УДК 512.54; 519.725

ОБЩАЯ АЛГЕБРАИЧЕСКАЯ СХЕМА РАСПРЕДЕЛЕНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И ЕЁ КРИПТОАНАЛИЗ[1]

В. А. Романьков, А. А. Обзор

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

Показано, что многие известные схемы алгебраического открытого распределения криптографических ключей, использующие двусторонние умножения, являются частными случаями общей схемы такого вида. В большинстве случаев схемы строятся на платформах, которые являются подмножествами линейных пространств. К ним уже неоднократно применялся метод линейного разложения, разработанный первым автором. Метод позволяет вычислять распределяемые ключи без определения секретных параметров схемы, не решая лежащих в основе схем трудно разрешимых алгоритмических проблем. В работе показано, что данный метод применим к общей схеме, то есть является в определённом смысле универсальным. Общая схема выглядит следующим образом. Пусть G — алгебраическая система, на которой определена ассоциативная операция умножения, например группа, выбранная в качестве платформы. Предположим, что G является подмножеством конечномерного линейного пространства. Сначала задаётся открытое множество элементов $g_1, \dots, g_k \in G$. Затем корреспонденты, Алиса и Боб, последовательно публикуют элементы вида $\varphi_{a,b}(f)$ для $a, b \in G$, где $\varphi_{a,b}(f) = afb$, $f \in G$ и f — заданный или предварительно построенный элемент. Распределённый ключ имеет вид $K = \varphi_{a_l,b_l}(\varphi_{a_{l-1},b_{l-1}}(\dots(\varphi_{a_1,b_1}(g_i)\dots)) = a_l a_{l-1} \dots a_1 g_i b_1 \dots b_{l-1} b_l$. Предположим, Алиса выбирает параметры a, b из конечно порождённой подгруппы A группы G, Боб выбирает аналогичные параметры из конечно порождённой подгруппы B группы G, с помощью которых они конструируют преобразования вида $\varphi_{a,b}$, использованные в схеме. Тогда при некоторых естественных предположениях относительно G, A и B показывается, что любой злоумышленник может эффективно вычислить распределяемый ключ K без вычисления использованных в схеме преобразований.

Ключевые слова: *криптография, криптоанализ, распределение ключа, линейное разложение.*

DOI 10.17223/20710410/37/4

GENERAL ALGEBRAIC CRYPTOGRAPHIC KEY EXCHANGE SCHEME AND ITS CRYPTANALYSIS

V. A. Roman'kov, A. A. Obzor

Dostoevskii Omsk State University, Omsk, Russia

E-mail: romankov48@mail.ru, obzor2503@gmail.com

We show that many known schemes of the cryptographic key public exchange protocols in algebraic cryptography using two-sided multiplications are the special cases of a general scheme of this type. In most cases, such schemes are built on the platforms

[1]Исследование выполнено за счёт гранта Российского научного фонда (проект № 16-11-10002).

that are subsets of some linear spaces. They have been repeatedly compromised by the linear decomposition method introduced by the first author. The method allows to compute the exchanged keys without computing any private data and, consequently, without solving the hard algorithmic problems on which the assumptions are based. Here, we show that this method can be successfully applied to the following general scheme and, thus, is a universal one. The general scheme proceeds as follows. Let G be an algebraic system with the associative multiplication, for example, a group chosen as the platform. We assume that G is a subset of a finitely dimensional linear space. First, some public elements $g_1, \ldots, g_k \in G$ are taken. Then the correspondents, Alice and Bob, sequentially publicise the elements of the form $\varphi_{a,b}(f)$ for some $a, b \in G$, where $\varphi_{a,b}(f) = afb$, $f \in G$ and f is a given or previously built element. The exchanged key has the form

$$K = \varphi_{a_l,b_l}(\varphi_{a_{l-1},b_{l-1}}(\ldots(\varphi_{a_1,b_1}(g_i)\ldots)) = a_l a_{l-1}\ldots a_1 g_i b_1 \ldots b_{l-1} b_l.$$

We suppose that Alice chooses parameters a, b in a given finitely generated subgroup A of G, and Bob picks up parameters a, b in a finitely generated subgroup B of G to construct their transformations of the form $\varphi_{a,b}$. Under some natural assumptions about G, A and B, we show that an intruder can efficiently calculate the exchanged key K without calculation of the transformations used in the scheme.

Keywords: *cryptography, cryptanalisis, key exchange, linear decomposition.*

Введение

В алгебраической криптографии известен ряд схем шифрования и распределения ключей на алгебраических системах: группах, полугруппах, кольцах или алгебрах, в которых используются двусторонние умножения на элементы соответствующих систем. Таковы схемы Андрекута [1], Ванга и др. [2], Стикеля [3], Б. и Т. Харли [4, 5], Шпильрайна — Ушакова [6], а также ряд других схем, часть из которых изложена в [7, 8]. Сюда же можно отнести схемы, применяющие сопряжения, из которых наиболее известна схема Ко и др. [9] — некоммутативный аналог алгоритма Диффи — Хеллмана [10].

Введённый первым автором в рассмотрение метод линейного разложения, теоретические основы которого изложены в [11] (см. также [12, 13]), позволяет при определённых условиях эффективно находить в перечисленных выше и в ряде других криптографических схем и протоколов передаваемые или распределяемые данные без вычисления соответствующих секретных ключей шифрования. Основным условием является наличие в используемой платформе структуры линейного пространства. Приложения метода содержатся в приведённых выше работах, а также в [14 – 16] и ряде других работ. Заметим также, что в [17] предложен метод нелинейного разложения, уже не предполагающий наличия структуры векторного пространства у платформы, на которой строится схема. Метод хорошо работает, например, на ряде схем, построенных на полициклических группах, которые сейчас часто предлагаются в качестве платформ [18 – 20].

В данной работе мы обращаем внимание на то, что перечисленные схемы алгебраического открытого распределения ключей являются частными случаями одной общей схемы. При условиях, о которых говорилось выше, метод линейного разложения для нахождения распределяемых данных применим к этой общей схеме.

1. Описание общей схемы распределения ключей

В качестве платформы выбирается алгебраическая система G: группа, полугруппа, кольцо или алгебра. Каждая такая система наделена операцией умножения «$\cdot$». Предполагаем, что эта операция ассоциативна. Любой паре элементов $a, b \in G$ отвечает преобразование $\varphi_{a,b} : G \to G$, определённое правилом $\varphi_{a,b}(g) = a \cdot g \cdot b$, $g \in G$. В дальнейшем для упрощения записи операция «$\cdot$» не указывается.

Преобразования удовлетворяют соотношению $\varphi_{a,b} \circ \varphi_{c,d} = \varphi_{ca,bd}$ и образуют полугруппу $S(G)$. При наличии в G единицы 1 существует тождественное преобразование указанного вида $\varepsilon = \varphi_{1,1}$. Если элементы a и b обратимы, то определено обратное преобразование $\varphi_{a,b}^{-1} = \varphi_{a^{-1},b^{-1}}$. Если G — группа, то $S(G)$ также группа.

Обычно в протоколах указываются подмножества $A, B \subseteq G$, из которых выбираются элементы, участвующие в записи преобразований. При этом первый корреспондент — Алиса — выбирает эти элементы из A, а второй корреспондент — Боб — из B. Часто считается, что элементы из A и B попарно перестановочны между собой, то есть для любого $a \in A$ и любого $b \in B$ выполнено равенство $ab = ba$.

Рассматриваемые схемы устроены следующим образом. Сначала публикуются, то есть объявляются открытыми, несколько (обычно один) элементов $g_1, \ldots, g_k \in G$. Затем Алиса и Боб последовательно публикуют значения вида $\varphi_{a,b}(f)$, где $f \in G$ — уже опубликованный ранее элемент. Распределённый ключ выглядит как

$$K = \varphi_{a_l,b_l}(\varphi_{a_{l-1},b_{l-1}}(\ldots(\varphi_{a_1,b_1}(g_i)\ldots)) = a_l a_{l-1} \ldots a_1 g_i b_1 \ldots b_{l-1} b_l. \tag{1}$$

Отсюда видно, что для получения ключа K достаточно применить к элементу g_i преобразование $\varphi_{u,v}$, где $u = a_l a_{l-1} \ldots a_1$, $v = b_1 \ldots b_{l-1} b_l$. Предполагается, что все преобразования вида φ_{a_j,b_j} были использованы при публикации данных. Другими словами, для любой пары a_j, b_j среди опубликованных данных есть c и d, такие, что $d = \varphi_{a_j,b_j}(c)$. Если элементы a_j и b_j обратимы, то $c = \varphi_{a_j,b_j}^{-1}(d)$, то есть можно считать, что преобразование φ_{a_j,b_j}^{-1} также использовано и может быть включено в запись (1). Именно это обстоятельство при определённых условиях на G, A и B позволяет эффективно вычислить K, не определяя элементы a_j, b_j. Об этом говорится в п. 2. Заметим, что при этом становится несущественным, кто из корреспондентов выбирает конкретные значения a_j, b_j, определяя преобразование φ_{a_j,b_j}. Заметим, что в некоторых схемах (см., например, [4, 5]), кроме значений вида $\varphi_{a,b}(f)$, иногда публикуются суммы таких значений. Для рассматриваемых схем это несущественно, так как в процессе криптографического анализа восстанавливаются слагаемые таких сумм (см. пример из п. 3).

2. Основные леммы

Предположим, что в качестве платформы распределения ключей используется группа G, являющаяся подмножеством некоторого конечномерного линейного пространства V. Два корреспондента (Алиса и Боб) договариваются об элементе $h \in G$, а также о двух конечно порождённых подгруппах A и B группы G. Предполагается, что любой из элементов $a \in A$ перестановочен с любым из элементов $b \in B$. Все эти данные считаются открытыми.

Предположим, что в данной схеме корреспонденты, начиная с элемента h, последовательно публикуют элементы вида $\varphi_{a_i,b_i}(u) = a_i u b_i$, где $a_i, b_i \in A$ (Алиса), и $\varphi_{c_j,d_j}(u) = c_j u d_j$, где $c_j, d_j \in B$ (Боб), в записях которых u — один из уже полученных до этого элементов. Распределяемый ключ имеет вид

$$K = \varphi_{f_1,g_1}^{\varepsilon_1}(\varphi_{f_2,g_2}^{\varepsilon_2}(\ldots(\varphi_{f_t,g_t}^{\varepsilon_t}(h)\ldots)),$$

где каждая пара (f_r, g_r) совпадает либо с парой вида (a_i, b_i), либо с парой вида (c_j, d_j), $\varepsilon_r \in \{\pm 1\}$.

Следующая лемма показывает, как можно строить базисы линейных подпространств пространства V, порождаемые элементами из G определённого вида. Эта лемма содержится в [11 – 13] и приводится здесь для замкнутости изложения.

Лемма 1. Пусть A — конечно порождённая подгруппа группы G, $A = \langle a_1, \ldots, a_k \rangle$, G является подмножеством конечномерного линейного пространства V над полем $\mathbb{F}$ и h — элемент группы G. Допустим, что все основные вычисления в V, то есть сложение, умножение на скаляр, решение системы линейных уравнений, эффективны. Тогда существует эффективный способ построения базиса $E = \{e_1, \ldots, e_s\}$ линейного подпространства $\mathrm{Lin}(AhA)$, порождённого в V всеми элементами вида ahb, где $a, b \in A$.

Доказательство. Рассмотрим произвольно упорядоченное, начинающееся с h множество всех элементов вида $c^\varepsilon h d^\eta$, где $\varepsilon, \eta \in \{\pm 1\}$; c, d — элементы вида a_i или 1. Назовём это множество первым списком, обозначив его L_1. Выполним следующие операции построения части $\{e_1, e_2, \ldots\}$ базиса E, являющейся базисом линейного подпространства, порождённого списком L_1:

1) Полагаем $e_1 = h$.

2) Пусть уже построены элементы $\{e_1, \ldots, e_t\}$ базиса E. Рассматриваем следующий элемент списка $c^\varepsilon h d^\eta$. Если он линейно зависим с уже выбранными элементами, он удаляется из списка. Если независим, включается в E.

Когда первый список закончится, формируется новый произвольно упорядоченный список L_2 всех элементов вида $c^\varepsilon e_j d^\nu$, как при формировании первого списка, где e_j — элемент части E, сформированной после окончания первого списка (за исключением e_1).

Далее последовательно рассматриваются элементы списка L_2 и выполняется действие 2. После окончания действий с L_2, в результате которых будет получена часть базиса E, являющаяся базисом подпространства, порождённого списками L_1 и L_2, составляется третий список по тому же правилу, и т. д.

3) Процесс построения E закончен, если при обработке очередного списка в E не добавится ни одного элемента.

Объясним это заключение. Каждый новый список состоит из элементов предыдущего списка, домноженных слева и справа на порождающие элементы из A или их обратные, допускается, что один из домножаемых элементов равен 1. Введём обозначение $X = \{a_1^{\pm 1}, \ldots, a_k^{\pm 1}, 1\}$. Тогда первый список L_1 является подмножеством в XhX, второй — L_2 — подмножеством в X^2hX^2 и т. д. Если при обработке очередного списка $L_{i+1} \subseteq X^{i+1}hX^{i+1}$ ни один из его элементов не был включен в строящийся базис E, значит, L_{i+1} принадлежит линейному подпространству, порождённому всеми предыдущими списками (соответственно всеми уже построенными элементами базиса), т. е. $X^{i+1}hX^{i+1} \subseteq \mathrm{Lin}(\cup_{j=1}^{i} X^j h X^j)$. Но тогда $X^{i+2}hX^{i+2} \subseteq X(\mathrm{Lin}(\cup_{j=1}^{i} X^j h X^j))X \subseteq$ $\subseteq \mathrm{Lin}(\cup_{j=1}^{i+1} X^j h X^j) \subseteq \mathrm{Lin}(\cup_{j=1}^{i} X^j h X^j)$. Значит, рассмотрение списка L_{i+2} также не добавит базисных элементов, и т. д. В то же время очевидно, что рассматриваемое подпространство лежит в подпространстве, порождённом всеми списками. Из приведённого рассуждения следует, что всего списков, которые могут дать вклад в строящийся базис, не больше, чем размерность всего линейного пространства V. ■

Следующая лемма является ключевой в последующем криптографическом анализе. Предполагается, что выполнены все перечисленные выше соглашения.

Лемма 2. Пусть G — группа, являющаяся подмножеством конечномерного линейного пространства V над полем $\mathbb{F}$. Предположим, что даны элементы u и $v = \varphi_{a,b}(u)$, где $a, b \in A$ являются секретными для стороннего наблюдателя.

Тогда для любого элемента вида $w = \varphi_{c,d}(u)$, где $c, d \in B$ также неизвестны (другими словами, $w \in BuB$), можно определить элемент $z = \varphi_{a,b}(w)$, используя структуру линейного пространства V.

Доказательство. По условию $v \in AuA$. Строим базис E пространства $\mathrm{Lin}(AuA)$, как это объяснено в лемме 1. Пусть $E = \{a_1ub_1, \ldots, a_rub_r\}$, $a_i, b_i \in A$. Используя алгоритм Гаусса при решении соответствующих систем линейных уравнений, получаем разложение

$$v = \sum_{i=1}^{r} \alpha_i a_i u b_i, \ \alpha_i \in \mathbb{F}.$$

Все величины, входящие в запись (1), известны. Подставим в правую часть (1) вместо u элемент w и выполним необходимые преобразования, используя поэлементную перестановочность подгрупп A и B:

$$\sum_{i=1}^{r} \alpha_i a_i w b_i = \sum_{i=1}^{r} \alpha_i a_i c u d b_i = c \left(\sum_{i=1}^{r} \alpha_i a_i u b_i \right) d = cvd = caubd = a(cud)b = awb = z.$$

Лемма доказана. ■

Замечание 1. Приведённые результаты с очевидными поправками проходят также для случая, когда G — полугруппа (с единицей или без неё), A и B — подполугруппы.

Сформулируем *мнемоническое правило* эффективного получения элемента, вытекающее из лемм 1 и 2:

$$v = \varphi_{a,b}(u) \ (a, b \in A) \ \& \ w \in BuB \ \Rightarrow \ \varphi_{a,b}(w);$$
$$v = \varphi_{c,d}(u) \ (c, d \in B) \ \& \ w \in AuA \ \Rightarrow \ \varphi_{c,d}(w).$$

Приведённая запись означает, что, вычислив по лемме 1 базис соответствующего векторного пространства и зная элементы u и v из левой части правила (его предположений), можно эффективно вычислить образ элемента w из правой части правила (его заключения).

3. Примеры нахождения распределяемого ключа

Пример 1. Опишем протокол 1 Ванга и др. из [2]. В этой работе в качестве платформы протокола распределения ключа предлагается использовать одну из групп Артина B_n, $n \in \mathbb{N}$.

По известному представлению Лоуренс — Краммера каждая из групп B_n допускает точное матричное представление ρ над некоторым полем $\mathbb{F}$. Представление ρ и поле $\mathbb{F}$ определяются в явном виде. Обратное отображение ρ^{-1} также определяется эффективно [21]. Значит, можно предположить, что платформа G описываемого ниже протокола является частью конечномерного линейного пространства V.

Алиса и Боб соглашаются относительно выбора (неабелевой) группы G и случайно выбранного элемента $h \in G$, а также двух подгрупп A и B группы G, таких, что $ab = ba$ для любой пары элементов $a \in A$ и $b \in B$. Предполагаем, что подгруппы A и B заданы конечными множествами порождающих элементов $\{a_1, \ldots, a_n\}$ и $\{b_1, \ldots, b_m\}$ соответственно. Все эти данные считаются известными.

Алгоритм распределения ключа работает следующим образом:

— Алиса выбирает четыре элемента $c_1, c_2, d_1, d_2 \in A$, вычисляет $x = d_1c_1hc_2d_2$ и пересылает по открытой сети (публикует) элемент x, предназначенный Бобу.
— Боб выбирает шесть элементов $f_1, f_2, g_1, g_2, g_3, g_4 \in B$, вычисляет $y = g_1f_1hf_2g_2$ и $w = g_3f_1xf_2g_4$, затем публикует элемент (y, w), предназначенный Алисе.
— Алиса выбирает два элемента $d_3, d_4 \in A$, вычисляет $z = d_3c_1yc_2d_4$ и $u = d_1^{-1}wd_2^{-1}$, затем публикует элемент (z, u) для Боба.
— Боб вычисляет и публикует элемент $v = g_1^{-1}zg_2^{-1}$ для Алисы.
— Алиса вычисляет ключ $K_A = d_3^{-1}vd_4^{-1} = c_1f_1hf_2c_2$.
— Боб вычисляет ключ $K_B = g_3^{-1}ug_4^{-1} = c_1f_1hf_2c_2$, равный K_A.

В результате Алиса и Боб вырабатывают общий секретный ключ $K = K_A = K_B$.

Криптографический анализ

В протоколе использованы следующие преобразования:

$$\varphi_{d_1c_1,c_2d_2},\ \varphi_{g_1f_1,f_2g_2},\ \varphi_{g_3f_1,f_2g_4},\ \varphi_{d_3c_1,c_2d_4},\ \varphi^{-1}_{d_1,d_2},\ \varphi^{-1}_{g_1,g_2}.$$

Непосредственно проверяется, что ключ K можно представить в виде

$$K = \varphi_{c_1f_1,f_2c_2}(h) = \varphi^{-1}_{d_1,d_2}(\varphi_{d_1c_1,c_2d_2}(\varphi^{-1}_{g_1,g_2}(\varphi_{g_1f_1,f_2g_2}(h)))).$$

Проследим, что все вычисления при таком представлении ключа K может проделать любой наблюдатель (не знающий параметров преобразований), используя только леммы 1 и 2.

Результат первого преобразования $y = \varphi_{g_1f_1,f_2g_2}(h)$ известен, как передаваемое по сети сообщение.

Результат второго преобразования $\varphi^{-1}_{g_1,g_2}(y)$ определяется по мнемоническому правилу

$$v = \varphi^{-1}_{g_1,g_2}(z)\ \&\ y \in AzA\ \Rightarrow\ \varphi^{-1}_{g_1,g_2}(y) = f_1hf_2.$$

Результат третьего преобразования определяется по мнемоническому правилу

$$x = \varphi_{d_1c_1,c_2d_2}(h)\ \&\ f_1hf_2 \in BhB\ \Rightarrow\ \varphi_{d_1c_1,c_2d_2}(f_1hf_2) = d_1c_1f_1hf_2c_2d_2.$$

Результат четвертого преобразования определяется по мнемоническому правилу

$$u = \varphi^{-1}_{d_1,d_2}(w)\ \&\ d_1c_1f_1hf_2c_2d_2 \in BwB\ \Rightarrow\ \varphi^{-1}_{d_1,d_2}(d_1c_1f_1hf_2c_2d_2) = c_1f_1hf_2c_2 = K.$$

Пример 2. Известный протокол Ко и др. [9] называют *некоммутативным аналогом протокола Диффи — Хеллмана*. Предлагаемая его авторами платформа — одна из групп кос Артина B_n, $n \in \mathbb{N}$. Относительно её представления матрицами см. пример 1. Соглашения о первоначальном выборе платформы $G = B_n$, элемента $h \in G$, двух конечно порождённых подгрупп A и B группы G те же самые, что и в примере 1.

Алгоритм распределения ключа работает следующим образом:

— Алиса выбирает элемент $a \in A$, вычисляет $h^a = aha^{-1}$ и пересылает по открытой сети (публикует) элемент h^a, предназначенный Бобу.
— Боб выбирает элемент $b \in B$, вычисляет $h^b = bhb^{-1}$ и пересылает по открытой сети (публикует) элемент h^b, предназначенный Алисе.
— Алиса вычисляет ключ $K_A = (h^b)^a = h^{ab}$.
— Боб вычисляет ключ $K_B = (h^a)^b = h^{ba}$.

Так как $ab = ba$, эти ключи совпадают, предоставляя корреспондентам Алисе и Бобу секретный распределённый ключ $K = K_A = K_B$.

Криптографический анализ

Заметим, что

$$K = abha^{-1}b^{-1} = \varphi_{a,a^{-1}}(\varphi_{b,b^{-1}}(h)).$$

Результат первого преобразования $h^b = \varphi_{b,b^{-1}}(h)$ известен, как передаваемое по сети сообщение.

Результат второго преобразования определяется по мнемоническому правилу

$$h^a = \varphi_{a,a^{-1}}(h) \ \&\ h^b \in BhB \ \Rightarrow \ \varphi_{a,a^{-1}}(h^b) = K.$$

Пример 3. Опишем протокол Б. и Т. Харли [4, 5]. Пусть G — конечно порождённая коммутативная подгруппа общей линейной группы $\mathrm{GL}_n(\mathbb{F})$ над полем $\mathbb{F}$. Эти данные открыты.

Алгоритм работает следующим образом:

— Боб выбирает $y \in \mathbb{F}^n$ и элемент $b \in G$, вычисляет и публикует yb.
— Алиса хочет послать Бобу секрет $x \in \mathbb{F}^n$. Для этого она выбирает элементы $a_1, a \in G$, вычисляет и пересылает по сети сообщение (xa, yba_1), предназначенное Бобу.
— Боб выбирает $b_1, b_2 \in G$, вычисляет и пересылает сообщение (xab_1, ya_1b_2), предназначенное Алисе.
— Алиса вычисляет (xb_1, yb_2) и пересылает сообщение $xb_1 - yb_2$ для Боба.
— Боб вычисляет $x - yb_2b_1^{-1}$ и восстанавливает x.

Боб может использовать yb в дальнейшем.

Криптографический анализ

Так как платформа G — коммутативная группа, можно считать, что корреспонденты используют произвольные односторонние (правые) умножения $\rho_c = \varphi_{1,c}$, $c \in G$, а также, что $A = B = G$. Аргументы леммы 1 позволяют построить базисы подпространств вида $\mathrm{Lin}(gG)$, $g \in G$. Условие $w \in BuB$ леммы 2 выполняется автоматически. Соответственно упрощается мнемоническое правило. Подгруппа G порождает в $\mathrm{GL}_n(\mathbb{F})$ конечномерную подалгебру, на которую продолжаются действия преобразований ρ_c. Отсюда следует, что для вычисления секрета достаточно найти его выражение как элемента этой подалгебры через заданные элементы и использованные в протоколе преобразования вида ρ_c.

В рассматриваемом протоколе заданы элементы yb, xa и $xb_1 - yb_2$, использованы преобразования $\rho_{b_1}, \rho_{a_1}, \rho_{a_1b_2b^{-1}}$. Первое преобразование отвечает паре (xa, xab_1), второе — паре (yb, yba_1), третье — паре (yb, ya_1b_2).

Запишем искомое выражение:

$$x = \rho_{b_1}^{-1}(xb_1 - yb_2) + \rho_{b_1}^{-1}(\rho_{a_1}^{-1}(ya_1b_2)).$$

4. Оценка сложности алгоритмов в предложенном криптографическом анализе

Алгоритм, описанный в лемме 1, строит базис подпространства конечномерного линейного пространства над полем, используя метод Гаусса решения систем линейных уравнений. В каждом рассматриваемом случае нужно определить только наличие или отсутствие решения у данной системы. Для верхней оценки числа полевых операций

в алгоритме заметим, что это число в алгоритме Гаусса для матрицы размера $(t \times s)$ оценивается как $\mathrm{O}(t^2 s)$. Пусть r — размерность пространства V, что совпадает с числом уравнений в системах. Число неизвестных не превышает r, так как оно равно числу уже включённых в базис подпространства элементов и не может превышать размерности всего пространства. Значит, каждый раз выполняется не более $\mathrm{O}(r^3)$ операций. Общее число просматриваемых списков не превышает r, так как из каждого из них, за исключением последнего, хотя бы один элемент должен добавляться в базис. В то же время первый список должен дать хотя бы два элемента базиса. В каждом из списков не более $4k^2 r$ элементов. Всего таких элементов не более $2k^2 r^2$. Итоговая оценка даёт $\mathrm{O}(k^2 r^5)$ операций. Эта оценка весьма грубая.

В некоторых случаях необходимо учитывать предварительное представление платформы матрицами и операции, связанные с обратным переходом относительно таких представлений, чтобы записать полученный ключ в исходном виде. Например, в [21] показано, что из матричного вида элемента группы кос B_n его стандартная запись восстанавливается с использованием не более чем $\mathrm{O}(n^3 \log_2 d_t)$ операций, где d_t — некоторый эффективно вычислимый параметр, зависящий от соответствующего элемента. Заметим, что получение матричной записи элемента производится фактически за время, определяемое линейной функцией его длины.

В алгоритме леммы 2 также применяется алгоритм Гаусса. В данном случае он каждый раз находит единственное решение. Так как всего используется ограниченное число построений базиса и разложений по нему, общая оценка остается прежней: $\mathrm{O}(k^2 r^5)$.

ЛИТЕРАТУРА

1. *Andrecut M.* A Matrix Public Key Cryptosystem. arXiv math.: 1506.00277v1 [cs.CR], 31 May 2015.
2. *Wang X., Xu C., Li G., et al.* Double Shielded Public Key Cryptosystems. Cryptology ePrint Archive, Report 2014/558, Version 20140718:185200, 2014. `https://eprint.iacr.org/2014/558`
3. *Stickel E.* A new method for exchanging secret keys // Proc. Third Intern. Conf. ICITA 05. Contemp. Math. 2005. V. 2. P. 426–430.
4. *Harley B. and Harley T.* Group Ring Cryptography. arXiv: 1104.17.24v1 [math.GR], 9 April 2011. 20 p.
5. *Harley T.* Cryptographic Schemes, Key Exchange, Public Key. arXiv math.: 1305.4063v1 [cs.CR], May 2013. 19 p.
6. *Shpilrain V. and Ushakov A.* A new key exchange protocol based on the decomposition problem // Algebraic Methods in Cryptography. Contemp. Math. 2006. V. 418. P 161–167.
7. *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.
8. *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.
9. *Ko K. H., Lee S. J., Cheon J. H., et al.* New public-key cryptosystem using braid groups // CRYPTO 2000. LNCS. 2000. V. 1880. P. 166–183.
10. *Романьков В. А.* Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.
11. *Романьков В. А.* Алгебраическая криптография. Омск: Изд-во Ом. ун-та, 2013. 135 с.

12. *Романьков В. А.* Криптографический анализ некоторых известных схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.
13. *Myasnikov A. G. and Roman'kov V. A.* A linear decomposition attack // Groups Complexity Cryptology. 2015. V. 7. P. 81–94.
14. *Roman'kov V. A. and Menshov A. V.* Cryptanalysis of Andrecut's Public Key Cryptosystem. arXiv math.: 1507.01496v1 [math.GR], 6 Jul 2015.
15. *Горнова М. Н., Кукина Е. Г., Романьков В. А.* Криптографический анализ протокола аутентификации Ушакова — Шпильрайна, основанного на проблеме бинарно скрученной сопряжённости // Прикладная дискретная математика. 2015. № 2(28). С. 46–53.
16. *Roman'kov V. A.* A polynomial time algorithm for the braid double shielded public key cryptosystems // Bulletin of the Karaganda University. Mathematics Series. 2014. No. 4(84). P. 110–115; arXiv math.:1412.5277v1 [math.GR], 17 Dec 2014.
17. *Roman'kov V. A.* A nonlinear decomposition attack // Groups Complexity Cryptology. 2017. V. 8. P. 197–207.
18. *Eick B. and Kahrobaei D.* Polycyclic Groups: A New Platform for Cryptology? arXiv math.: 0411.077v1 [math.GR], 3 Nov 2004. 7 p.
19. *Gryak K. J. and Kahrobaei D.* The status of polycyclic group-based cryptography: A survey and open problems // Groups Complexity Cryptology. 2017. V. 8. P. 171–186.
20. *Cavallo B. and Kahrobaei D.* A Family of Polycyclic Groups over which the Conjugacy Problem is NP-complete. arXiv math.: 1403.4153v2 [math. GR], 19 Mar 2014. 14 p.
21. *Cheon J. H. and Jun B.* A polynomial time algorithm for the Braid Diffie — Hellman Conjugacy Problem // CRYPTO-2003. LNCS. 2003. V. 2729. P. 212–225.

REFERENCES

1. *Andrecut M.* A Matrix Public Key Cryptosystem. arXiv math.: 1506.00277v1 [cs.CR], 31 May 2015.
2. *Wang X., Xu C., Li G., et al.* Double Shielded Public Key Cryptosystems. Cryptology ePrint Archive, Report 2014/558, Version 20140718:185200, 2014. `https://eprint.iacr.org/2014/558`
3. *Stickel E.* A new method for exchanging secret keys. Proc. Third Intern. Conf. ICITA 05. Contemp. Math., 2005, vol. 2, pp. 426–430.
4. *Harley B. and Harley T.* Group Ring Cryptography. arXiv: 1104.17.24v1 [math.GR], 9 April 2011. 20 p.
5. *Harley T.* Cryptographic Schemes, Key Exchange, Public Key. arXiv math.: 1305.4063v1 [cs.CR], May 2013. 19 p.
6. *Shpilrain V. and Ushakov A.* A new key exchange protocol based on the decomposition problem. Algebraic Methods in Cryptography. Contemp. Math., 2006, vol. 418. pp 161–167.
7. *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.
8. *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.
9. *Ko K. H., Lee S. J., Cheon J. H., et al.* New public-key cryptosystem using braid groups. LNCS, 2000, vol. 1880, pp. 166–183.
10. *Roman'kov V. A.* Vvedenie v kriptografiyu. Kurs lektsiy [Introduction to Cryptography. Lecture Course]. Moscow, Forum Publ., 2012. 240 p. (in Russian)

11. *Roman'kov V. A.* Algebraicheskaya kriptografiya [Algebraic Cryptography]. Omsk, OmSU Publ., 2013. 135 p. (in Russian)
12. *Roman'kov V. A.* Kriptograficheskiy analiz nekotorykh izvestnykh skhem shifrovaniya, ispol'zuyushchikh avtomorfizmy [Cryptographic analysis of some known encryption schemes using automorphisms]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 35–51. (in Russian)
13. *Myasnikov A. G. and Roman'kov V. A.* A linear decomposition attack. Groups Complexity Cryptology, 2015, vol. 7, pp. 81–94.
14. *Roman'kov V. A. and Menshov A. V.* Cryptanalysis of Andrecut's Public Key Cryptosystem. arXiv math.: 1507.01496v1 [math.GR], 6 Jul 2015.
15. *Gornova M. N., Kukina E. G., and Roman'kov V. A.* Kriptograficheskiy analiz protokola autentifikatsii Ushakova —Shpil'rayna, osnovannogo na probleme binarno skruchennoy sopryazhennosti [Cryptographic analysis of the autentification protocol by Ushakov — Shpilrain based on the bi-twisted conjugacy problem]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 46–53. (in Russian)
16. *Roman'kov V. A.* A polynomial time algorithm for the braid double shielded public key cryptosystems. Bulletin of the Karaganda University. Mathematics Series, 2014, no. 4(84), pp. 110–115; arXiv math.:1412.5277v1 [math.GR], 17 Dec 2014.
17. *Roman'kov V. A.* A nonlinear decomposition attack. Groups Complexity Cryptology, 2017, vol. 8, pp. 197–207.
18. *Eick B. and Kahrobaei D.* Polycyclic Groups: A New Platform for Cryptology? arXiv math.: 0411.077v1 [math.GR], 3 Nov 2004. 7 p.
19. *Gryak K. J. and Kahrobaei D.* The status of polycyclic group-based cryptography: A survey and open problems. Groups Complexity Cryptology, 2017, vol. 8, pp. 171–186.
20. *Cavallo B. and Kahrobaei D.* A Family of Polycyclic Groups over which the Conjugacy Problem is NP-complete. arXiv math.: 1403.4153v2 [math. GR], 19 Mar 2014. 14 p.
21. *Cheon J. H. and Jun B.* A polynomial time algorithm for the Braid Diffie — Hellman Conjugacy Problem. CRYPTO-2003, LNCS, 2003, vol. 2729, pp. 212–225.