arbitrary diophantine equation to one in 13 unknowns // Acta Arithmetica. 1975. V. 27. P. 521-553.

[103] Megrelishvili R., Chelidze M., Chelidze K.
On the construction of secret and public-key cryptosystems // Applied Mathematics, Informatics and Mechanics. 2006. V. 11 №2. Tbilisi, Georgia: Tbilisi University Press. P. 29-36.

[104] Megrelishvili R., Chelidze M., Besiashvili G.
One-way matrix function – analogy of Diffie-Hellman protocol. In: Proceedings of Seventh International Conference, IES-2010, 28Sept.–3.Oct., Vinnytsia, Ukraine, 2010. P. 341-344.

[105] Menezes A. J., van Oorschot P. C., Vanstone S. A.
Handbook of Applied Cryptography. CRC Press, 1996. 816 p.

[106] Menezes A., Vanstone S.
A note on cyclic groups, finite fields, and the discrete logarithm problem // Applicable algebra in Engineering, Communication and Computing. 1992. V. 3. P. 67-74.

[107] Menezes A. J., Wu Y.-H.
The discrete logarithm problem in GL(n, q) // Ars Combinatoria. 1997. V. 47. P. 23–32.

[108] 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.

[109] Miller V.
Uses of elliptic curves in cryptography // Advances in Cryptology – Proceedings of Crypto'85. Lecture Notes in Computer Science. V. 218. Berlin-Heidelberg. 1986. Springer-Verlag. P. 417-426.

[110] Myasnikov A., Roman'kov V., Ushakov A., Vershik A.
The word and geodesic problems in free solvable groups // Trans. Amer. Math. Soc. 2010. V. 362. P. 4655-4682.

[111] Myasnikov A., Shpilrain V., Ushakov A.
Group-based cryptography. Advances courses in Math. CRM,

Barselona. Basel-Berlin-New York: Birkhäuser Verlag, 2008. 183 p.

[112] Myasnikov A., Shpilrain V., Ushakov A.
Non-commutative cryptography and complexity of group-theoretic problems // Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2011. 385 p.

[113] Odoni R., Varadharajan V., Sanders P.
Public key distribution on matrix rings // Electronic Letters. 1984. V. 20. P. 386-387.

[114] Papadimitriou C.
Computation complexity. Boston: Addison-Wesley, 1994. 523 p.

[115] Petrides G.
Cryptoanalisis of the public key cryptosystem based on the word problem on the Grigorchuk groups // 9th IMA Internat. Conf. on Cyptography and Coding. Lect. Notes in Computer Science. V. 2898, 234-244. Berlin: Springer Verlag, 2003. P. 234-244.

[116] Quasigroups and Loops: theory and applications // Chein O., Pflugfelder H. O., Smith J. D. H. – editors Sigma series in Pure Math. V. 8. Berlin: Heldermann Verlag. 1990. 568 p.

[117] Romanczuk U., Ustimenko V.
On the $PSL_2(q)$, Ramanujan graphs and key exchange protocols // http://aca2010.info/index.php/aca2010/aca2010/paper/viewFile/80/3.

[118] Roman'kov V. A.
A linear decomposition attack
J. Mathematical Cryptology. (сдано в печать)

[119] Roman'kov V. A.
Equations over groups // Groups. Complexity. Cryptology. 2012. V. 4 №2. P. 191-239.

[120] Sakalauskas L., Tvarijonas P., Raulynaitis A.
Key agreement protocol (kap) using conjugacy and discrete logarithm problems in group representation level // Informatica. 2007. V. 18. P. 115-124.

[121] Scheimer S.
Polynomial-time word problems // Comment. Math. Helv. 2008. V. 83 №4. P. 741-765.

[122] Segal D.
Words: notes on verbal width in groups // London Math. Soc. Lect. Notes. V. 361. Cambridge: Cambridge Univ. Press, 2009. 215 p.

[123] Shpilrain V.
www.grouptheory.info/PersonalPages/Shpilrain, Vladimir/Cryptology ePrint Archive

[124] Shpilrain V.
Cryptanalysis of Stickel's key exchange scheme // Computer Science in Russia 2008, Lect. Notes in Computer Science. V. 4296. Springer-Verlag. 2008. P. 283-288.

[125] Shpilrain V., Ushakov A.
Thompson's group and public key cryptography // Applied Cryptography and Network Security – ACNS 2005. P. 3531 of Lecture Notes Comp. Sc., Springer-Verlag. 2005, 151-164.

[126] Shpilrain V., Ushakov A.
A new key exchange protocol based on the decomposition problem // Algebraic Methods in Cryptography. 2006. Contemp. Math. V. 418. Providence R.I.: Amer. Math. Soc. P. 161-167.

[127] Shpilrain V., Ushakov A.
The conjugacy search problem in public key cryptography: unnecessary and unsufficient // Appl. Algebra Engrg. Comm. Comput. 2006. V. 17. P. 285-289.

[128] Shpilrain V., Ushakov A.
An autentication scheme based on the twisted conjugacy problem // ACNS 2008. V. 5037 of Lecture Notes Comp. Science. Springer-Verlag. 2008. P. 366-372.

[129] Shpilrain V., Ushakov A.
The conjugacy search problems in public key cryptography: unecessary and insufficient // Applicable Algebra in Engineering Communication and Computing. 2006. V. 17. P. 285-289.

[130] Shpilrain V., Zapata G.
Using the subgroup membership problem in public key cryptography // Contemp. Math. V. 418. Providence R.I.: Amer. Math. Soc., 2006. P. 169-179.

[131] Shpilrain V., Zapata G.
Combinatorial group theory and public key cryptography // Applicable Algebra in Engineering Communication and Computing. 2006. V. 17. P. 291-302.

[132] Shpilrain V., Zapata G.
Using decision problems in public key cryptography // Groups. Complexity. Cryptology. 2009. V. 1. P. 33-40.

[133] Sims C. C.
Computation with finitely presented groups. Cambridge: Cambridge Univ. Press, 1994. 604 p.

[134] Sipser M.
Introduction to the theory of computation. PWS Publishing, 1997. 416 p.

[135] Smale S.
On the average number of steps of the simplex method of linear programming // Math. Programming. 1983. V. 27. P. 241-262.

[136] Smith J. D. H.
An Introduction to Quasigroups and their representations. Chapman & Hall. CRC. 2007.

[137] Stickel E.
A New Method for Exchanging Secret Keys // Proc. of the Third Intern. Conf. on Information Technology and Applications (ICITA 05). Contemp. Math. V. 2. 2005. IEEE Computer Society. P. 426-430.

[138] Stroud P.
Ph. D. Thesis. Cambridge, 1966. 121 p.

[139] Ushakov A.
Authenticated commutator key-agreement protocol (submitted).

[140] Vasco M. I. G., Pérez del Poso A. L., Duarte P. T.
Cryptanalysis of a key exchange scheme based on block matrices // Preprint: IACR Cryptology e-print Archive 01/2009, 2009.553. P. 1-16. :

[141] Vassileva S.
Polynomial time conjugacy in wreath products and free solvable groups // Groups. Complexity. Cryptology. 2011. V. 3. P. 105-120.

[142] Wang L., Wang L., Cao Z., Okamoto E., Shao J.
New constructions of public-key encryption schemes from conjugacy search problems // Information security and cryptology. V. 6584 of Lecture Notes Comp. Sc. Springer. 2010. P. 1-17.

Научное издание

Алгебраическая криптография
Монография

Романьков Виталий Анатольевич

Редактор Д.С. Нерозник
Технический редактор Н.С. Серопян
Дизайн обложки З.Н. Образова

Подписано в печать 30.07.2013. Формат 60×84 1/16.
Печ. л. 8,75. Усл.-печ. л. 8,1. Уч.-изд. л. 6.
Тираж 75 экз. Заказ 178.

Издательство Омского государственного унивеситета
644077, Омск-77, пр. Мира, 55а
Отпечатано на полиграфической базе ОмГУ
644077, Омск-77, пр. Мира, 55а