В. А. Романьков, Криптографический анализ аналога схемы Диффи–Хеллмана, использующего сопряжение и возведение в степень, на матричной платформе, *ПДМ. Приложение*, 2014, выпуск 7, 56–58

ЛИТЕРАТУРА

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
2. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
3. *Рацеев С. М.* О совершенных имитостойких шифрах // Прикладная дискретная математика. 2012. № 3 (17). С. 41–47.
4. *Рацеев С. М.* О совершенных имитостойких шифрах замены с неограниченным ключом // Вестник Самарского государственного университета. Естественнонаучная серия. 2013. № 9/1 (110). С. 42–48.

УДК 512.62

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АНАЛОГА СХЕМЫ ДИФФИ — ХЕЛЛМАНА, ИСПОЛЬЗУЮЩЕГО СОПРЯЖЕНИЕ И ВОЗВЕДЕНИЕ В СТЕПЕНЬ, НА МАТРИЧНОЙ ПЛАТФОРМЕ[1]

В. А. Романьков

Доказано, что смешанный обобщённый вариант протокола Диффи — Хеллмана на матричной платформе, использующий одновременное возведение в степень и сопряжение фиксированной матрицы, в генерическом случае допускает вычисление разделённого ключа за полиномиальное время, если соответствующая кратная задача дискретного логарифма решается за полиномиальное время. Алгоритм вычисления использует разработанный автором метод линейного разложения, позволяющий находить разделённый ключ без решения задачи поиска сопрягающих элементов, и подход Менезеса с соавт., сводящий вычисление степени матрицы к решению кратной задачи дискретного логарифма. Комбинация этих двух подходов не может использоваться напрямую. Доказательство основного утверждения требует анализа содержаний мономиальных матриц в смежных классах по перестановочным подгруппам группы матриц. Это, в свою очередь, требует изучения аналогичного вопроса для групп подстановок. Последнее облегчается тем, что имеется ряд известных утверждений на эту тему.

Ключевые слова: *криптоанализ, проблема поиска, сопряжение, протокол Диффи — Хеллмана.*

Идея реализации протокола Диффи — Хеллмана на различных платформах, отличных от классических мультипликативных групп конечных полей и завоевавших признание групп эллиптических кривых, использована в целом ряде работ. Чаще всего в качестве платформы выбирались матричные группы, также предлагались конечные и абстрактные бесконечные группы, почти всегда допускающие точное представление матрицами над полем (кроме конечных — это свободные, конечно порождённые нильпотентные и метабелевы, а также полициклические группы, группы кос Артина и т. п.). В данной работе мы ограничимся рассмотрением матричного случая. В начальный период схема Диффи — Хеллмана просто переносилась с мультипликативной группы поля на матричную группу, то есть фиксировался элемент g матричной группы G, первый из корреспондентов (Алиса) выбирал случайное натуральное число k и посылал по открытой сети степень g^k, второй корреспондент (Боб) аналогично выбирал l и посылал g^l. После этого Алиса и Боб легко вычисляли общий ключ g^{kl}.

[1]Работа поддержана грантом РФФИ, проект № 13-01-00239-а.

Впрочем, довольно быстро было замечено [1, 2], что в случае матричной группы над полем можно одновременно сопряжением одной и той же матрицей в общем случае над расширением основного поля за счёт характеристических чисел фиксированной матрицы g приводить матрицу g к жордановой форме, а матрицы g^k и g^l — к соответствующим степеням этой жордановой формы. В случае, если размер хотя бы одной клетки жордановой формы матрицы g оказывался больше единицы, а степени k и l были меньше характеристики основного поля, эти числа вычислялись элементарно.

Основным, таким образом, оказывался случай, когда матрица g имела диагональную жорданову форму. Тогда вычисление секретных параметров k и l сводилось к решению кратных проблем дискретного логарифма для соответствующих друг другу наборов диагональных элементов полученных матриц. Конечно, в общем случае кратная проблема не сложнее обычной, а при случайном выборе данных может оказаться значительно проще обычной задачи вычисления дискретного логарифма в мультипликативной группе конечного поля. Действительно, задачу достаточно решить хотя бы для одной пары соответствующих диагональных элементов. К тому же тогда не имеет смысла рассматривать данный протокол как обобщение протокола Диффи — Хеллмана на некоммутативные платформы. Для полей нулевой характеристики задача, как правило, решается ещё проще и практически не рассматривается.

По только что описанной причине стали предлагать вместо возведения в степень сопряжение матрицы g матрицами a и b, которые случайным образом генерировались корреспондентами Алисой и Бобом (см., например, хорошо известный протокол Ко, Ли и др. [3]). Напомним, что сопряжение матрицы g матрицей a записывается как $g^a = a^{-1}ga$. Корреспонденты передают по сети результаты сопряжений g^a и g^b, а разделённый ключ вычисляется как $g^{ab} = g^{ba}$. Чтобы последнее равенство было справедливым, требуется, чтобы Алиса выбирала a из подгруппы A, а Боб — b из подгруппы B группы G, таких, что любой элемент a из A перестановочен с любым элементом b из B. Это возможно, например, если $A = B$ — абелева подгруппа группы G. Такой протокол основывался на трудности вычисления сопрягающих элементов по исходному и сопряжённому элементам. В дальнейшем происходил поиск групп, в которых эта проблема трудна. Почти всегда всё сводилось к вычислению в матричных группах. Например, как уже упоминалось выше, одна из наиболее популярных серий групп кос Артина может рассматриваться как серия матричных групп, поскольку все группы этой серии допускают точные и, что также имеет значение, эффективные представления матрицами над полем.

Однако оказалось, что в таких случаях совсем не обязательно вычислять матрицы a и b, чтобы получить разделённый ключ g^{ab}. Метод линейного разложения, описанный автором в [4] (см. также [5]), позволяет за полиномиальное время с помощью стандартных вычислений линейной алгебры найти g^{ab} без вычисления a и b. Таким образом, использованные в подобных протоколах предположения секретности, опиравшиеся на обоснования трудности решения проблемы поиска сопрягающего элемента, оказались бесполезными.

Но есть ещё один, смешанный, вариант протокола, когда Алиса выбирает число k и матрицу a, посылая по сети результат $(g^k)^a$, а Боб аналогично выбирает и посылает $(g^l)^b$. Разделённый ключ имеет вид $(g^{kl})^{ab}$. Этот протокол также неоднократно предлагался в различных версиях (см., например, [6]). Непосредственно вычислить этот ключ, используя метод линейного разложения, нельзя, так как возведение в степень не является автоморфизмом матричной группы. Вычислить k и l также затруднительно, поскольку сопряжения после приведения к жордановой форме содержат

диагональные элементы не в том порядке, как их содержала матрица g. Для вычисления параметров на первый взгляд нужно рассмотреть $n!$ кратных задач дискретного логарифма, где n — размер матриц. В общем случае это нереально. Основным результатом настоящей работы является следующая теорема, показывающая, что задача тем не менее решается в генерическом случае за полиномиальное время. Это обусловлено тем, что число случаев, которые действительно необходимо рассмотреть, значительно меньше $n!$, и в пределе равно 1.

Теорема 1. Смешанный обобщённый вариант протокола Диффи — Хеллмана, описанный выше, в генерическом случае допускает вычисление разделённого ключа $(g^{kl})^{ab}$ за полиномиальное время, если соответствующая кратная задача дискретного логарифма решается за полиномиальное время.

Слово «генерический» в данном контексте означает, что при случайном выборе коммутирующих поэлементно подгрупп A и B заявленное полиномиальное вычисление возможно «почти всегда» относительно естественной меры или асимптотически.

Поясним, что фигурирующая в формулировке кратная задача предполагается записанной для соответствующих друг другу наборов характеристических чисел исходной матрицы g и их степеней — характеристических чисел возведённой в эту степень матрицы g. Возможность полиномиального вычисления из формулировки теоремы объясняется тем, что сопрягающие элементы выбираются корреспондентами из коммутирующих поэлементно подгрупп, а в группах подстановок коммутирующие подгруппы допускают эффективное описание. В матричных группах подгруппа, элементы которой коммутируют с элементами другой достаточно «большой» подгруппы, не может содержать большой подгруппы мономиальных матриц.

ЛИТЕРАТУРА

1. *Menezes A. J. and Vanstone S.* A note on cyclic groups, finite fields, and the discrete logarithm problem // Applic. Alg. Eng. Commun. Comput. 1992. No. 3. P. 67–74.
2. *Menezes A. J. and Wu Y.-H.* The discrete logarithm problem in GL(n, q) // Ars Combinatoria. 1997. V. 47. P. 23–32.
3. *Ko K. H., Lee S. J., Cheon J. H., et al.* New public-key cryptosystem using braid groups // Advances in Cryptology — CRYPTO'2000. LNCS. 2000. V. 1880. P. 166–183.
4. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013. 135 с.
5. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3. С. 36–51.
6. *Kahrobaei D. and Khan B.* A non-commutative generalization of ElGamal key exchange using polycyclic groups // Global Telecommun. Conf. 2006. GLOBECOM'06, IEEE. P. 1–5.