МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.5; 00326.09

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ НЕКОТОРЫХ СХЕМ ШИФРОВАНИЯ, ИСПОЛЬЗУЮЩИХ АВТОМОРФИЗМЫ[1]

В. А. Романьков

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

E-mail: romankov48@mail.ru

Приводится криптографический анализ схем шифрования и распределения ключа, базирующихся на групповых (луповых) алгебрах и градуированных алгебрах с мультипликативным базисом, предложенных в работах С. К. Росошека, А. В. Михалева и др., А. Махалонобиса и др. Объединяет эти схемы (кроме одной из схем А. В. Михалева и др.) использование в них автоморфизмов. Приводится также криптографический анализ протокола распределения ключа Мегрелишвили и Джинджихадзе. Описывается оригинальный метод нахождения шифрованного сообщения или общего ключа, основанный на обычном аппарате линейной алгебры, при условии, что соответствующая платформа может быть выбрана как конечномерная алгебра, например как матричная алгебра над полем. Метод не предполагает нахождения секретных автоморфизмов, фигурирующих в указанных работах. Теоретические основы метода и ряд атак на его основе схем шифрования и распределения ключа, базирующихся на различных обобщениях задачи дискретного логарифма и идей Диффи — Хеллмана — Меркля на некоммутативные группы, изложены в других работах автора. Здесь метод находит новые применения.

Ключевые слова: *схема шифрования, групповая алгебра, луповая алгебра, матричная алгебра, градуированная алгебра, дискретный логарифм, обобщения дискретного логарифма, схема Диффи — Хеллмана, протокол ЭльГамаля, автоморфизм.*

Введение

Зарождение современной криптографии с открытым ключом обычно связывают с публикацией короткой заметки У. Диффи и М. Хеллмана [1]. В ней авторы не только впервые высказали замечательную идею открытой передачи секретных данных по незащищённым каналам связи без предварительного обмена корреспондентами какими-либо секретами, 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 М. Хеллмана [2], идея подобного

[1]Исследование выполнено при поддержке Министерства образования и науки РФ, проекты № 14.B37.21.0359 и 0859.

распределения ключей принадлежала Мерклю, поэтому сам протокол следует именовать *протокол Диффи — Хеллмана — Меркля*.

Протокол Диффи — Хеллмана — Меркля (DHM) работает следующим образом:

— Двое корреспондентов, скажем Алиса (А) и Боб (Б), выбирают конечную группу G и некоторый элемент g этой группы. При выборе А и Б пользуются незащищённым каналом связи, поэтому величины G и g считаются общеизвестными.
— Далее А выбирает случайным образом натуральное число $k \in \mathbb{N}$, вычисляет элемент g^k и передаёт его по открытому каналу корреспонденту Б. Само число k считается секретным.
— Б поступает аналогично: выбирает $l \in \mathbb{N}$, вычисляет и передает А элемент g^l. Число l считается секретным.
— Получив элемент g^l, А вычисляет элемент $(g^l)^k = g^{kl}$.
— Б делает то же самое, получая g^k и вычисляя $(g^k)^l = g^{kl}$.
— Элемент g^{kl} считается общим секретным ключом.

Реализация DHM должна быть такой, чтобы вычисление по данным G, g^k, g^l общего ключа g^{kl} было трудной вычислительной задачей. Эту задачу называют *проблемой Диффи — Хеллмана* (PDH). Она тесно связана с проблемой дискретного логарифма (PDL): по фиксированному элементу g известной конечной группы G и его степени $f = g^t$, $t \in \mathbb{N}$, определить число t, которое называется *дискретным логарифмом* элемента f относительно базы g и обозначается $\log_g f$. При ограничении $0 \leqslant t \leqslant \mathrm{ord}(g)$, где $\mathrm{ord}(g)$ обозначает порядок элемента g, дискретный логарифм $t = \log_g f$ определён однозначно. Обычно в качестве элемента g берется порождающий элемент конечной циклической группы $G = \mathrm{gp}(g)$. 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}.

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

В качестве платформ для DHM и других протоколов, основанных на трудности разрешимости PDL, стали использоваться также мультипликативные группы произвольных конечных полей F_q^*, $q = p^r$, p — простое, r — натуральное. Эти группы циклические, их элементы однозначно записываются в виде многочленов из кольца $F_p[x]$ степени не больше чем $r-1$. Вычисления ведутся по модулю неприводимого многочлена $h(x)$ степени r, по которому построено поле $F_q \simeq F_p[x]/(h(x))$.

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. 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 [3, 4], 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. Если матрица g приводится к диагональному виду, где на главной диагонали стоят эти характеристические числа, то такое сведение очевидно. В общем случае необходимо использовать более детальные рассуждения относительно жордановой формы матрицы g и её степеней. Есть и другие возможности сведения, о них см., например, в [5].

С самого начала использования некоммутативных групп появились аналоги дискретного логарифма. Наиболее популярным стало использование вместо возведения в степень сопряжения, в дальнейшем стали применяться правые и левые умножения и т. п. На этом строится целый ряд известных протоколов [6, 7]. 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. [8 – 11].

В [5] автор предложил 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 ряда известных протоколов, среди которых протоколы разделения ключа Ко, Ли и др. (сопряжение), протокол Стикелса (двустороннее домножение), итоговый секретный результат протокола (общий 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 всё 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 [12], линейны. Группы кос Артина — один из наиболее популярных объектов в криптографии [13 – 15]. Также линейны (см., например, [16, 17]) конечнопорождённые нильпотентные или, более общо, полициклические группы, которые всё чаще предлагаются в качестве платформ криптографических протоколов. Почти всегда предлагаемые для платформ алгебраические системы так или иначе представляются матрицами, что позволяет проводить атаку этим методом.

Данная работа посвящена криптографическому анализу 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.

1. Основная идея

Для представления основной общей идеи, позволяющей проводить эффективные атаки на схемы разделения ключа и шифрования в случае, когда платформой служит конечномерная алгебра над конечным полем, рассмотрим следующий достаточно простой протокол разделения ключа.

Протокол распределения ключей Мегрелишвили и Джинджихадзе [18] (см. также [19, 20])

Описание

Установка

Корреспонденты А и Б договариваются о выборе векторного пространства $V = F_2^n$ размерности n над полем F_2. Далее фиксируется квадратная матрица A размера $n \times n$ и вектор $v \in V$. Эти данные открыты.

Генерация ключей

Корреспондент А выбирает случайным образом натуральное число k, вычисляет и пересылает корреспонденту Б вектор $u = vA^k$. В свою очередь, корреспондент Б выбирает число l, вычисляет и пересылает А вектор $w = vA^l$.

Затем каждый из корреспондентов вычисляет общий ключ

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

Криптографический анализ системы Мегрелишвили и Джинджихадзе

Выпишем векторы $v = vA^0$, vA, …, vA^m до максимально возможной степени m с условием линейной независимости этого набора. Ясно, что $m \leqslant n$, поэтому процесс эффективен. Данный набор является базисом линейного пространства $\mathrm{lin}_{F_2}(vA^k, k \in \mathbb{N})$, порождённого всеми векторами вида $vA^k, k \in \mathbb{N}$. Для этого достаточно доказать, что любой вектор $vA^k, k \geqslant m+1$, линейно выражается через данный набор. Поскольку набор $v, vA, \ldots, vA^m, vA^{m+1}$ является первым линейно зависимым набором, вектор vA^{m+1} допускает разложение вида

$$vA^{m+1} = \sum_{i=0}^{m} \alpha_i vA^i,\ \alpha_i \in F_2.$$

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

$$vA^k = \sum_{i=0}^{m} \beta_i vA^i,\ \beta_i \in F_2. \tag{1}$$

Умножим обе части (1) справа на матрицу A и проведём преобразование с использованием равенства (1):

$$vA^{k+1} = \sum_{i=0}^{m} \beta_i vA^{i+1} = \sum_{i=0}^{m-1} \beta_i vA^{i+1} + \beta_m \sum_{i=0}^{m} \beta_i vA^i = \beta_m\beta_0 v + \sum_{i=1}^{m} (\beta_{i-1} + \beta_m\beta_i) vA^i.$$

Утверждение о базисе $v, vA, \ldots, vA^m$ пространства $\mathrm{lin}_{F_2}(vA^k, k \in \mathbb{N})$ следует по индукции.

Теперь можно получить разложение

$$u = vA^k = \alpha_0 v + \alpha_1 vA + \ldots + \alpha_m vA^m,\ \alpha_i \in F_2. \tag{2}$$

Заметим, что для получения разложения (2) не нужно знать k, а только u.

После этого подставим в правую часть полученного выражения (2), где все компоненты известны, вектор w вместо v и получим

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

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 подхода, основанного на вычислениях в линейных пространствах. В работе [5] дано описание целого ряда известных криптографических протоколов, которые также могут быть атакованы подобным образом. Конечно, конкретные реализации могут выглядеть более сложно, но основная идея проста. Она хорошо работает, если в качестве платформы выбирается конечномерная алгебра над конструктивным (например, конечным) полем. Конструктивность обеспечивает эффективную работу в соответствующем линейном пространстве, вычисление разложения по базису и т. п. В криптографии очень часто в качестве платформ шифрования предлагаются именно конечномерные алгебры над полями. Часто это алгебры матриц. Иногда это группы или полугруппы, допускающие представление матрицами над полем. Достаточно упомянуть группы кос, которые допускают точное представление матрицами над полем.

2. Криптографическая система Росошека [21, 22]

Описание

Установка

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

Корреспондент A выбирает автоморфизм σ кольца K большого порядка, а также автоморфизм ν группы G также большого порядка. Через $C(\sigma)$ обозначим централизатор элемента σ в группе $\operatorname{Aut} K$, а через $C(\nu)$ — централизатор автоморфизма ν в $\operatorname{Aut} G$. Считаем, что оба этих централизатора строго больше, чем подгруппы $\operatorname{gp}(\sigma)$ и $\operatorname{gp}(\nu)$ соответственно.

Генерация ключей

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

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

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 корреспондента A служит автоморфизм φ.

Далее A выбирает обратимый элемент $x \in KG$ и вычисляет $x^\varphi \in KG$.

Открытым ключом для A служит $(\sigma, \nu, x, x^\varphi)$.

Шифрование

Корреспондент Б для шифрования своего сообщения, закодированного в виде элемента m группового кольца KG, выбирает упорядоченную пару случайных натураль-

ных чисел (i, j), по которым определяет сессионный автоморфизм ψ группового кольца KG, полагая для любого элемента $h = a_{g_1}g_1 + \ldots + a_{g_n}g_n$, где $a_{g_1}, \ldots, a_{g_n} \in K$,

$$h^\psi = (a_{g_1}^{\sigma^i} g_1^{\nu^j} + \ldots + a_{g_n}^{\sigma^i} g_n^{\nu^j})_\xi, \tag{3}$$

где ξ есть случайная подстановка на множестве номеров слагаемых. После этого Б вычисляет $(x^{-1})^\psi$, используя открытый ключ А и автоморфизм ψ. Набор параметров (i, j, ψ) считается секретным сессионным ключом корреспондента Б.

Зашифрованное сообщение m имеет вид

$$c = ((x^{-1})^\psi, m(x^\varphi)^\psi). \tag{4}$$

Расшифрование

Корреспондент А, получив зашифрованное сообщение (4), 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.

К р и п т о г р а ф и ч е с к и й а н а л и з с и с т е м ы Р о с о ш е к а

Обозначим через $\sigma^i \wedge \nu^j, i, j \geqslant 0$, автоморфизмы алгебры KG, задаваемые указанным выше способом (3). Предположим, что K — алгебра над конечным полем F конечной размерности l и что любой автоморфизм кольца K является автоморфизмом K как алгебры над F. Это условие выполнено автоматически, если F — простое конечное поле. Поэтому достаточно требовать, чтобы K было алгеброй над простым конечным полем. В этом случае KG также естественно является алгеброй над 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 F.

Определим на группе Φ всех автоморфизмов вида $\sigma^i \wedge \nu^j$ для произвольного $r \geqslant 0$ *сферу* и *шар* радиуса r, полагая $S_r = \{\sigma^i \wedge \nu^j : i + j = r\}$ и $B_r = \bigcup\limits_{t=0}^{r} S_t$ соответственно. При этом $S_0 = B_0 = \{\sigma^0 \wedge \nu^0\} = \{1\}$.

Пусть x — фиксированный ненулевой элемент алгебры KG, выбранный корреспондентом А. Обозначим через x^Φ множество всех элементов алгебры KG вида $x^\eta, \eta \in \Phi$, другими словами — Φ-орбиту элемента x. Через $V = \mathrm{lin}_F(x^\Phi)$ обозначим линейное подпространство алгебры KG над полем F, порождённое множеством x^Φ.

Базис пространства V строим последовательно. Сначала полагаем $L_0 = \{x\}$. Затем расширяем L_0 до максимального линейно независимого множества L_1 подпространства $V_1 = \mathrm{lin}_F(x^{B_1})$. Для этого 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 $V_p = \mathrm{lin}_F(x^{B_p})$. Рассматриваем последовательно только те элементы вида $x^{\sigma^i \wedge \nu^j}, i + j = p + 1$, множества $x^{S_{p+1}}$, 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 $L = \{x^{\sigma^{q_i}\wedge\nu^{t_i}} : i = 1, \ldots, s\}$. Вычисляем соответствующее разложение

$$x^{\psi} = \sum_{i=1}^{s} \alpha_i x^{\sigma^{q_i}\wedge\nu^{t_i}}, \alpha_i \in F, i = 1, \ldots, s. \tag{5}$$

Подставим в правую часть выражения (5) вместо x элемент x^{φ}. Поскольку φ является автоморфизмом алгебры (достаточно даже — линейного пространства) KG над F и перестановочен с любым автоморфизмом из Φ, получаем

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

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

Комментарий

В работе [22] есть примеры, в которых в качестве K выбирается кольцо матриц $M_2(F_p)$, p — простое. Такое кольцо может рассматриваться как алгебра над F_p размерности 4. Если выбрать в нём произвольную матрицу a, а затем применить к ней автоморфизм σ^i, то образ a^{σ^i} можно довольно легко записать в виде линейной комбинации над 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 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 ещё 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}.

3. Протокол выработки общего секретного ключа Маркова, Михалева, Грибова, Золотых и Скаженика на платформе лупы Муфанг [23]

Напомним вкратце некоторые определения [24 – 26].

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 $(xy)(zx) = (x(yz))x$.

Приведём некоторые свойства лупы Муфанг [24 – 26]:

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 порождают в G подгруппу.

Описание

Установка

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

Алгоритм

1) Корреспондент А выбирает тройку случайных натуральных чисел (m, k, n), затем вычисляет и посылает Б сообщение вида

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

2) Корреспондент Б выбирает тройку случайных чисел (r, l, s), вычисляет и посылает А сообщение

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

3) Получив сообщение от Б, корреспондент А вычисляет элементы

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

4) Подобным же образом Б получает элементы

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

Общим ключом корреспондентов А и Б служит

$$K_{AB} = (a^{m+r} b^{k+l})(b^{k+l} c^{n+s}).$$

Объяснение

Утверждение 1 [23]. Если G — лупа Муфанг, $a, b \in G$, то для любых показателей $k, l, m, n, r, s \geqslant 0$ выполнено равенство

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

Корреспондент А получает ключ K_{AB} с помощью следующих вычислений:

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

Корреспондент Б получает ключ K_{AB} совершенно аналогично.

Криптографический анализ протокола выработки общего секретного ключа Маркова, Михалева, Грибова, Золотых и Скаженика на платформе лупы Муфанг

Предположим, что лупа Муфанг G содержится в конечномерной алгебре размерности m над полем F. В работе [23], например, рассматриваются в качестве возможных платформ для протокола неассоциативные, конечные и простые лупы Муфанг, которые называются лупами *Пейджа*. Они могут быть вложены в алгебры Цорна размерности 8 над конечным полем.

Возьмём 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 $b^{k+l} c^{n+s}$.

Сначала определим базисы подпространств $V_1 = \lin_F(a^i b^j : i, j \geqslant 0)$ и $V_2 = \lin_F(b^p c^q : p, q \geqslant 0)$ соответственно. Опишем построение базиса пространства V_1. (Базис пространства V_2 строится аналогично.) Для этого на множестве $\{a^i b^j\}$ для произвольного $r \geqslant 0$ определим сферу радиуса r, полагая $S_r = \{a^i b^j : i + j = r\}$, и шар радиуса r формулой $B_r = \bigcup_{t=0}^{r} S_t$. По определению, $S_0 = B_0 = \{1\}$. Пусть $L_0 = \{1\}$. Далее расширяем L_0 до $L_1 = \lin_F B_1$, просматривая последовательно по лексикографическому порядку элементы из S_1, включая в L_1 те из них, которые не выражаются

линейно через уже включенные. Если базис L_i пространства $\mathrm{lin}_F(B_i)$ уже определён, просматриваем последовательно элементы S_{i+1}, имеющие уже включенных в базис предшественников. У элемента a^ib^j предшественниками считаются $a^{i-1}b^j$ (если $i \neq 0$) и a^ib^{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 $L = \{a^{p_i}b^{q_i} : i = 1, \ldots, t\}$. Вычисляем соответствующее разложение

$$a^m b^k = \sum_{i=1}^{t} \alpha_i a^{p_i} b^{q_i}, \alpha_i \in F, i = 1, \ldots, t. \tag{6}$$

Используя правую часть (6), где все параметры известны, и элемент $a^r b^l$, получим

$$\sum_{i=1}^{t} \alpha_i (a^{p_i}(a^r b^l)) b^{q_i} = \left(a^r \left(\sum_{i=1}^{t} a^{p_i} b^{q_i} \right) \right) b^l = (a^r (a^m b^k)) b^l = a^{m+r} b^{k+l}.$$

Точно так же получаем элемент $b^{k+l}c^{n+s}$. Затем вычисляем искомое произведение $K_{AB} = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s})$.

4. Криптографическая система Грибова, Золотых и Михалева [27]

Описание

Установка

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

Корреспондент А выбирает автоморфизм σ кольца K большого порядка, а также 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

Корреспондент А 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 он задаёт автоморфизм φ лупового кольца KG следующим образом: для любого $h \in KG$ вида $h = a_{g_1}g_1 + \ldots + a_{g_n}g_n$, где $g_i \in G, a_{g_i} \in K, i = 1, \ldots, n$, определяет значение h^φ формулой

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

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

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

Шифрование

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

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

После этого Б 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

$$c = (a^{\chi}x^{\psi}, m((a^{\varphi})^{\chi}(x^{\varphi})^{\psi})). \tag{7}$$

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

Расшифрование

Корреспондент А, получив зашифрованное сообщение (7), вычисляет, пользуясь перестановочностью автоморфизмов φ, ψ и χ, очевидной из их построения, элемент $(a^{\chi}x^{\psi})^{\varphi} = (a^{\varphi})^{\chi}(x^{\varphi})^{\psi}$.

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

К р и п т о г р а ф и ч е с к и й а н а л и з к р и п т о г р а ф и ч е с к о й с и с т е м ы Г р и б о в а, З о л о т ы х и М и х а л е в а

Как и в криптографическом анализе протокола выработки общего секретного ключа Маркова, Михалева, Грибова, Золотых и Скаженика на платформе лупы Муфанг, обозначим через $\sigma^i \wedge \nu^j, i, j \geqslant 0$, автоморфизмы кольца KG, задаваемые указанным выше способом. Предположим, что KG — алгебра над конечным полем F конечной размерности m. Также предполагаем, что любой из рассматриваемых автоморфизм кольца K будет автоморфизмом K как алгебры над F. Это условие выполнено автоматически, если F — простое конечное поле. Поэтому достаточно требовать, чтобы K было алгеброй над простым конечным полем. Определим на группе Φ всех автоморфизмов вида $\sigma^i \wedge \nu^j, i, j \geqslant 0$, для произвольного $r \geqslant 0$ сферу S_r и шар 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 $V = \mathrm{lin}_F(a^{\Phi} \cdot x^{\Phi})$ обозначим линейное подпространство алгебры KG над полем F, порождённое множеством $a^{\Phi} \cdot x^{\Phi}$.

Базис L пространства V строим последовательно. Сначала полагаем $L_0 = \{a \cdot x\}$, затем расширяем L_0 до максимального линейно независимого множества L_1 подпространства $V_1 = \mathrm{lin}_F(a \cdot x^{B_1} \cup a^{B_1} \cdot x)$. Для этого рассматриваем последовательно в соответствии с лексикографическим порядком элементы $a \cdot x^{\sigma^i \wedge \nu^j}$, $i + j = 1$, и $a^{\sigma^i \wedge \nu^j} \cdot x$, $i + j = 1$, включая в L_1 те из них, которые не выражаются линейно через уже включенные до них элементы. Пусть уже построен базис L_r подпространства $V_r = \mathrm{lin}_F(a^{B_q} \cdot x^{B_p} : p + q = r)$. 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. либо элемент $a^{\sigma^{k-1} \wedge \nu^l} \cdot x^{\sigma^i \wedge \nu^j}$, либо элементы указанного вида, отвечающие наборам индексов $(k, l-1, i, j)$, $(k, l, i-1, j)$ 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 $L = \{a^{\sigma^{p_i}\wedge\nu^{r_i}} \cdot x^{\sigma^{q_i}\wedge\nu^{t_i}} : i = 1, \ldots, s\}$. Вычисляем соответствующее разложение

$$a^{\chi} \cdot x^{\psi} = \sum_{i=1}^{s} \alpha_i a^{\sigma^{p_i}\wedge\nu^{r_i}} \cdot x^{\sigma^{q_i}\wedge\nu^{t_i}}, \quad \alpha_i \in F, \quad i = 1, \ldots, s. \tag{8}$$

Подставим в правую часть выражения (8) a^{φ} вместо a и x^{φ} вместо x. Поскольку φ перестановочен с любым автоморфизмом из Φ, получаем

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

Остаётся, решив систему линейных уравнений, получить m.

Как отмечается в [27], «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. Криптографическая система Маркова, Михалева, Грибова, Золотых и Скаженика на платформе градуированного кольца с мультипликативным базисом [23]

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 $R = \bigoplus\limits_{\sigma\in G} R_\sigma$, $R_\sigma R_\tau \subseteq R_{\sigma\tau}$ 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 её базис B, что $B \cup \{0\}$ замкнуто относительно умножения.

Описание

Установка

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

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

Генерация ключей

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

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

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

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

Шифрование

Корреспондент Б 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 $h = a_{b_1}b_1 + \ldots + a_{b_n}b_n$, где $a_{b_i} \in R_e$, $i = 1, \ldots, n$,

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

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

Зашифрованное сообщение m имеет вид

$$c = (a^\chi \cdot x^\psi, m \cdot ((a^\varphi)^\chi \cdot (x^\varphi)^\psi)). \tag{9}$$

Расшифрование

Корреспондент А, получив зашифрованное сообщение (9), 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 корреспонденту А 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 системы Маркова, Михалева, Грибова, Золотых и Скаженика

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

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

Дальнейший анализ буквально повторяет рассуждения из криптоанализа системы Грибова, Золотых и Михалева. Для элементов $a, x \in R$ вычисляется базис подпространства $V = \mathrm{lin}_F(a^\Phi \cdot x^\Phi)$: $L = \{a^{\sigma^{p_i} \wedge \nu^{r_i}} \cdot x^{\sigma^{q_i} \wedge \nu^{t_i}} : i = 1, \ldots, s\}$. Далее вычисляем соответствующее разложение вида (8). 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. Протоколы обмена ключом Махалабониса [28]

6.1. Протокол обмена ключом Махалабониса 1

Описание

Установка

Пусть G — группа, g — элемент в G. Пусть Φ и Ψ — две подгруппы группы автоморфизмов $\mathrm{Aut}\,(G)$ группы G, элементы которых попарно коммутируют друг с другом, т. е. для любых $\varphi \in \Phi$, $\psi \in \Psi$ выполняется $\varphi \cdot \psi = \psi \cdot \varphi$. Эти данные являются открытыми.

Генерация ключей

1) Корреспондент А случайным образом выбирает автоморфизм $\varphi \in \Phi$. Затем вычисляет g^{φ} и посылает этот результат по незащищённому каналу связи корреспонденту Б.

2) Корреспондент Б случайным образом выбирает автоморфизм $\psi \in \Psi$. Затем вычисляет g^{ψ} и посылает результат по незащищённому каналу связи корреспонденту А.

Распределение ключей

Корреспондент А вычисляет $K_A = (g^{\psi})^{\varphi}$. Корреспондент Б вычисляет $K_B = (g^{\varphi})^{\psi} = (g^{\psi})^{\varphi}$.

Общий ключ есть $K = K_A = K_B = (g^{\psi})^{\varphi}$.

Криптографический анализ протокола обмена ключом Махалабониса 1

Пусть G — подгруппа группы всех обратимых матриц $\mathrm{GL}_n(A)$ над алгеброй A конечной размерности l над полем F. Тогда размерность алгебры $\mathrm{M}_n(A)$ над полем F равна $m = l \cdot n$.

Для простоты считаем, что подгруппы Φ и Ψ группы автоморфизмов $\mathrm{Aut}(G)$, фигурирующие в протоколе, конечно порождены. Пусть $\Phi = \mathrm{gp}(\varphi_1, \ldots, \varphi_k)$ и $\Psi = \mathrm{gp}(\psi_1, \ldots, \psi_l)$. Предположим также, что автоморфизмы подгруппы Ψ естественно продолжаются до линейных преобразований линейного пространства $\mathrm{lin}_F(G)$, порождённого группой G в линейном пространстве алгебры $\mathrm{M}_n(A)$ над F.

Тогда для любого $r \in \mathbb{N}$ определим сферу $S_r(\Phi)$ радиуса r, состоящую из всех групповых слов от порождающих элементов подгруппы Φ длины r. Шар $B_r(\Phi)$ радиуса r определяется как $\bigcup\limits_{i=0}^{r} S_i(\Phi)$. Как и раньше, $S_0(\Phi) = \{1\}$, т. е. сфера радиуса 0 состоит из пустого слова, записывающего единицу группы. Аналогично определяются сферы $S_r(\Psi)$ и шары $B_r(\Psi)$ подгруппы Ψ.

Обозначим через g^{Φ} множество всех элементов группы G вида $g^{\eta}, \eta \in \Phi$, другими словами — это Φ-орбита элемента g. Через $V = \mathrm{lin}_F(g^{\Phi})$ обозначим линейное подпространство алгебры $\mathrm{M}_n(F)$ над полем F, порождённое множеством g^{Φ}.

Базис подпространства V строим последовательно. Сначала полагаем $L_0 = \{g\}$. Затем расширяем L_0 до базиса L_1 подпространства $V_1 = \mathrm{lin}_F(g^{B_1})$. Для этого рассматриваем последовательно в соответствии с лексикографическим порядком элементы g^{λ}, $\lambda \in S_1(\Phi)$, включая в L_1 те из них, которые не выражаются линейно через уже включенные до них элементы. Пусть уже построен базис L_p подпространства $V_p = \mathrm{lin}_F(g^{B_p})$. Рассматриваем последовательно только те элементы вида g^{λ}, $\lambda \in S_{p+1}(\Phi)$, которые имеют предшественников в L_p, т. е. если в λ подслово (начиная со второй буквы) λ_1 длины p определяет элемент $g^{\lambda_1} \in L_p$. Перебираем их 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 $L = \{g^{\lambda_i}, \lambda_i \in \Phi, i = 1, \ldots, s\}$. Вычисляем соответствующее разложение

$$g^{\varphi} = \sum_{i=1}^{s} \alpha_i g^{\lambda_i}, \quad \alpha_i \in F, \quad i = 1, \ldots, s. \tag{10}$$

Подставим в правую часть выражения (10) вместо g элемент g^{ψ}. Поскольку ψ перестановочен с любым автоморфизмом из Φ и по предположению продолжается до линейного преобразования пространства $\mathrm{lin}_F(G)$, получаем

$$\sum_{i=1}^{s} \alpha_i (g^{\psi})^{\lambda_i} = \left(\sum_{i=1}^{s} \alpha_i g^{\lambda_i} \right)^{\psi} = (g^{\varphi})^{\psi} = (g^{\psi})^{\varphi}.$$

Таким образом получен общий ключ протокола.

Комментарий

Предлагаемый криптоанализ, более точно — атака на протокол возможна при двух условиях: точной представимости группы G матрицами над конечномерной алгеброй над полем и возможности расширения хотя бы одной из групп Φ или Ψ до группы линейных преобразований подпространства $\mathrm{lin}_F(G)$ пространства $\mathrm{M}_n(A)$. Это условие не является ограничительным, если G — конечная группа. Действительно, тогда голоморф $\mathrm{Hol}(G)$ (полупрямое расширение группы G с помощью её группы автоморфизмов $\mathrm{Aut}\,(G)$) также конечен и поэтому допускает точное представление матрицами над конечным полем. Все автоморфизмы группы G индуцируются внутренними автоморфизмами группы $\mathrm{Hol}(G)$, т. е. сопряжениями. Но любое сопряжение определяет не только линейное преобразование, но и автоморфизм соответствующей алгебры матриц.

Автор [28] предлагает использовать в качестве G конечно порождённую нильпотентную группу, ограничиваясь, впрочем, конечными группами в более детальных рекомендациях. Однако, если G — конечно порождённая нильпотентная (или даже более общо — полициклическая) группа, то ее голоморф $\mathrm{Hol}(G)$ представим матрицами над кольцом целых чисел $\mathbb{Z}$ (значит, и над полем рациональных чисел $\mathbb{Q}$) по теореме Мерзлякова [29]. Это также снимает ограничение на возможность использования описанной атаки.

6.2. Протокол обмена ключом Махалабониса 2

Описание

Установка

Пусть G — группа, g — элемент в G. Пусть Φ и Ψ — две подгруппы группы автоморфизмов $\mathrm{Aut}\,(G)$ группы G, элементы которых попарно коммутируют друг с другом. Данные G, Φ, Ψ являются открытыми. Элемент g — секретный.

Алгоритм

1) Корреспондент А случайным образом выбирает автоморфизм $\varphi \in \Phi$. Затем вычисляет g^{φ} и посылает этот результат по незащищённому каналу связи корреспонденту Б.

2) Корреспондент Б случайным образом выбирает автоморфизм $\psi \in \Psi$. Затем вычисляет $(g^{\varphi})^{\psi}$ и посылает результат корреспонденту А.

3) А вычисляет обратный автоморфизм φ^{-1} и применяет его к последнему сообщению, получая $((g^{\varphi})^{\psi})^{\varphi^{-1}} = g^{\psi}$. Затем А берёт другой автоморфизм $\xi \in \Phi$, вычисляет $(g^{\psi})^{\xi}$ и посылает результат корреспонденту Б.

Распределение ключа

Корреспондент Б вычисляет ψ^{-1} и применяет его к последнему сообщению, получая в итоге $((g^{\psi})^{\xi})^{\psi^{-1}} = g^{\xi}$.

Это и есть общий ключ.

К р и п т о г р а ф и ч е с к и й а н а л и з п р о т о к о л а о б м е н а к л ю ч о м М а х а л а б о н и с а 2

Пусть G — подгруппа группы всех обратимых матриц $\mathrm{GL}_n(A)$ над алгеброй A конечной размерности l над полем F. Тогда размерность алгебры $\mathrm{M}_n(A)$ над полем F равна $m = l \cdot n$.

Для простоты считаем, что подгруппы Φ и Ψ группы автоморфизмов $\mathrm{Aut}(G)$, фигурирующие в протоколе, конечно порождены. Пусть $\Phi = \mathrm{gp}(\varphi_1, \ldots, \varphi_k)$ и $\Psi = \mathrm{gp}(\psi_1, \ldots, \psi_l)$. Предположим также, что автоморфизмы подгруппы Ψ естественно продолжаются до линейных преобразований линейного пространства $\mathrm{lin}_F(G)$, порождённого группой G в линейном пространстве алгебры $\mathrm{M}_n(A)$ над F.

Строим базис L подпространства $\mathrm{lin}_F((g^\varphi)^\psi)^\Phi$ точно так же, как в криптоанализе предыдущего протокола. Пусть $L = \{((g^\varphi)^\psi)^{\lambda_i} : \lambda_i \in \Phi, i = 1, \ldots, s\}$. Получим выражение

$$(g^\psi)^\xi = \sum_{i=1}^{s} \alpha_i ((g^\varphi)^\psi)^{\lambda_i} = \left(\sum_{i=1}^{s} \alpha_i (g^\varphi)^{\lambda_i} \right)^\psi, \quad \alpha_i \in F. \tag{11}$$

Отсюда следует равенство

$$g^\xi = \sum_{i=1}^{t} \alpha_i (g^\varphi)^{\lambda_i}.$$

Значит, общий ключ g^ξ получается подстановкой элемента g^φ вместо $(g^\varphi)^\psi$ в правую часть выражения (11).

Заключение

Итак, в работе представлен подход, позволяющий находить передаваемое сообщение или общий ключ в целом ряде криптографических протоколов, базирующихся на конечномерных алгебрах. В ряде случаев протокол, не использующий конечномерной алгебры, можно превратить в протокол, базирующийся на конечномерной алгебре. Например, протокол, основанный на группе кос, можно с помощью известного представления группы кос матрицами превратить в протокол, базирующийся на матричной алгебре над полем. Подобный перевод на матричную платформу почти всегда возможен, если используются конечные алгебраические структуры.

Отличительной особенностью подхода является то, что в нём не вычисляются некоторые ключевые параметры протокола, не решаются соответствующие задачи поиска. Обычное представление о необходимости, а не только достаточности их решения оказывается в целом ряде случаев неверным.

В некоторых достаточно простых случаях эта идея уже высказывалась. Так, анализируя протокол распределения ключей, предложенный У. Романчук и В. Устименко [30], авторы [31] предложили атаку, похожую на описанные выше, а именно: в протоколе из [30] берётся в качестве платформы группа $\mathrm{GL}_n(F)$ над конечным полем F. Затем выбираются две коммутирующие матрицы $C, D \in \mathrm{GL}_n(F)$. Пусть $g \in F^n$ — фиксированный вектор. Эти данные открыты.

Корреспондент А выбирает многочлен $P = P(C, D) \in F[x, y]$, вычисляет и посылает вектор gP корреспонденту Б, который в свою очередь выбирает многочлен $Q = Q(C, D) \in F[x, y]$, вычисляет вектор gQ и посылает его А. Корреспондент А вычисляет ключ $K_A = (gQ)P = gQP$, Б делает то же самое, получая $K_B = (gP)Q = gPQ$. Так как C и D коммутируют, их общим ключом будет вектор $K = K_A = K_B$.

Потенциальный взломщик, подсмотрев по открытой сети gP, gQ и открытые данные C, D и g, вычисляет матрицу X, такую, что X коммутирует с A и D и, кроме

этого, выполняется равенство $gQ = gX$. Так как условия на X линейны, такая матрица легко вычислима. Далее легко получить ключ: $(gP)X = gXP = gQP = K$.

ЛИТЕРАТУРА

1. *Diffie W. and Hellman M. E.* New directions in cryptography // IEEE Trans. Inform. Theory. 1976. V. 22. P. 644–654.
2. *Hellman M. E.* An overview of public key cryptography // IEEE Communication Magazine. 2002. Iss. 50. P. 42–49.
3. *Menezes A. and 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.
4. *Menezes A. J. and Wu Y.-H.* The discrete logarithm problem in $\mathrm{GL}(n, q)$ // Ars Combinatoria. 1997. V. 47. P. 23–32.
5. *Романьков В. А.* Алгебраическая криптография. Омск: Изд-во Ом. ун-та, 2013. 207 с.
6. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-based cryptography. (Advances courses in Math., CRM, Barselona). Basel, Berlin, New York: Birkhäuser Verlag, 2008. 183 p.
7. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative cryptography and complexity of group-theoretic problems. (Amer. Math. Soc. Surveys and Monographs). Providence, RI: Amer. Math. Soc., 2011. 385 p.
8. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Trans. Inform. Theory. 1985. V. IT-31. No. 4. P. 469–472.
9. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.
10. *Koblitz N.* A Course in Number Theory and Cryptology. New York, Heidelberg, Berlin: Springer Verlag, 1994.
11. *Романьков В. А.* Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.
12. *Krammer D.* Braid groups are linear // Ann. Math. 2002. V. 151. P. 131–156.
13. *Dehornoy P.* Braid-based cryptography // Contemp. Math. 2004. V. 360. P. 5–33.
14. *Garber D.* Braid group cryptography. Lecture notes of Tutorials given at Braids PRIMA Summer School at Singapore, June 2007. `arXivmath.:0711.3941v2[cs.CR]` 27 Sep. 2008. P. 1–39.
15. *Mahlburg K.* An overview of braid groups cryptography // `www.math.wisc.edu/~boston/mahlburg.pdf`, 2004.
16. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1972.
17. *Lennox J. C. and Robinson D. J. S.* The Theory of Infinite Soluble Groups. Oxford Math. Monographs. Oxford: Oxford Science Publications, 2004.
18. *Мегрелишвили Р. П., Джинджихадзе М. В.* Однонаправленная матричная функция для обмена криптографическими ключами, метод генерации мультипликативных матричных групп // Proc. Intern. Conf. SAIT 2011, May 23–28, Kyiv, Ukraine. P. 472.
19. *Megrelishvili R., Chelidze M., and Chelidze K.* On the construction of secret and public-key cryptosystems // Appl. Math., Inform. Mech. 2006. V. 11. No. 2. P. 29–36.
20. *Megrelishvili R., Chelidze M., and Besiashvili G.* One-way matrix function — analogy of Diffie — Hellman protocol // Proc. Seventh Intern. Conf. IES-2010, 28 Sept.–3 Oct., Vinnytsia, Ukraine, 2010. P. 341–344.
21. *Росошек С. К.* Криптосистемы групповых колец // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 57–62.
22. *Росошек С. К.* Криптосистемы в группах автоморфизмов групповых колец абелевых групп // Фундаментальная и прикладная математика. 2007. Т. 13. № 3. С. 157–164.

23. *Марков В. Т., Михалев А. В., Грибов А. В. и др.* Квазигруппы и кольца в кодировании и построении криптосхем // Прикладная дискретная математика. 2012. № 4(18). С. 32–52.
24. *Белоусов В. Д.* Основы теории квазигрупп и луп. М.: Наука, 1967.
25. *Pflugfelder H. O.* Quasigroups and Loops: Introduction. Berlin: Heldermann Verlag, 1990.
26. *Smith J. D. H.* An Introduction to Quasigroups and their representations. Boca Raton, FL: Chapman & Hall/CRC, 2007.
27. *Грибов А. В., Золотых П. А., Михалев А. В.* Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 23–33.
28. *Mahalanobis A.* The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. 2008. V. 165. P. 161–187.
29. *Мерзляков Ю. И.* Целочисленное представление голоморфов полициклических групп // Алгебра и логика. 1970. Т. 9. № 5. С. 539–558.
30. *Romanczuk U. and Ustimenko V.* On the $PSL2(q)$, Ramanujan graphs and key exchange protocols // `http://aca2010.info/index.php/aca2010/aca2010/paper/viewFile/80/3`.
31. *Blackburn S. R., Cid C., and Mullan C.* Cryptanalysis of three matrix-based key establishment protocols // J. Mathematical Cryptology. 2011. V. 5. P. 159–168.