

АЛГЕБРАИЧЕСКАЯ КРИПТОГРАФИЯ: НОВЫЕ КОНСТРУКЦИИ И ИХ НАДЁЖНОСТЬ ОТНОСИТЕЛЬНО ДОКАЗУЕМОГО ВЗЛОМА

© Д. Ю. ГРИГОРЬЕВ, А. КОЖЕВНИКОВ, С. И. НИКОЛЕНКО

Известно не так уж много схем криптографических примитивов, основанных на идеях некоммутативной алгебры. Каждая новая схема представляет существенный интерес, поскольку для неабелевых конструкций многие стандартные атаки не работают. С другой стороны, в криптографии не известны доказательства надёжности, которые бы позволяли транслировать надёжность того или иного примитива в утверждения о сложностных классах. Поэтому представляют интерес исследования более слабых понятий надёжности.

В этой работе мы представляем новые конструкции криптографических примитивов на основе теории инвариантов групп и предлагаем возможные варианты их усложнения для практического применения. Кроме того, введено новое понятие *взлома с доказательством*, представляющее собой ослабленную версию обычного криптографического взлома, в котором взломщик должен представить доказательство того, что он действительно правильно расшифровал сообщение. Доказано, что криптосистемы, основанные на инвариантах матричных групп, а также вариант протокола согласования ключа Аншель–Аншеля–Голдфельда для модулярных групп, являются устойчивыми относительно взлома с доказательством, если $NP \not\subseteq RP$.

§1. Алгебраическая криптография

Криптография с открытым ключом, начиная с самого своего появления [19, 52], активно пользуется алгебраическими конструкциями. Система RSA, например, основана на методах теории чисел; уже сама её конструкция содержит вычисление функции Эйлера от ключа, $\varphi(n)$, а её надёжность основана на сложности задачи разложения чисел на множители, точнее говоря, на сложности так называемой „RSA problem“: поиска корней заданной степени по модулю числа $n = pq$, где p и q — простые (стоит

Исследования были выполнены во время пребывания в Max-Planck-Institut für Mathematik, Бонн, Германия. Работа второго и третьего авторов частично поддержана грантами INTAS YSF 05-109-5565 и РФФИ 05-01-00932, 06-01-00502.

отметить, что эта задача может оказаться не эквивалентна разложению чисел на множители; эта проблема пока остаётся открытой [17, 53, 18]).

Однако обычно под *алгебраической криптографией* с открытым ключом принято понимать несколько более узкое понятие. Алгебраическая криптография рассматривает конструкции, в которых отображения кодирования и декодирования являются гомоморфизмами групп. В [2] даётся следующее определение *гомоморфной криптосистемы* (ср. с определением 2, где вводится понятие криптосистемы вообще).

Определение 1. Пусть H — конечная группа, $H \neq \{e\}$, G — конечно-порождённая группа, $f : G \rightarrow H$ — эпиморфизм. Пусть даны множество R представителей правых классов смежности G по нормальной подгруппе $\text{Ker}(f)$ и множество A слов в некотором алфавите вместе с таким отображением $P : A \rightarrow G$, что $\text{Im}(P) = \text{Ker}(f)$. Набор (R, A, P) называется *гомоморфной криптосистемой* над H относительно f , если:

- имеются вероятностные алгоритмы для случайного порождения элементов множеств A , G , H , для вычисления обратного элемента и произведения в группах G и H , вероятностная сложность которых полиномиальна от размера задания групп G , H и множества A ;
- $|R| = |H|$, и для всякого $g \in R$ его образ $f(g)$ можно вычислить за полиномиальное от размера задания участвующих групп время, также как и для всякого элемента $h \in H$ можно вычислить его единственный прообраз $g \in R$: $f(g) = h$;
- P является секретно-обратимым отображением (trapdoor).

Формально даже в этом, более узком, смысле алгебраическая криптография с открытым ключом всё равно появилась практически одновременно с криптографией с открытым ключом; криптосистема, основанная на квадратичных вычетах, была первой гомоморфной криптосистемой и одной из первых криптосистем вообще [26, 25].

Однако собственно алгебраическая криптография в её современном понимании ведёт начало от работ, связанных с криптографическими примитивами, построенными на эллиптических кривых [44, 37]. Основные конструкции этих примитивов на самом деле мало отличаются от конструкций, основанных на дискретном логарифме, таких как протокол согласования ключа Диффи–Хеллмана. Основное отличие в том, что вычисления ведутся в абелевой группе точек эллиптической кривой вида $y^2 = x^3 + ax + b$ или $y^2 + xy = x^3 + ax^2 + b$; это позволяет существенно

уменьшить размеры ключей и сделать криптосистемы более эффективными [13, 57, 32]. В последнее время в США был принят ряд криптографических стандартов, основанных на эллиптических кривых.

Отметим одну важную особенность. И классические конструкции, и криптография на эллиптических кривых имеют дело с *абелевыми* группами. Эта дополнительная структура позволяет сделать алгоритмы кодирования и декодирования ещё более эффективными, а также существенно упрощает анализ возникающих задач. Однако за последние десять лет, начиная с основополагающих работ Питера Шора [54, 12], абелевы конструкции оказались подвергнуты новому типу атак, со стороны *квантовых вычислений*. Задачи разложения чисел на множители и дискретного логарифма, на которых, с некоторыми вариациями, были основаны все наиболее популярные криптосистемы, включая криптосистемы, основанные на эллиптических кривых, получили простые и эффективные алгоритмы решения на квантовом компьютере (см. также [41, 47] и гл. 20 [10]). Это происходит вследствие того, что на квантовом компьютере при помощи квантовых преобразований Фурье можно эффективно решить задачу вычисления порядка элемента в абелевой группе, частным случаем которой, собственно, и является дискретный логарифм. Решение этой задачи настолько помогает для взлома криптографических примитивов, основанных на абелевых группах конструкций, что в ситуации, когда квантовые компьютеры уже присутствуют на горизонте (хотя их практические перспективы пока не до конца ясны), ограничиваться коммутативными конструкциями уже недостаточно: хотелось бы получить и *неабелевы* конструкции, от которых можно ожидать большей устойчивости [8].

Именно поэтому эллиптические конструкции и классические криптографические конструкции Диффи–Хеллмана и RSA были обобщены, и задача построения гомоморфных криптосистем была поставлена в [22, 59]. Первые шаги в использовании алгебраических конструкций, в частности теории групп, для построения криптографических примитивов были сделаны в работах [11, 46, 48, 49]. Важный шаг на пути разработки неабелевых криптографических примитивов составили работы И. Аншель, М. Аншеля и Д. Голдфельда, одну из конструкций которых мы будем подробно рассматривать в §9 [6, 7, 5].

Дальнейшая разработка этих идей продолжалась в работах первого автора и И. Н. Пономаренко. Был разработан аппарат определений, таких как определение 1. Были построены конструкции неабелевых гомоморфных криптосистем с открытым ключом [2], конструкции гомоморфных криптосистем над кольцами [29], была разработана общая схема конструкции более сложных гомоморфных криптосистем из блоков [31] (эта

схема будет играть важную роль в настоящей работе), исследована связь между гомоморфными криптосистемами и кодированием булевских схем [30].

В работе [1] первый автор предложил использовать для криптографических целей теорию инвариантов групп. В §5 мы обсудим эти конструкции более подробно, а сейчас перейдём к обсуждению взлома с доказательством — второй основополагающей идеи настоящей работы. Эта статья представляет собой существенно расширенную версию работы [28].

§2. Ослабленные результаты современной криптографии

Современная криптография практически не позволяет предоставить строгие доказательства надёжности тех или иных примитивов. Начиная с самой первой конструкции протокола согласования ключа Диффи–Хеллмана [19] и криптосистемы с открытым ключом RSA [52], криптографы построили огромное количество конструкций, но не смогли предоставить *ни одного* доказательства их надёжности. Конечно, найти безусловное доказательство действительно вряд ли получится, потому что оно включало бы в себя доказательство $P \neq NP$. Но и условные доказательства вида „Если $P \neq NP$, то такой-то протокол надёжен“ тоже не так-то просто получить. Дело здесь в том, что классическое понятие криптографической надёжности естественным образом связано со сложностью в среднем, а не классической сложностью в худшем случае. Приведём для примера классическое понятие *семантической надёжности* криптосистемы; она определяется следующим образом (придётся начать с определения собственно криптосистемы) [25].

Определение 2. *Криптосистема с открытым ключом S состоит из трёх вероятностных алгоритмов (G, E, D) для порождения ключа, кодирования и декодирования соответственно, каждый из которых работает в худшем случае полиномиально долго.*

Алгоритм порождения ключа G на входе 1^n (где n — параметр надёжности) порождает пару $G(1^n) = (e, d)$ из публичного и секретного ключа. Алгоритм кодирования E получает на вход публичный ключ e и сообщение m , после чего выдаёт закодированное сообщение

$$E(e, m) = c.$$

Алгоритм декодирования D получает на вход секретный ключ d и код c . Выходом D является сообщение

$$D(d, c) = m',$$

которое может не равняться исходному сообщению только тогда, когда $E(e, m) = E(e, m')$. Такие ситуации называются *коллизиями*; в дальнейшем мы предполагаем, что коллизии происходят с пренебрежимо малой вероятностью.

Определение 3. Криптосистема с открытым ключом (G, E, D) называется *семантически надёжной*, если для всех полиномиальных алгоритмов M и A , функций h и многочленов Q существует такой полиномиальный алгоритм B , что для достаточно больших k

$$\begin{aligned} \Pr_r \left[A(1^k, c, e) = h(m) \mid (e, d) \xleftarrow{r} G(1^k), m \xleftarrow{r} M(1^k), c \xleftarrow{r} E(e, m) \right] \\ \leq \Pr_r \left[B(1^k) = h(m) \mid m \xrightarrow{r} M(1^k) \right] + \frac{1}{Q(k)}. \end{aligned}$$

Неформально говоря, любой потенциальный взломщик, который, зная распределение исходных сообщений M , получает на вход закодированное сообщение и публичный ключ, не сможет его декодировать значительно чаще, чем алгоритм, который не знает ничего, кроме M (M нужно потому, что, например, если известно, что всё время кодируется одно и то же сообщение, противник действительно сможет его раскодировать, но ему для этого не обязательно будет смотреть на код и публичный ключ). Основная проблема здесь в том, что вероятности в этом определении берутся в том числе и по распределению на входах криптосистемы, на сообщениях; это, конечно, по существу, потому что на практике обычно достаточно взламывать криптосистему не на всех сообщениях, а на существенной их доле.

Недавние результаты позволили связать криптографическую сложность (в смысле определения 3) с предположениями о сложности определённых задач в худшем случае [4, 20, 50, 51]. Однако пока что эти предположения выглядят достаточно искусственными и, как и раньше, не транслируются в предположения о (не)равенстве тех или иных сложностных классов. Вообще говоря, представляется, что современной криптографии ещё очень далеко до *доказуемо* надёжных конструкций. Есть даже результаты, говорящие о том, что это может оказаться невозможным или приведёт к маловероятным последствиям для сложностных классов [16].

Поэтому вполне естественно, что исследователи, столкнувшись со слишком трудной проблемой, начали работу над альтернативными определениями, критериями и контекстами, пытаясь доказать надёжность хоть чего-нибудь, хоть в каких-нибудь определениях.

Первый естественный подход — рассмотреть не „настоящие“ криптографические примитивы, а их более слабые аналоги, такие, например, как *односторонние функции*, one-way functions (отметим, что односторонняя

функция ещё не означает криптосистемы с открытым ключом, для неё нужна функция с секретом, *trapdoor function*). И действительно, результаты об односторонних функциях оказывается проще доказать. Например, полные односторонние функции (*полной* мы называем такую функцию f , что если односторонние функции вообще существуют, то f тоже односторонняя) известны уже достаточно давно [40, 24], а полные криптосистемы с открытым ключом появились только в последние годы в работах Харника и первого автора с соавторами [27, 33]. Более того, недавно Леонид Левин разработал более или менее естественные конструкции комбинаторных полных односторонних функций [3]; эта работа была продолжена в исследованиях второго и третьего авторов [38].

Другой подход, тоже приводящий к более слабым результатам, заключается в том, чтобы изменить само понятие надёжности. Если рассмотреть более слабые определения надёжности, оказывается возможным построить даже доказуемо надёжные примитивы. Как пример такого подхода можно привести теорию *слабо односторонних* (*feebly one-way*) функций, развитую А. Хилтгеном [34, 35]. В работах Хилтгена функции рассматривались с позиций схемной сложности в базисе из всех бинарных булевских функций, что является наиболее сложным для доказательства нижних оценок случаем [15, 58]. Однако ему удалось построить линейную обратимую функцию, вычисление которой почти в два раза проще, чем её обращение; эти оценки, сколь бы слабыми они ни были, были первыми абсолютными, ни от чего не зависими доказательствами надёжности односторонних функций. В последнее время в работах третьего автора и Э. А. Гирша была построена аналогичная конструкция слабой функции с секретом [36]; возможно, в будущем удастся построить и доказуемо надёжную криптосистему („надёжную“, разумеется, в вышеописанном весьма ограниченном смысле).

С другой стороны, были получены частичные результаты в направлении, где надёжность определена для *противника в худшем случае*. Этот противник должен взламывать криптосистему *всегда*, для всех сообщений. Поэтому неудивительно, что в таком контексте можно получить результаты, связывающие надёжность со сложностными предположениями [21, 39]. Желающим найти детальный обзор этого и других результатов мы рекомендуем [45, 30, 31].

В следующем параграфе мы введём и начнём исследовать другой подход, ослабляющий понятие надёжности в другом смысле. Оказывается, что наше понятие *доказуемого взлома*, хотя и довольно искусственное,

позволяет связать доказуемый взлом криптосистем, основанных на теории инвариантов, и протоколов согласования ключа Аншель–Аншеля–Голдфельда с предположениями о классах сложности в худшем случае.

§3. Доказуемый взлом

Рассмотрим систему с тремя участниками: Алисой, Бобом и Чарли. Пусть, как это обычно предполагается в криптографии, Алиса (А) и Боб (В) пытаются общаться друг с другом по некоторому криптографическому протоколу (в протоколе согласования ключа Алиса и Боб — его равноправные участники, в криптосистеме Алиса формирует пару из публичного и секретного ключа и выдаёт публичный ключ, а Боб кодирует сообщение и пересылает его Алисе по открытому каналу), а Чарли (С) пытается расшифровать их беседу, перехватывая сообщения, которые Боб посылает Алисе. Однако на этот раз задача Чарли выглядит по-другому: ему нужно не просто расшифровать сообщение Боба, но и каким-нибудь образом доказать, что сообщение у Боба было именно такое. Например, Чарли может сам не особенно доверять своей расшифровке, или у него есть начальник, которому нужен не просто ответ, а ответ с доказательством. Именно это мы понимаем под задачей *доказуемого взлома*.

В контексте доказуемого взлома Чарли должен получить не только сообщение m из кода c , но ещё и какое-нибудь доказательство того, что m можно закодировать в виде c . Что может служить таким доказательством? Мы примем за определение следующую естественную мысль: Чарли должен предъявить не только сообщение m , но и такой набор случайных битов r , для которого алгоритм E , получая на вход r и m , выдаёт тот же код c .

Замечание 1. В последующем тексте мы (эквивалентно) переопределим алгоритм кодирования E как детерминированный полиномиальный в худшем случае алгоритм с доступом к случайной строке r . Он получает в качестве входа публичный ключ e , исходное сообщение m и случайную строку r , а на выход подаёт закодированное сообщение $E(r, e, m) = c$.

Конечно, такой набор не обязан быть единственным: может быть несколько наборов случайных битов $\{r_1, \dots, r_k\}$, из которых получается один и тот же шифр:

$$E(m, pk, r_1) = \dots = E(m, pk, r_k).$$

В этом случае, разумеется, противнику достаточно предъявить *какой-нибудь* набор случайных битов, приводящий к искомому шифру; при $k > 1$ у Чарли всё равно нет никаких шансов отличить один от другого.

Первое неформальное обсуждение доказуемого взлома началось в связи с криптосистемой Рабина–Голдвассер–Микали, основанной на квадратичных вычетах [25]. Было показано, что доказуемый взлом этой криптосистемы означал бы, что задача разложения чисел на множители лежит в RP , т.е. в классе задач, которые решаются полиномиальным вероятностным алгоритмом с односторонней ошибкой (подробнее об этом и других сложных классах можно прочесть в [24, 10] и многих других источниках). Однако мы не знаем ни одной работы, где это (или хотя бы определение доказуемого взлома) было бы формально описано и изучено.

Как мы уже упоминали в §2, одним из главных нерешённых вопросов современной теоретической криптографии является возможность построения надёжных примитивов, основанных на каких-нибудь естественных сложных предположениях, таких как $P \neq NP$. В этой работе мы представляем два немного отличающихся определения доказуемого взлома (одно слабее другого) и доказываем, что два различных криптографических протокола — протокол согласования ключа Аншель–Аншеля–Голдфельда и криптосистемы, основанные на инвариантах групп, — являются устойчивыми относительно доказуемого взлома в худшем случае, если $NP \not\subseteq RP$. Кроме того, мы разрабатываем способы сделать криптосистемы, основанные на инвариантах, устойчивыми и в обычном криптографическом смысле.

§4. Определения

Сначала мы определим доказуемый взлом криптосистем с открытым ключом, а затем расширим данное определение на протоколы согласования ключа. Мы представим два различных определения, одно стандартное, в среднем, другое в худшем случае. Для этого вспомним определение 2 и определим соответствующий ему доказуемый взлом.

Определение 4. Противник C осуществляет *доказуемый взлом* криптосистемы (G, E, D) , если для равномерного распределения по множеству сообщений m и множеству случайных битов всех участвующих в конструкции алгоритмов (публичный ключ pk берётся из пары (pk, sk) , сгенерированной алгоритмом порождения ключа $G(1^n)$)

$$\Pr [C(E(m, pk, r), pk) = (m, r')] \geq \frac{1}{poly(n)},$$

где $E(m, pk, r') = E(m, pk, r)$, а n — параметр надёжности.

Параметр надёжности в определении 4 играет роль длины ключа; параметр надёжности нужно выбирать так, чтобы время работы алгоритмов взлома, подсчитанное с этим параметром, было достаточно большим, чтобы взлом за это время был лишён смысла.

Если E — детерминированный алгоритм, то доказуемый взлом эквивалентен обычному взлому (множество случайных битов пусто). Противник может подтвердить, что он правильно угадал сообщение, попросту закодировав его ещё раз. Это и есть в точности идея доказуемого взлома. Противник должен не просто угадать сообщение, но ещё и доказать, что это действительно корректный код этого сообщения. В некоторых из наших примеров первая задача будет тривиальной, что не мешает второй задаче иметь большую сложность.

Мы также введём ещё одно, совсем сильное определение — противника, который взламывает криптосистему в худшем случае. Разница с обычным определением заключается в том, что противник должен добиваться успеха на *всех* входах.

Определение 5. Противник C осуществляет *доказуемый взлом в худшем случае* криптосистемы (G, E, D) , если для всех сообщений m , всех пар ключей (pk, sk) , сгенерированных алгоритмом порождения ключа $G(1^n)$, и всех случайных битов алгоритма кодирования E

$$\Pr [C(E(m, pk, r), pk) = (m, r')] \geq \frac{1}{\text{poly}(n)},$$

где $E(m, pk, r') = E(m, pk, r)$, n — параметр сложности, а распределение берётся по множеству случайных битов взламывающего алгоритма C .

Будем говорить, что криптосистема (G, E, D) *надёжна против доказуемого взлома (в худшем случае)*, если не существует полиномиальной вероятностной машины Тьюринга C , которая бы осуществляла доказуемый взлом (в худшем случае) криптосистемы (G, E, D) .

Замечание 2. Легко придумать тривиальную криптосистему, которая надёжна против доказуемого взлома (в смысле определения 4, что автоматически делает её надёжной и против взлома по определению 5). Пусть Боб передаёт своё сообщение открыто (раскодирование тогда становится тривиальным), но при этом добавляет в конец сообщения значение некоторой односторонней функции от своей случайной строки. Алиса может не обращать внимания на эту функцию, но Чарли придётся её обратить, чтобы получить подходящий набор случайных битов Боба. Поэтому цель

нашей работы из задачи построения криптосистем, надёжных против доказуемого взлома, превращается в задачу построения таких криптосистем, которые к тому же ещё и могут быть сделаны надёжными в обычном криптографическом смысле. Конечно, мы не сможем *доказать* их „традиционную“ надёжность, но мы представим конструкции, которые являются, на наш взгляд, достаточно надёжными криптосистемами.

§5. Криптосистемы, основанные на инвариантах групп, и их доказуемый взлом

5.1. Криптосистемы, основанные на инвариантах групп. В работе [1] первый автор предложил новый класс криптосистем — криптосистемы, основанные на инвариантах групп. В такой криптосистеме Алиса выбирает группу $G \leq GL(n, F)$, действующую на некотором векторном пространстве F^n . В качестве секретного ключа Алиса выбирает некоторое множество X и такой инвариант $f : F^n \rightarrow X$, что $\forall g \in G f(gx) = f(x)$. Она также выбирает набор (или пространство, заданное базисом) сообщений $M \subseteq F^n$; выбирает она его так, чтобы для каждого $m_1 \neq m_2 \in M$ $f(m_1) \neq f(m_2)$. Иначе говоря, разные сообщения $m \in M$ представляют разные орбиты группы G на множестве M . Таким образом, криптосистема, основанная на инвариантах, определяется набором (G, f, M) . В качестве публичного ключа Алиса передаёт образующие группы G и базис пространства M .

Боб выбирает вектор $m \in M$ (где m — сообщение, которое нужно закодировать) и случайный элемент $g \in G$. Затем Боб передаёт Алисе gm . Алиса может расшифровать сообщение, вычислив известный ей инвариант $f(gm) = f(m)$. Поскольку Алиса выбирала пространство сообщений M трансверсально орбитам, значение инварианта $f(m)$ однозначно позволит ей найти исходное сообщение m . Будем называть набор (G, f, M) *допустимым*, если он корректно определяет криптосистему, основанную на инвариантах.

Становится очевидным, что главная сложность в конструировании криптосистем, основанных на инвариантах, заключается в том, чтобы найти хорошо скрытый инвариант. В дальнейшем мы покажем несколько способов выбрать такой инвариант. Эти способы аналогичны предложенным в [31] и могут быть в общем описаны следующей конструкцией. Рассмотрим дерево, каждая вершина которого содержит набор (G, f, M) . Алиса строит это дерево от листьев к корню, на каждом шаге запоминая G, f и M . После создания дерева Алиса берёт криптосистему, получившуюся в корне дерева, и использует её для кодирования вышеописанным способом.

Таким образом, противник сможет взломать криптосистему, если он будет знать структуру этого дерева (мы предполагаем, что криптосистемы в листьях дерева взломать нетрудно, иначе нет смысла его строить). С точки зрения надёжности эта структура эквивалентна полному описанию инварианта, так что её тоже можно рассматривать как секретный ключ Алисы. Надёжность полученной криптосистемы будет основываться на сложности задач сопряжения и принадлежности к подгруппе, как и надёжность конструкций в работе [31]. В §6 мы подробно изложим эту конструкцию.

5.2. Криптосистема на инвариантах, доказуемый взлом которой влечёт $NP \subseteq RP$. Наша конструкция будет основана на модулярной группе. *Модулярная группа* — это мультипликативная группа $SL_2(\mathbb{Z})$ матриц 2×2 с определителем 1 (*унимодулярных матриц*). Групповые свойства этой конструкции подробно изложены, например, в [9].

В [14, следствие 11.5] Бласс и Гуревич доказали, что для модулярной группы *ограниченная задача принадлежности* (bounded membership problem, BM) является NP-полной. Задача формулируется следующим образом.

Задача 1. Пусть X — унимодулярная матрица, S — конечное множество унимодулярных матриц, а N — положительное целое число. Можно ли представить X в виде $\prod_{i=1}^m Y_i$, где $m \leq N$, и для каждого i либо Y_i , либо Y_i^{-1} лежит в S ?

Замечание 3. Не стоит путать эту задачу с другими задачами из работы [14], о которых там доказывается, что они DistNP-полны (полны относительно сложности в среднем). Основное отличие в данном случае заключается в том, что здесь речь идёт о задаче принадлежности *группе*, а DistNP-полные задачи получаются из проверки принадлежности различным *полугруппам*.

Рассмотрим в качестве G унимодулярную группу

$$G = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, x \in \mathbb{Z} \right\}.$$

В качестве инварианта мы рассмотрим достаточно тривиальный инвариант

$$f \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_2,$$

а в качестве пространства сообщений — пространство векторов

$$M = \left\{ \begin{pmatrix} 1 \\ x \end{pmatrix}, x \in \mathbb{Z} \right\}.$$

Боб выбирает случайный элемент g в этой группе, получая его в результате произведения не более чем N образующих. Затем он применяет g к вектору-сообщению m и передаёт полученный вектор gm и N . Алиса вычисляет $f(gm)$ и решает, каким был вектор m .

Отметим, что взломать эту „криптосистему“ можно совершенно тривиально: кодирование не меняет ту часть вектора, которая отвечает за само сообщение. Однако мы сейчас увидим, что её доказуемый взлом NP-труден.

Теорема 1. *Если существует противник C , осуществляющий доказуемый взлом в худшем случае описанной выше криптосистемы за время, полиномиальное от длины входа C , то $NP \subseteq RP$.*

Доказательство. Идея доказательства состоит в том, что доказуемый взлом NP-труден, потому что к решению задачи ограниченной принадлежности в подгруппе модулярной группы легко свести известную NP-трудную задачу, что было показано в [14].

Во-первых, отметим, что

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda + \mu \\ 0 & 1 \end{pmatrix}.$$

Таким образом, задача ограниченной принадлежности в подгруппе модулярной группы эквивалентна задаче, можно ли заданное число представить в виде ограниченной суммы других заданных чисел. Это задача Суммы Целых Чисел (Integer Sum Problem), NP-полнота которой доказана в [14].

Если полиномиальный алгоритм решает задачу поиска с вероятностью успеха $1/n^{\text{const}}$, эту вероятность легко увеличить до $3/4$, повторяя алгоритм полиномиальное число раз и выдавая ответ простым большинством. Поэтому если полиномиально ограниченный противник доказуемо взламывает в худшем случае представленную криптосистему, то $NP \subseteq RP$. $\square$

В §6 и 7 мы представим конструкции, которые позволяют сделать криптосистемы, основанные на инвариантах групп, более разумными с точки зрения обычной криптографической надёжности.

§6. Дерево групп

6.1. Общие замечания. Основанный на инвариантах протокол, который мы описали в предыдущем параграфе, на практике взломать ничуть не сложнее, чем криптосистему, которую мы описали в замечании в §4.

Обе конструкции, к сожалению, взламываются тривиально. В этой части нашей работы мы представим конструкцию, которая позволит нам „спрятать“ эти примитивы в большом дереве групп. Мы также можем использовать эту конструкцию для того, чтобы улучшить надёжность протокола согласования ключа Аншель–Аншеля–Голдфельда.

Мы следуем идеям работы [31], чтобы получить дерево троек „группа–инвариант–сообщения“. Если знать структуру дерева, можно будет эффективно вычислить инвариант в его корне, а если не знать, то инвариант окажется „спрятан“ за достаточно сложными задачами.

В оставшейся части этого параграфа мы сконцентрируемся на крипто-системах, основанных на инвариантах групп (введённых в §5), поскольку к протоколам согласования ключа идеи статьи [31] можно применить прямо и дословно, а вот для криптосистем, основанных на инвариантах, мы разработаем несколько новых конструкций. Далее мы рассмотрим те же операции, что и в [31], и проследим судьбу инвариантов, а также предложим несколько новых операций, относящихся сугубо к инвариантам групп. Но сначала нужно ввести базовые определения.

Каждой вершине v дерева мы сопоставляем набор (G_v, f_v, M_v) . Эти наборы получаются рекурсивно по построению дерева, применяя к каждой вершине, начиная от листьев и заканчивая корнем, одну из описанных ниже операций. Для каждой вершины v группа G_v является матричной группой $G_v \leq \text{GL}(n, R)$ для некоторого n и некоторого кольца R .

Всему дереву мы сопоставим полученный в его корне набор (G, f, M) , где $G \leq \text{GL}(n, R)$ — группа, f — инвариант, т.е. такая функция $f : R^n \rightarrow R$, что $\forall g \in G \forall x \in R^n f(gx) = f(x)$, и $M \subset F^n$ — канонический набор *сообщений*, взятых из прообразов разных значений инварианта f : $\forall m \neq m' \in M f(m) \neq f(m')$.

Публичный ключ состоит из R , n , группы G , заданной матричными образующими, и M . Цель построения дерева в том, чтобы спрятать секретный ключ — стоящий в корне инвариант.

Замечание 4. Заметим, что в ситуациях, когда мы меняем инвариант, мы можем либо изменить инвариант с f на $f \circ h$, либо сменить пространство сообщений с M на $h(M)$. Поскольку нам нужно спрятать именно инвариант, а пространство сообщений мы будем выдавать публично, мы всегда будем выбирать первый из этих способов.

Наша цель — совместить полученную таким способом обычную криптографическую надёжность с надёжностью против доказуемого взлома в худшем случае, который мы доказали в теореме 1. Чтобы это сделать, мы разместим доказуемо надёжную конструкцию, основанную на модулярной группе, в один из листьев дерева. Тогда Чарли, чтобы решить

задачу принадлежности в корне дерева, придётся решить задачу принадлежности для каждого листа (наша конструкция будет обладать этим свойством).

6.2. База рекурсии. Введём несколько формальных обозначений. Рассмотрим класс групп $\mathcal{G}$, замкнутый относительно некоторого множества теоретико-групповых операций $\mathcal{O}$ (список операций будет приведён ниже), которые преобразуют допустимые наборы в допустимые наборы. Для множества $\mathcal{G}_0 \subset \mathcal{G}$ (которое является базой конструкции) мы рекурсивно определим класс $\mathcal{P}(\mathcal{G}_0, \mathcal{O})$ четвёрок (G, f, M, T) следующим образом.

- *База рекурсии:* любая четвёрка (G, f, M, T) , где $G \in \mathcal{G}_0$, (G, f, M) является допустимым набором, а T — дерево из одной вершины, маркированной набором (G, f, M) .
- *Шаг рекурсии:* для всех наборов четвёрок $\{(G_i, f_i, M_i, T_i)\}_{i=1}^s$ и любой s -арной операции $o \in \mathcal{O}$ класс $\mathcal{P}(\mathcal{G}_0, \mathcal{O})$ содержит четвёрку (G, f, M, T) , где $G = o(G_1, \dots, G_s)$, $f = o(f_1, \dots, f_s)$, $M = o(M_1, \dots, M_s)$, а T — дерево, получающееся из деревьев $T_1, \dots, T_s$ добавлением нового корня с меткой o , к которому поддеревья $T_1, \dots, T_s$ добавляются как потомки.

6.3. Шаг рекурсии. В этом пункте мы рассматриваем конкретные операции, которые можно применять к допустимым наборам. Первый их набор был рассмотрен в [30]; нам только нужно проверить, что происходит с инвариантами в каждой из этих конструкций.

1. *Изменение базового кольца* $\phi : R \rightarrow R'$. Если кольцо уменьшается (R' вкладывается в R с некоторым вложением $\varphi : R' \rightarrow R$, и $\phi\varphi = id$), инвариант f преобразуется в инвариант $\phi(f)$, который действует по формуле $\phi(f)(x') = f(\varphi(x'))$. Если $\forall x \in R^n, g \in G$ $f(x) = f(gx)$, то

$$\forall x' \in R'^n, g \in G \quad \phi(f)(gx') = f(g\varphi(x')) = f(\varphi(x')) = \phi(f)f(x').$$

А вот если кольцо увеличивается, с инвариантами могут происходить менее приятные вещи (поскольку в кольце появляются новые элементы, старые равенства могут уже не выполняться). Поэтому в качестве операции по расширению дерева групп мы допускаем только уменьшение базового кольца.

Кроме прочего, это свойство позволяет нам заключить, что каждый инвариант, известный из теории инвариантов над полями, останется инвариантом и над кольцами, являющимися подкольцами этих полей; например, всякий инвариант над $\mathbb{C}$ останется инвариантом и над $\mathbb{Z}$.

Однако изменение базового кольца требует особой осторожности насчёт пространства сообщений. Если в пространстве сообщений были такие разные представители $m \neq m' \in M$, что $\phi(m) = \phi(m')$, то соответствующие сообщения в новом пространстве сообщений $\phi(M)$ станут неразличимы. Поэтому есть смысл применять эту операцию только тогда, когда $\phi(M)$ остаётся нетривиальным.

2. *Сопряжение* $g \mapsto h^{-1}gh$. Инвариант $f(x)$ под действием сопряжения превращается в инвариант $f'(x) = f(hx)$. Если $\forall g \in G \forall x \in R^n$ $f(gx) = f(x)$, то

$$\forall g \in G \forall x \in R^n \quad f'(h^{-1}ghx) = f(hh^{-1}ghx) = f(g(hx)) = f(hx) = f'(x).$$

Пространство сообщений M остаётся неизменным.

3. *Прямое произведение* $G_1, G_2 \mapsto G_1 \times G_2$. Будем рассматривать естественное представление прямого произведения: если $G_1 \leq GL(n_1, F)$ и $G_2 \leq GL(n_2, F)$, то $G_1 \times G_2 \leq GL(n_1 + n_2, F)$, и эта группа действует покомпонентно (а составляющие её матрицы блочно-диагональны). В этой ситуации если $f_1(x)$ и $f_2(x)$ были инвариантами G_1 и G_2 соответственно, то любой элемент $f \in \langle f_1(x), f_2(y) \rangle \leq R[x, y]$ будет инвариантом $G_1 \times G_2$. Можно выбрать случайный элемент этого множества, а пространство сообщений в любом случае превратится в $M_1 \times M_2$ (если столько различных сообщений не требуются, всегда можно выбрать несколько случайных из них, а остальные отбросить).
4. *Сплетение* $G \wr H$, где $G \leq GL(n, R)$, $H \leq S_m$. В этом случае мы рассматриваем естественное представление $G \wr H$ на R^{mn} ; $G \wr H$ действует в нём как

$$(g_1, \dots, g_m, \pi) \begin{pmatrix} x_1 \\ \dots \\ x_m \end{pmatrix} = \begin{pmatrix} g_1 x_{\pi(1)} \\ \dots \\ g_m x_{\pi(m)} \end{pmatrix}.$$

Тогда для любого инварианта f , если $\forall g \in G, x \in R^n$ $f(gx) = f(x)$, то же самое будет верно и для $G \wr H$, если рассмотреть f^m как действующий покомпонентно инвариант. Перестановка ничего не меняет в инвариантном равенстве. Пространство сообщений тогда вырастет до M^m (и вновь, если так много сообщений нам не нужно, мы можем либо выбрать несколько случайных, либо, например, оставить в качестве пространства сообщений только диагональ $\Delta = \{(x, \dots, x) \mid x \in M\}$).

Кроме этих способов, соответствующих групповым операциям, теория инвариантов может предложить несколько новых способов. В качестве

некоторых элементов наших преобразований троек $o \in \mathcal{O}$ мы возьмём преобразования, которые оставляют группу прежней ($o(G) = G$), а изменения касаются только инварианта f и пространства сообщений M . Следующие конструкции сработают, только если f — полиномиальный инвариант.

1. *Хессин* $H(f)$. Если f — полиномиальный инвариант G , и $\forall g \in G \leq GL(n, F) \det g = \pm 1$ (отметим, что в этой конструкции F должно быть полем), то

$$H(f) = \det \left(\frac{\partial^2 f}{\partial z_i \partial z_j} \right)$$

также будет инвариантом G . Группа G и пространство сообщений M остаются без изменений.

2. *Якобиан* J . Если $f_1, \dots, f_n$ — полиномиальные инварианты $G \leq SL(n, F)$ (отметим, что в этой конструкции F должно быть полем), то

$$J(f_1, \dots, f_n) = \det \left(\frac{\partial f_i}{\partial z_j} \right)$$

также будет инвариантом G . Таким способом мы можем объединить n одинаковых групп с разными инвариантами в один набор; скорее всего, это преобразование будет наиболее полезно на первом уровне дерева, где мы вольны выбрать сколько угодно одинаковых групп.

§7. Листья дерева

В предыдущем параграфе мы показали, как построить новый инвариант из существующих (проделать рекурсивный шаг конструкции). Однако остаётся вопрос: что должно быть базой этой рекурсии? Что мы можем поместить в листьях дерева?

7.1. Общие замечания. Первое замечание состоит в том, что в информатике мы не можем на самом деле работать над $\mathbb{C}$ или $\mathbb{R}$. Всё, что мы делаем при помощи компьютера, на самом деле происходит над $\mathbb{Q}$. Теория инвариантов над $\mathbb{Q}$ существенно отличается от классической теории инвариантов над $\mathbb{C}$. К счастью, отказываться от неё тоже не понадобится: если функция f была инвариантом группы $G \leq GL(n, \mathbb{C})$, представленной в виде матриц с рациональными коэффициентами, она всё равно останется инвариантом группы $G \leq GL(n, \mathbb{Q})$, поскольку у элементов G рациональные коэффициенты. Поэтому в дальнейшем мы будем иногда рассматривать инварианты над $\mathbb{C}$, но только в тех случаях, когда они без изменений переносятся на случай $\mathbb{Q}$.

Мы также могли бы рассматривать инварианты над конечными полями, так называемые *модулярные инварианты*; при этом теория заметно усложняется технически (ср. пример 4 в п. 7.3).

7.2. Классы Черна. В качестве стандартного хорошо известного примера конструкции из теории инвариантов мы напомним конструкцию *классов Черна* (см., например, [55]). Классы Черна — один из самых больших известных источников инвариантов конечных групп. Идея проста: рассмотрим орбиту a^G некоторого элемента $a \in F^n$ (мы будем предполагать, что G действует над полем) и заметим, что произведение

$$\prod_{b \in a^G} (x + b),$$

где x — формальная переменная, инвариантно под действием G (элементы G просто переставляют сомножители в этом произведении). Коэффициенты этого многочлена и называются *классами Черна*. Например, $\sum_{b \in a^G} b$ — первый класс Черна — это инвариант группы G .

Все классы Черна являются просто симметрическими функциями элементов орбиты действия G . Если a рассмотреть как неизвестное (переменную), мы получим искомые инварианты. Аналогичные конструкции верны и для компактных групп.

7.3. Примеры инвариантов конечных групп. В этом пункте мы приведём несколько примеров инвариантов различных конечных групп. Разумеется, это лишь несколько характерных примеров, их легко можно дополнить другими.

Пример 1. У симметрической группы S_n есть мономиальное представление $F^n \rightarrow GL(n, F)$; в этом представлении элементы S_n переставляют переменные. Кольцо инвариантов в этом представлении порождается всеми симметрическими многочленами, от $x_1 + \dots + x_n$ до $x_1 \dots x_n$. Это простейший пример классов Черна.

Пример 2. Образующую циклической группы $\mathbb{Z}_n$ можно представить как матрицу $g \in GL(m, F)$, для которой $g^n = e$ (унипотентную матрицу подходящего порядка). Чтобы функция f была инвариантом представления циклической группы, достаточно проверить, что она не меняется под действием единственной образующей: $f(x) = f(gx)$.

Например, циклическая группа $\mathbb{Z}_n$ имеет естественное представление в виде группы, порождённой $\xi_n e$, где ξ_n — примитивный корень из единицы степени n , а e — единичная матрица. Очевидно, инвариантом этой группы будет любой однородный многочлен. Можно сделать следующий

шаг и рассмотреть представление циклической группы $\mathbb{Z}_n$, порождённое матрицей

$$\begin{pmatrix} \xi_1 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & \xi_m \end{pmatrix},$$

где ξ_i — корни из единицы, $\xi_i^n = 1$. Тогда кольцом инвариантов этой группы будет кольцо многочленов $\mathbb{C}[x_1^n, \dots, x_m^n]$.

Заметим, что инварианты зависят не только от самих групп, но и от их представлений; одна и та же группа в разных представлениях будет иметь разные инварианты.

Пример 3. Диэдральная группа D_{2k} имеет представление $D_{2k} \rightarrow GL(2, \mathbb{R})$ как группа симметрий правильного многоугольника. В этом представлении D_{2k} порождается двумя матрицами

$$D_{2k} = \left\langle \begin{pmatrix} \cos \frac{2\pi}{k} & -\sin \frac{2\pi}{k} \\ \sin \frac{2\pi}{k} & \cos \frac{2\pi}{k} \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Тогда кольцо инвариантов диэдральной группы в этом представлении порождается многочленами

$$q = x^2 + y^2, \quad h = \prod_{i=0}^{k-1} \left(\left(\cos \frac{2\pi i}{k} \right) x + \left(\sin \frac{2\pi i}{k} \right) y \right).$$

Поскольку мы хотим рассуждать над $\mathbb{Q}$, нам требуется каким-либо образом перевести непрерывные тригонометрические функции на язык рациональных чисел. Это можно сделать сугубо формальным алгебраическим путём, введя дополнительные функциональные символы $\sin$ и $\cos$ с известными соотношениями на них $\sin^2 x + \cos^2 x = 1$, формулы двойного угла и т.д.

Пример 4. Для нечётного простого числа p диэдральная группа D_{2p} имеет представление $D_{2p} \rightarrow GL(2, \mathbb{F}_p)$ над конечным полем $\mathbb{F}_p$. Это представление порождается матрицами

$$D_{2k} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

В этом случае кольцо инвариантов изоморфно $\mathbb{F}_p[y, (xy^{p-1} - x^p)^2]$. Однако если перейти к дуальному представлению (просто транспонировав матрицы), кольцо инвариантов существенно изменится: оно теперь будет изоморфно $\mathbb{F}_p[x^2, y(y^{p-1} - x^{p-1})]$. В этом примере было важно, что группа была представлена над конечным полем степени, не взаимно-простой со степенью группы.

Эти два примера показывают, как сильно инварианты зависят от конкретного представления. Несколько других примеров инвариантов в контексте криптосистем, основанных на инвариантах, можно найти в [1].

7.4. Инварианты классических групп. В этом пункте мы представим несколько примеров хорошо известных инвариантов классических групп. Они также могут лежать в листьях дерева.

Пример 5. У ортогональной группы чётной размерности $SO(2l, F)$ есть хорошо известный *инвариант Диксона*: если $\text{char} F \neq 2$, а мы предположим, что так и есть, он имеет вид $(-1)^{\det g}$ для $g \in SO(2l, F)$. Этот инвариант работает в любом поле характеристики, отличной от двух. Отметим, что у этого инварианта всего два значения, поэтому он хорош для кодирования только одного бита.

Пример 6. Симплектическая группа $Sp(2n, F)$ по определению сохраняет невырожденную кососимметрическую билинейную форму. Значение этой формы и будет инвариантом (и, в отличие от предыдущего примера, полиномиальным инвариантом).

§8. Атаки на криптосистемы, основанные на инвариантах

Если мы хотим представить новую криптосистему или семейство криптосистем, представляется естественным проанализировать возможные атаки на эти криптосистемы. В этом параграфе мы рассмотрим несколько возможных атак на криптосистемы, основанные на инвариантах, а также дадим практические рекомендации о том, как от них защититься.

8.1. Атаки линейной алгеброй. Обычно самые тяжёлые атаки на алгебраические криптосистемы проходят посредством линейной алгебры: противник составляет систему линейных уравнений и находит секретный ключ (самый известный пример такого подхода взламывает схему Polly Cracker [23]; лишь в последнее время удалось улучшить эту схему так, чтобы атаки линейной алгеброй стали менее эффективными [43]).

Предположим, что инвариант f — это многочлен степени d . Тогда противник может рассмотреть его как многочлен с $\binom{n+d-1}{d}$ неопределёнными коэффициентами. Чтобы вычислить коэффициенты, противник должен решить уравнения $f(g_i m_j) = f(m_j)$ для всех элементов пространства сообщений $m_j \in M$ и всех образующих $g_i \in G$. Пространство решений этой системы даст противнику инвариант, разделяющий орбиты элементов M (вместе, конечно, с тривиальными инвариантами, такими, например, как

$f = \text{const}$). Если d константно, то эта атака действительно будет успешной, поэтому Алиса должна выбирать такие инварианты, чтобы $\binom{n+d+1}{d}$ было суперполиномиальным.

Пример 7. Предположим, что мы пытаемся построить криптосистему, основанную на инвариантах, на базе мономиального представления симметрической группы S_n , порождённой транспозициями τ_{ij} и её инвариант первой степени

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n.$$

В качестве пространства сообщений мы должны выбрать несколько векторов так, чтобы у них различались суммы коэффициентов; мы обозначим их через $m_i = (m_{i1}, \dots, m_{in})$. Противник, применяющий атаку линейной алгеброй, просто рассмотрит многочлен

$$h = \lambda_1 x_1 + \dots + \lambda_n x_n$$

и решит систему уравнений, удостоверяющих, что транспозиции не меняют h . Уравнение, соответствующее τ_{ij} , имеет вид $h(\tau_{ij}x) = h(x)$, что эквивалентно просто $\lambda_i = \lambda_j$. Таким образом, у противника получится вычислить правильный инвариант (возможно, умноженный на константу, что в данном случае не важно) после выполнения полиномиального алгоритма. Заметим, что для того чтобы эта атака не смогла преуспеть, можно было бы выбрать такие сообщения, чтобы в пространстве сообщений оказались сообщения с одинаковыми суммами элементов. Противнику не обязательно искать *тот самый* инвариант, ему достаточно найти *какой-нибудь* инвариант, разделяющий векторы из M .

8.2. Атаки методом Монте-Карло и размеры орбит. Другая проблема происходит из размеров орбит элементов M . Действительно, предположим, что элемент $m \in M$ имеет орбиту m^G полиномиального размера. Тогда у противника есть полиномиальный шанс декодировать $E(m)$, просто пытаясь случайно выбрать элемент $g \in G$ и сравнивая $E(m)$ и gm . Таким образом, элементы пространства сообщений нужно выбирать так, чтобы у них были орбиты большого размера.

Пример 8. В качестве тривиального, но характерного примера рассмотрим пространство сообщений, состоящее из нулевого вектора и какого-нибудь другого вектора (при этом не важно, какая группа — всё будет выполняться для любой подгруппы $GL(n, F)$ и любого инварианта). Размер орбиты нулевого вектора равен 1, и противнику вообще ничего не надо делать: если он видит нулевой вектор, значит, и сообщения было нулевым; а если он видит ненулевой вектор, значит, мы „закодировали“ что-то другое.

8.3. Атака, реконструирующая дерево групп. Наконец, противник может попытаться восстановить дерево, при помощи которого Алиса построила свой инвариант. На этом пути он может столкнуться с задачей, к примеру, поиска такой матрицы a , что $a^{-1}Ga = H$ для данных групп G и H . Это хорошо известная сложная задача; например, в [42] показано, что задача изоморфизма графов сводится к задаче сопряжения групп. Атаки такого рода были подробно рассмотрены в работе [30]; те же соображения можно применить и здесь, потому что задача восстановления дерева проще не стала. На самом деле она стала сложнее, потому что теперь узлы дерева дополнены инвариантами, которые тоже могут нетривиально меняться от узла к узлу. Следовательно, для восстановления дерева придётся восстановить не только группы, его составляющие, но и инварианты.

§9. Схема согласования ключа Аншель–Аншеля–Голдфельда и её устойчивость против взлома с доказательством

Прежде всего вспомним определение схемы согласования ключа Аншель–Аншеля–Голдфельда [6]. Рассмотрим группу G , и пусть два игрока A и B выбирают некоторые подгруппы G , заданные своими образующими:

$$G_A = \langle a_1, \dots, a_m \rangle, \quad G_B = \langle b_1, \dots, b_n \rangle.$$

Замечание 5. Отметим, что все рассуждения в этом параграфе проходят без изменений, если вместо G_A и G_B рассматривать $\bar{G}_A$ и $\bar{G}_B$, которые порождаются теми же образующими $\langle a_1, \dots, a_m \rangle$ и $\langle b_1, \dots, b_n \rangle$ соответственно, но не как группы, а как полугруппы. Все коммутаторы берутся в объемлющей группе G .

Группа G и элементы a_i , $1 \leq i \leq m$, и b_j , $1 \leq j \leq n$, выдаются публично. Оба игрока A и B случайно выбирают секретные элементы $a \in G_A$ и $b \in G_B$ как произведения не более чем N образующих, а затем передают друг другу следующую последовательность:

$$X_A = \{a^{-1}b_ja\}_{j=1}^n, \quad X_B = \{b^{-1}a_ib\}_{i=1}^m.$$

После этой передачи у игрока A (соотв. B) имеется представление элемента a (соотв. b) в подгруппе G_A (соотв. G_B). Значит, он может вычислить представление элемента $b^{-1}ab$ (соотв. $a^{-1}ba$), используя элементы последовательности X_A (соотв. X_B). Таким образом, у обоих участников образуется общий ключ, а именно коммутатор

$$a^{-1}(b^{-1}ab) = [a, b] = (a^{-1}ba)^{-1}b.$$

Очевидное необходимое условие надёжности этого протокола состоит в том, что множество всех коммутаторов элементов $a \in G_A$ и $b \in G_B$ должно состоять как минимум из двух элементов.

Чтобы доказуемо взломать протокол согласования ключа Аншель–Аншеля–Голдфельда, нужно найти представления определённых элементов a' в G_A и b' в G_B , где

$$X_A = \{a'^{-1}b_ja'\}_{j=1}^n, \quad X_B = \{b'^{-1}a_ib'\}_{i=1}^m.$$

Теорема 2. *Существуют такие подгруппы G_A и G_B модулярной группы $G = \text{SL}_2(\mathbb{Z})$, что если протокол согласования ключа Аншель–Аншеля–Голдфельда для группы G и её подгрупп G_A и G_B подвержен доказуемому взлому в худшем случае, то $NP \subseteq RP$. То же самое верно, если вместо G_A и G_B рассмотреть $\tilde{G}_A$ и $\tilde{G}_B$, порождённые теми же образующими $\langle a_1, \dots, a_m \rangle$ и $\langle b_1, \dots, b_n \rangle$ соответственно, но не как группы, а как полугруппы.*

Доказательство. Предположим, что есть такая вероятностная машина Тьюринга M , работающая полиномиально долго, что для бесконечной последовательности параметров надёжности N и входа

$$I = \{a_1, \dots, a_m, b_1, \dots, b_n, a^{-1}b_1a, \dots, a^{-1}b_ma, b^{-1}a_1b, \dots, b^{-1}a_nb\}$$

выполняется следующее условие:

$$\Pr \left[M(I) = a'_1, s_1, \dots, a'_f, s_f, b'_1, t_1, \dots, b'_g, t_g \right] \geq 1/p(N),$$

где $G_A = \langle a_1, \dots, a_m \rangle$ и $G_B = \langle b_1, \dots, b_n \rangle$ — подгруппы модулярной группы, p — некоторый полином, $a \in G_A$, $b \in G_B$, $a' = \prod_{i=1}^f a_i'^{s_i}$, $b' = \prod_{j=1}^g b_j'^{t_j}$, $a'_i \in \{a_i\}_{i=1}^m$, $b'_j \in \{b_j\}_{j=1}^n$, $a'^{-1}b_ja' = a^{-1}b_ja$ для всех $1 \leq j \leq n$, $b'^{-1}a_ib' = b^{-1}a_ib$ для всех s_i , а t_j лежат в $\{-1, 1\}$ для всех $1 \leq i \leq f$ и $1 \leq j \leq g$, $f, g \leq N$. Отметим, что мы можем проверить корректность ответа M , поэтому мы предполагаем, что M никогда не ошибается.

Используя M , можно построить вероятностную полиномиальную машину Тьюринга M' , которая содержит $p(N)/2$ копий M и на входе $(X, \{Y_i\}_i, N)$ выполняет следующий алгоритм.

1. Если $X = \prod_{i=1}^m Y_i'^{s_i}$, где $Y' \in \{Y_i\}_i$, $m \leq N$, $s_i \in \{-1, 1\}$ (если рассматривать G_A и G_B как полугруппы, здесь нужно брать только положительные степени), то $\Pr[M' \text{ принимает}] \geq 1/2$.
2. В противном случае $\Pr[M' \text{ принимает}] = 0$.

На вход всем копиям M мы подадим $a = b = X$, $a_i = b_i = Y_i$, а затем вычислим все $a^{-1}b_1a, \dots, a^{-1}b_ma, b^{-1}a_1b, \dots, b^{-1}a_nb$ за полиномиальное время. По [14, следствие 11.5] задача ВМ NP-полна, следовательно, $NP \subseteq RP$. $\square$

Замечание 6. Если $\tilde{G}_A$ и $\tilde{G}_B$ — полугруппы, то задача ВМ сложна, более того, в среднем [56].

Заметим, что описанный протокол согласования ключа может быть неустойчив против атак линейной алгеброй (см. п. 8.1): он даёт противнику решение задачи сопряжения, которое может оказаться единственным, при условии, что порождённое G_A (или G_B) кольцо совпадает с полным матричным кольцом. Чтобы этот протокол стал более устойчив против атак линейной алгеброй, можно заменить G древовидной конструкцией из групп или полугрупп, как это делалось в §6.

Формально говоря, мы строим следующую рекурсивную конструкцию для класса групп $\mathcal{G}$, замкнутого относительно некоторого набора теоретико-групповых операций $\mathcal{O}$; на этот раз нам не нужно беспокоиться о допустимых наборах, и все операции определены просто на группах из класса $\mathcal{G}$. Для множества $\mathcal{G}_0 \subset \mathcal{G}$ (базы нашей конструкции) мы рекурсивно определяем класс $\mathcal{P}(\mathcal{G}_0, \mathcal{O})$ пар (G, T) .

Рекурсивное определение делается точно так же, как в 6.2, опуская конструкции инвариантов и пространств сообщений. В нашем случае множество $\mathcal{O}$ допустимых операций состоит из изменения базового кольца, прямых произведений, сплетений и сопряжений (всё так же, как для криптосистем, основанных на инвариантах, но без специфических операций над инвариантами).

Надёжность протокола согласования ключа Аншель–Аншеля–Голдфельда для матричных групп основана на следующей задаче.

Задача линейной транспортировки (Linear Transporter Problem, LTP). Рассмотрим коммутативное кольцо R и R -модуль V . Пусть $G \leqslant GL(V, R)$. По данным $u \in V$ и $v \in u^G = \{u^g : g \in G\}$ найти такой элемент $g \in G$, что $v = u^g$.

Если противник может эффективно решить LTP, он может взломать протокол согласования ключа Аншель–Аншеля–Голдфельда. В [31] было доказано следующее утверждение (см. лемму 3.4).

Предложение 1. Пусть $G \in \mathcal{G}$. Тогда по данному дереву G , LTP для G можно решить за время, полиномиальное от размера дерева и времени решения задачи LTP для листьев дерева.

Конечно, это не доказывает, что надёжность протокола согласования ключа Аншель–Аншеля–Голдфельда в корне дерева зависит от надёжности протокола в листьях дерева. У нас на самом деле доказано куда более слабое утверждение, которое *дважды* идёт в неправильную сторону: во-первых, если мы можем решить ЛТР, мы можем взломать протокол Аншель–Аншеля–Голдфельда, а если мы можем решить ЛТР для листьев дерева, мы можем решить ЛТР для его корня. Чтобы доказать надёжность, нам нужно было бы обратить оба этих утверждения. Однако это лучшее, что мы можем сделать, и мы не знаем похожих конструкций с более сильными утверждениями.

§10. Заключение и открытые вопросы

В этой работе мы ввели новое понятие доказуемого взлома и, как следствие, доказуемой надёжности криптографических примитивов. В то время как это понятие, безусловно, гораздо слабее обычной криптографической надёжности, оно представляется достаточно естественным, хорошо определённым и разумным. Более того, это понятие надёжности — одно из немногих, для которых удаётся получить доказуемые позитивные результаты. Мы привели два примера криптографических протоколов, для которых удалось доказать устойчивость относительно доказуемого взлома: криптосистемы, основанные на инвариантах (теория этих криптосистем также была нами существенно расширена по сравнению с [1]), и частный случай протокола согласования ключа Аншель–Аншеля–Голдфельда. Мы уверены, что можно привести и новые примеры конструкций, для которых будут верны аналогичные утверждения.

Таким образом, с одной стороны, важным направлением для дальнейшей работы является поиск новых криптографических примитивов, надёжных против доказуемого взлома. С другой стороны, возможно, ещё важнее было бы связать доказуемый взлом и другие существующие понятия надёжности. Легко придумать криптосистему, для которой доказуемый взлом эквивалентен обычному (достаточно рассмотреть криптосистему, в которой Боб не использует случайных битов). Однако менее тривиальные примеры или общие утверждения, классифицирующие криптографические примитивы по этому признаку, могут представлять серьёзный интерес. Возможно, эту работу можно будет провести по схеме, впервые представленной в работах М. Айтая и С. Дворк [4, 20], позднее дополненных О. Регевом [50, 51], в которых удалось свести решение задачи в худшем случае к решению задачи в среднем и, таким образом, получить криптосистему, надёжную в обычном криптографическом смысле в некотором предположении о сложности задачи в худшем случае.

Благодарности. Авторы благодарны Э. А. Гиршу за плодотворные обсуждения результатов статьи и замечание 2.

Список литературы

- [1] Григорьев Д. Ю., *Криптография с открытым ключом и теория инвариантов*, Зап. науч. семин. ПОМИ **293** (2002), 26–38.
- [2] Григорьев Д. Ю., Пономаренко И. Н., *О неабелевых гомоморфных криптосистемах с открытым ключом*, Зап. науч. семин. ПОМИ **293** (2002), 39–58.
- [3] Левин Л. А., *Односторонние функции*, Проблемы передачи информации **39** (2003), №1, 103–117.
- [4] Ajtai M., Dwork C., *A public-key cryptosystem with worst-case/average-case equivalence*, STOC'97: 29th Annual ACM Symposium on Theory of Computing (El Paso, TX, 1997), ACM, New York, 1999, pp. 284–293 (electronic).
- [5] Anshel I., Anshel M., Fisher B., Goldfeld D., *New key agreement protocols in braid group cryptography*, Topics in Cryptology — CT-RSA 2001 (San Francisco, CA), Lecture Notes in Comput. Sci., vol. 2020, Springer, Berlin, 2001, pp. 13–27.
- [6] Anshel I., Anshel M., Goldfeld D., *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), 287–291.
- [7] Anshel I., Anshel M., Goldfeld D., *Non-abelian key agreement protocols*, Discrete Appl. Math. **130** (2003), no. 1, 3–12.
- [8] Anshel M., *Braid group cryptography and quantum cryptanalysis*, 8th Internat. Wigner Symposium (New York, USA, 2003), Baruch College of CUNY, pp. 13–27.
- [9] Apostol T. M., *Modular functions and Dirichlet series in number theory*, Grad. Texts in Math., vol. 41, Springer, New York, 1990.
- [10] Arora S., Barak B., *Complexity theory: a modern approach*, <http://www.cs.princeton.edu/theory/complexity/>, 2008.
- [11] Benaloh J., *Dense probabilistic encryption*, 1st Annual Workshop on Selected Areas in Cryptology (Queen's Univ., Kingston, Canada, 1994), Springer-Verlag, London, 1994, pp. 120–128.
- [12] Bennett C. H., Shor P. W., *Quantum information theory*, Information Theory: 1948–1998, IEEE Trans. Inform. Theory **44** (1998), no. 6, 2724–2742.
- [13] Blake I., Seroussi G., Smart N., *Elliptic curves in cryptography*, London Math. Soc. Lecture Note Ser., vol. 265, Cambridge Univ. Press, Cambridge, 2000.

- [14] Blass A., Gurevich Y., *Matrix transformation is complete for the average case*, SIAM J. Comput. **24** (1995), 3–29.
- [15] Blum N., *A Boolean function requiring $3n$ network size*, Theoret. Comput. Sci. **28** (1984), 337–345.
- [16] Bogdanov A., Trevisan L., *On worst-case to average-case reductions for NP problems*, 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS'03) (Cambridge, MA, USA, 2003), IEEE Computer Soc., Washington, DC, 2003, pp. 308–317.
- [17] Boneh D., Venkatesan R., *Breaking RSA may not be equivalent to factoring*, Advances in Cryptology — EUROCRYPT'98 (Espoo), Lecture Notes in Comput. Sci., vol. 1403, Springer, Berlin, 1998, pp. 59–71.
- [18] Brown D. R. L., *Breaking RSA may be as difficult as factoring*, Tech. Rep. 2005/380, Cryptology ePrint Archive, 2005.
- [19] Diffie W., Hellman M. E., *New directions in cryptography*, IEEE Trans. Inform. Theory **IT-22** (1976), 644–654.
- [20] Dwork C., *Positive applications of lattices to cryptography*, Mathematical Foundations of Computer Science 1997 (Bratislava) (MFCS'97), Lecture Notes in Comput. Sci., vol. 1295, Springer, Berlin, 1997, pp. 44–51.
- [21] Even S., Yacobi Y., *Cryptocomplexity and NP-completeness*, Automata, Languages and Programming (Proc. Seventh. Internat. Colloq., Noordwijkerhout, 1980), Lecture Notes in Comput. Sci., vol. 85, Springer, Berlin–New York, 1980, pp. 195–207.
- [22] Feigenbaum J., Merritt M., *Open questions, talk abstracts, and summary of discussions*, Distributed Computing and Cryptography (Princeton, NJ, 1989), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 2, Amer. Math. Soc., Providence, RI, 1991, pp. 1–45.
- [23] Fellows M., Koblitz N., *Combinatorial cryptosystems galore! Finite Fields: Theory, Applications, and Algorithms* (Las Vegas, NV, 1993), Contemp. Math., vol. 168, Amer. Math. Soc., Providence, RI, 1994, pp. 51–61.
- [24] Goldreich O., *Introduction to complexity theory*, Lecture notes, Weizmann Inst. Sci., 1998–99.
- [25] Goldwasser S., Bellare M., *Lecture notes on cryptography*, Summer course on cryptography at MIT, 2001.
- [26] Goldwasser S., Micali S., *Probabilistic encryption*, J. Comput. System Sci. **28** (1984), 270–299.
- [27] Grigoriev D., Hirsch E. A., Pervyshev K., *A complete public-key cryptosystem*, Tech. Rep. 006-046, Electronic Colloquium on Computational Complexity, 2006.

- [28] Grigoriev D., Kojevnikov A., Nikolenko S. I., *Invariant-based cryptosystems and their security against provable break*, Tech. Rep. 158, Max-Planck-Inst. Preprints, 2007.
- [29] Grigoriev D., Ponomarenko I., *Homomorphic public-key cryptosystems over groups and rings*, Complexity of Computations and Proofs, Quad. Mat., No. 13, Dept. Math. Seconda Univ. Napoli, Caserta, 2004, pp. 305–325.
- [30] Grigoriev D., Ponomarenko I., *Homomorphic public-key cryptosystems and encrypting Boolean circuits*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), 239–255.
- [31] Grigoriev D., Ponomarenko I., *Constructions in public-key cryptography over matrix groups*, Algebraic Methods in Cryptography (L. Gerritzen, D. Goldfeld, M. Kreuzer, R. Gerhard, and V. Shpilrain, eds.), Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 103–119.
- [32] Hankerson D., Menezes A., Vanstone S., *Guide to elliptic curve cryptography*, Springer-Verlag, New York, 2004.
- [33] Harnik D., Kilian J., Naor M., Reingold O., Rosen A., *On robust combiners for oblivious transfer and other primitives*, Advances in Cryptology — EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol. 3494, Springer, Berlin, 2005, pp. 96–113.
- [34] Hiltgen A. P., *Constructions of feebly-one-way families of permutations*, Advances in Cryptology — AUSCRYPT'92 (Gold Coast, 1992), Lecture Notes in Comput. Sci., vol. 718, Springer, Berlin, 1993, pp. 422–434.
- [35] Hiltgen A. P., *Towards a better understanding of one-wayness: facing linear permutations*, Advances in Cryptology — EUROCRYPT'98 (Espoo), Lecture Notes in Comput. Sci., vol. 1403, Springer, Berlin, 1998, pp. 319–333.
- [36] Hirsch E. A., Nikolenko S. I., *A feebly trapdoor function* (unpublished); available from <http://logic.pdmi.ras.ru/~hirsch/>, 2008.
- [37] Koblitz N., *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.
- [38] Kojevnikov A., Nikolenko S. I., *New combinatorial complete one-way functions*, 25th Symposium on Theoretical Aspects of Computer Science (STACS'08) (Bordeaux, February 2008), Bordeaux, 2008.
- [39] Lempel A., *Cryptography in transition*, Comput. Surveys **11** (1979), no. 4, 215–220.
- [40] Levin L. A., *One-way functions and pseudorandom generators*, Combinatorica **7** (1987), 357–363.

- [41] Lo H.-K., Spiller T., Popescu S. (eds.), *Introduction to quantum computation and information*, World Sci. Publ. Co., Inc., River Edge, NJ, 1998.
- [42] Luks E. M., *Permutation groups and polynomial-time computation*, Groups and Computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 139–175.
- [43] Ly L. V., *Polly Two: a new algebraic polynomial-based public-key scheme*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), 267–283.
- [44] Miller V. S., *Use of elliptic curves in cryptography*, Advances in Cryptology — CRYPTO'85 (Santa Barbara, CA, 1985), Lecture Notes in Comput. Sci., vol. 218, Springer, Berlin, 1986, pp. 417–426.
- [45] Myasnikov A. G., Shpilrain V., Ushakov A., *Group-based cryptography*, Birkhäuser, Basel, 2008.
- [46] Naccache D., Stern J., *A new public-key cryptosystem based on higher residues*, 5th ACM Conference on Computer and Communication Security (San Francisco, CA, USA, 1998), ACM Press, San Francisco, CA, 1998, pp. 59–66.
- [47] Nielsen M. A., Chuang I. L., *Quantum computation and quantum information*, Cambridge Univ. Press, Cambridge, 2000.
- [48] Okamoto T., Uchiyama S., *A new public-key cryptosystem as secure as factoring*, Advances in Cryptology — EUROCRYPT'98 (Espoo), Lecture Notes in Comput. Sci., vol. 1403, Springer, Berlin, 1998, pp. 308–318.
- [49] Rappe D. K., *Algebraisch homomorphe kryptosysteme*, Diplomarbeit, Dem Fachbereich Mathematik der Universität Dortmund, 2000.
- [50] Regev O., *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05: 37th Annual ACM Symposium on Theory of Computing (Baltimore, MD, USA, 2005), ACM, New York, 2005, pp. 84–93.
- [51] Regev O., *Lattice-based cryptography*, 26th Annual International Cryptology Conference (CRYPTO'06) (Santa Barbara, CA, USA, 2006), Lecture Notes in Comput. Sci., vol. 4117, Springer, Berlin, 2006, pp. 131–141.
- [52] Rivest R., Shamir A., Adleman L., *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126.
- [53] Rivest R. L., Kaliski B., *RSA problem*, Encyclopedia of Cryptography and Security, Kluwer Publ. House, 2005.
- [54] Shor P. W., *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509.

- [55] Smith L., *Polynomial invariants of finite groups*, Res. Notes Math., vol. 6, A. K. Peters, Wellesley, MA, 1995.
- [56] Venkatesan R., Rajagopalan S., *Average case intractability of matrix and diophantine problems*, STOC'92: 24th Annual ACM Symposium on Theory of Computing (Victoria, British Columbia, Canada, May 1992), ACM, New York, 1992, pp. 632–642.
- [57] Washington L., *Elliptic curves. Number theory and cryptography*, Chapman & Hall / CRC, Boca Raton, FL, 2003.
- [58] Wegener I., *The complexity of Boolean functions*, John Wiley and Sons, Ltd., Chichester; B. G. Teubner, Stuttgart, 1987.
- [59] Yao A., *How to generate and exchange secrets*, 27th IEEE Symposium on the Foundations of Computer Science (FOCS'86) (Toronto, Canada, October 1986), IEEE Computer Society, 1986, pp. 162–187.

IRMAR, Université de Rennes

Поступило 9 января 2008 г.

Beaulieu, 35042, Rennes

France

<http://perso.univ-rennes1.fr/dmitry.grigoryev/>

С.-Петербургское отделение

Математического института

им. В. А. Стеклова РАН

191023, Санкт-Петербург

наб. р. Фонтанки, 27

Россия

<http://logic.pdmi.ras.ru/~{arist,sergey}/>