УДК 003.26 DOI 10.17223/2226308X/12/36

ЭФФЕКТИВНЫЕ МЕТОДЫ АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА И ЗАЩИТА ОТ НИХ[1]

В. А. Романьков

Работа состоит из двух частей. В первой части даётся представление авторских методов криптографического анализа алгоритмов алгебраической криптографии. Описываются основные элементы метода линейного разложения. Приводятся примеры его использования для эффективных атак на известные алгоритмы. Даётся представление об альтернативном подходе Б. Тсабана, также базирующемся на линейной алгебре и некоторых теоретико-вероятностных результатах. Кроме этого, приводится описание основных элементов метода нелинейного разложения с соответствующими примерами его применения. Вторая часть посвящена построению эффективных методов защиты от атак, использующих средства линейной алгебры. Для этого вводится новое понятие маргинального множества элементов группы относительно данного слова от порождающих элементов. Показывается, как использование маргинальных множеств позволяет уходить от проблемы нахождения сопрягающего элемента, лежащей в основе многих алгоритмов алгебраической криптографии, к значительно более сложной проблеме вхождения-сопряжённости.

Ключевые слова: *алгебраическая криптография, алгебраический криптоанализ.*

1. Методы криптоанализа алгебраической криптографии

1.1. Метод линейного разложения

Метод введён в рассмотрение автором в [1, 2], получил дальнейшее развитие в [3 – 5] и ряде других публикаций, подробно освещён в монографии [6]. Метод детерминированный и доказуемый, применим как к конечным, так и к бесконечным объектам. Его отличительной особенностью является то, что построенный по этому методу алгоритм криптографического анализа находит распределяемый ключ или передаваемое сообщение, не вычисляя секретных параметров, использованных при зашифровании. Алгоритм не решает алгоритмической проблемы, лежащей в основе криптографических построений, обходя тем самым построенную авторами защиту и не преодолевая трудностей, заложенных при построении криптографической схемы.

Метод использован для криптографического анализа криптографических алгоритмов Маркова — Михалева и др., Грибова — Золотых и др., Росошека, Харли, Мегрелишвили, Шпильрайна — Ушакова, Кахроби — Шпильрайна и др., Ко — Ли и др., Ванга и др., Курта, Хехта и ряда других авторов.

Метод работает в тех случаях, когда платформа шифрования G является частью линейного пространства V, например группой матриц над некоторым конструктивным полем $\mathbb{F}$ (конечным или бесконечным), рассматриваемой как подмножество линейного пространства $\mathrm{M}(n, \mathbb{F})$ матриц размера $n \times n$. Типичными элементами метода являются: построение базиса линейного подпространства, порождённого подмножеством из G определённого вида в пространстве V; использование свойств этого подпространства для определения секрета.

[1]Работа поддержана грантом РФФИ, проект № 18-41-550001а.

В криптографии с открытым ключом хорошо известна *проблема Диффи — Хеллмана*: для группы G и её элемента $g \in G$ определить по двум значениям g^k и g^l, где k, l — натуральные числа, значение g^{kl}.

В алгебраической криптографии рассматриваются следующие её некоммутативные аналоги:

— Аналог с сопряжениями: для группы G и её элемента $g \in G$ определить по двум сопряжённым к g элементам $g^a = aga^{-1}$ и $g^b = bgb^{-1}$, где $a, b \in G$, $ab = ba$, элемент $g^{ab} = abga^{-1}b^{-1} = bagb^{-1}a^{-1}$.

— Аналог с двусторонними домножениями: для группы G и её элемента $g \in G$ определить по двум элементам вида aga' и bgb', где $a, b \in G$, $ab = ba$, $a'b' = b'a'$, элемент $abga'b' = bagb'a'$.

— Аналог с автоморфизмами: для группы G и её элемента $g \in G$ определить по двум элементам вида $\alpha(g)$ и $\beta(g)$, где $\alpha, \beta \in \mathrm{Aut}(G)$, $\alpha\beta = \beta\alpha$, элемент $\alpha(\beta(g)) = \beta(\alpha(g))$.

Метод линейного разложения при некоторых естественных условиях на группу G (прежде всего это существование эффективного вложения в конечномерное линейное пространство) эффективно решает каждую из этих проблем.

1.2. Span-метод Б. Тсабана

В [7] (см. также [8]) Б. Тсабан и др. ввели в рассмотрение полиномиальный по времени вероятностный метод алгебраического криптоанализа, названный ими *линейным span-методом*. Метод позволяет разрабатывать способы эффективного решения вычислительных проблем в группах матриц над конечными полями, значит, и в группах, допускающих эффективные представления матрицами над конечными полями. Метод улучшает более ранние методы, описанные в [9, 10].

Как и в методе линейного разложения, span-метод предполагает построение базисов некоторых линейных подпространств, определяемых матричной группой G над конечным полем $\mathbb{F}_q$ порядка q.

Приведём типичный пример использования метода. Допустим, нужно решить проблему поиска сопрягающего элемента X для данных матриц A и $B = XAX^{-1}$ из группы $\mathrm{GL}(n, \mathbb{F}_q)$. Данное уравнение заменяется на систему линейных однородных уравнений, соответствующую матричному уравнению $XA = BX$. Строится базис $E = \{e_1, \ldots, e_s\}$ пространства решений и записывается общее решение $X = \sum\limits_{i=1}^{s} \alpha_i e_i$. Теперь нужно, варьируя коэффициенты α_i, $i = 1, \ldots, s$, найти среди решений невырожденную матрицу X. Нам известно, что невырожденное решение существует. Тогда можно воспользоваться следующей леммой.

Лемма 1 (лемма обратимости [7, Lemma 9]). Пусть элементы $e_1, \ldots, e_s$ кольца матриц $\mathrm{M}(n, \mathbb{F}_q)$ таковы, что некоторая их линейная комбинация $\sum\limits_{i=1}^{s} \alpha_i e_i$ с коэффициентами из $\mathbb{F}_q$ является обратимой матрицей. Если коэффициенты выбираются в соответствии с равномерным распределением на $\mathbb{F}_q$, то вероятность получения невырожденного решения будет не меньше чем $p = 1 - n/q$.

Метод эффективен, если n существенно мало по отношению к q.

1.3. Метод нелинейного разложения

Данный метод введён автором в [11] как дополнение к методу линейного разложения. Он работает в тех случаях, когда группа не допускает представления матрицами или это представление имеет слишком большой размер для возможного использования. Конечно, здесь также предполагается выполнение ряда условий, связанных

с разрешимостью проблемы вхождения в конечно порождённые подгруппы группы, выбранной в качестве платформы для криптографической схемы. Эти условия, как правило, выполняются в конечно порождённых нильпотентных и полициклических группах, часто предлагаемых для такого применения в последние годы. Относительно соответствующей теории см. [6], приложения можно найти в [4, 5, 12].

Метод нелинейного разложения при некоторых естественных предположениях о группе G (прежде всего, они касаются эффективной разрешимости проблемы представления элемента конечно порождённой подгруппы в виде слова от её порождающих элементов) эффективно решает перечисленные выше три проблемы, аналогичные проблеме Диффи — Хеллмана.

1.4. Примеры использования методов линейного и нелинейного разложения

Рассмотрим общую схему, под которую подпадает большое число алгоритмов, использующих двусторонние домножения. Далее приведены два примера конкретных протоколов, показывающие широкую применимость методов линейного и нелинейного разложения для построения алгоритмов криптографического анализа.

Общая схема алгоритмов, использующих двусторонние домножения

Данный раздел основан на работе автора [13]. Большинство известных схем алгебраической криптографии, использующих двусторонние домножения, являются частными случаями одной общей схемы (см. описание ниже). Часто такие схемы строятся на группах, являющихся подгруппами линейных пространств, например на матричных группах. Метод линейного разложения позволяет эффективно вычислять в данном случае распределяемый ключ или передаваемое сообщение без вычисления секретных параметров [1 – 4, 14 – 17]. Далее описаны некоторые основные элементы такого вычисления и приведены примеры его использования.

Некоторые такие схемы предложены М. Андрекутом [18], Л. Гу и др. [19, 20], Б. и Т. Харли [21, 22], В. Шпильрайном и А. Ушаковым [23], Е. Стикелем [24], Х. Вангом и др. [25]. Ряд схем описан в [26, 27]. Схемы, использующие сопряжения, например известная схема Ко — Ли и др. [28], рассматриваемая как некоммутативный аналог классической схемы Диффи — Хеллмана [29], также могут анализироваться указанным способом.

Пусть G — группа, выбранная в качестве платформы для схемы распределения ключа. Предположим, что G — подмножество конечномерного линейного пространства V. Два корреспондента, Алиса и Боб, соглашаются относительно элемента $h \in G$ и двух конечно порождённых подгрупп A и B группы G, заданных конечными множествами порождающих элементов. Предположим, что любой элемент $a \in A$ перестановочен с любым элементом $b \in B$. Все эти данные открыты.

Корреспонденты, начиная с h, попеременно публикуют элементы вида $\varphi_{a,a'}(u) = aua'$, где $a, a' \in A$ (Алиса), и $\varphi_{b,b'}(u) = bub'$, где $b, b' \in B$ (Боб), а u равен h или совпадает с одним из ранее построенных элементов. Алиса, как и Боб, может публиковать сразу несколько элементов. Распределённый ключ имеет вид

$$K = \varphi_{c_l,c'_l}(\varphi_{c_{l-1},c'_{l-1}}(\dots(\varphi_{c_1,c'_1}(g)))) = c_l c_{l-1} \dots c_1 g c'_1 \dots c'_{l-1} c'_l,$$

где каждая пара (c_t, c'_t) совпадает либо с парой вида (a, a'), $a, a' \in A$, либо с парой вида (b, b'), $b, b' \in B$.

Криптоанализ общей схемы

Следующая лемма говорит о возможности эффективного построения базиса линейного подпространства пространства V, порожденного элементами группы G определённого вида. Различные версии этой леммы доказаны в [1–4, 13], см. также [6].

Лемма 2. Пусть A — конечно порождённая подгруппа группы G, являющейся подмножеством конечномерного пространства V над полем $\mathbb{F}$, и h — фиксированный элемент из G. Предположим, что все основные операции в V, то есть сложение и умножение на скаляр, эффективно вычислимы. В этом случае эффективно строится базис $E = \{e_1, \ldots, e_s\}$ любого линейного подпространства $\mathrm{Lin}(AhA)$, порождённого всеми элементами вида aha', где $a, a' \in A$.

Следующая лемма является ключевым утверждением для алгебраического криптоанализа схем с двусторонними домножениями. Предполагается выполнение условий, данных выше.

Лемма 3. Пусть $v = \varphi_{a,a'}(u)$, где $a, a' \in A$ — закрытые параметры Алисы. Тогда для любого элемента $w = \varphi_{b,b'}(u)$, где $b, b' \in B$ (другими словами, $w \in BuB$), эффективно строится элемент $z = \varphi_{a,a'}(w)$. Построение этого элемента основывается на структуре линейного пространства V.

Пример 1. Рассмотрим протокол Ванга и др. из [25]. В нём корреспонденты выбирают в качестве платформы одну из групп B_n кос Артина. В 1990 г. Р. Лоуренс описала семейство представлений групп B_n матрицами. Примерно через 10 лет С. Бигелоу [30] и Д. Краммер [31] независимо доказали линейность групп B_n. В частности, было установлено, что представления Лоуренс $\rho_n : B_n \to \mathrm{GL}_{n(n-1)/2}(\mathbb{Z}[t^{\pm 1}, s^{\pm 1}])$ являются вложениями для любого $n \in \mathbb{N}$. Они стали называться представлениями *Лоуренс — Краммера*. Образ $\rho_n(g)$ эффективно строится по любому $g \in B_n$. Более того, существует эффективная процедура восстановления косы $g \in B_n$ по её образу $\rho_n(g)$. В [9] показано, что это может быть сделано за $\mathrm{O}(2m^3 \log d_t)$ умножений элементов матриц $\rho_n(g)$. Здесь $m = n(n-1)/2$ и d_t — параметр, эффективно вычислимый по $\rho_n(g)$ (см. [9] относительно деталей).

Таким образом, можно предположить, что G является частью линейного пространства V.

Перейдём к описанию протокола. Алиса и Боб выбирают группу G и случайный элемент $h \in G$. Также они выбирают две конечно порождённые подгруппы A и B группы G, такие, что $ab = ba$ для любой пары элементов $a \in A$ и $b \in B$. Эти данные открыты.

Алгоритм.

1) Алиса выбирает элементы $c_1, c_2, d_1, d_2 \in A$, вычисляет и публикует $x = d_1 c_1 h c_2 d_2$ для Боба.
2) Боб выбирает элементы $f_1, f_2, g_1, g_2, g_3, g_4 \in B$, вычисляет и публикует $y = g_1 f_1 h f_2 g_2$ и $w = g_3 f_1 x f_2 g_4$ для Алисы.
3) Алиса выбирает элементы $d_3, d_4 \in A$, вычисляет и публикует $z = d_3 c_1 y c_2 d_4$ и $u = d_1^{-1} w d_2^{-1}$ для Боба.
4) Боб вычисляет и публикует $v = g_1^{-1} z g_2^{-1}$ для Алисы.
5) Алиса вычисляет распределённый ключ $K_A = d_3^{-1} v d_4^{-1} = c_1 f_1 h f_2 c_2$.
6) Боб вычисляет распределённый ключ $K_B = g_3^{-1} u g_4^{-1} = c_1 f_1 h f_2 c_2$ равный K_A.
7) Распределённый ключ: $K = K_A = K_B$.

Криптоанализ.

Протокол использует следующие преобразования:

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

Прямым вычислением получаем выражение K:

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

Покажем, что ключ K эффективно вычислим по леммам 2 и 3.
Выход первого преобразования $y = \varphi_{g_1f_1,f_2g_2}(h)$ открыт.
Выход второго преобразования $\varphi^{-1}_{g_1,g_2}(y)$ эффективно вычислим:

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

Выход третьего преобразования эффективно вычислим:

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

Выход четвёртого преобразования эффективно вычислим:

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

Таким образом вычислен K.

Пример 2. Следующий протокол Махалонобиса [32] можно рассматривать как некоммутативный аналог классического протокола Масси — Омуры. Естественно предположить, что в группе G эффективно выполнимы основные операции умножения и взятие обратного, а также что эффективно задаются автоморфизмы группы G, для которых эффективно вычисляются обратные элементы. Также необходимо считать, что в группе эффективно разрешима проблема равенства.

Алиса и Боб выбирают группу G и конечно порождённую абелеву подгруппу S её группы автоморфизмов $\mathrm{Aut}(G)$.

Алгоритм.

1) Алиса выбирает (случайным образом) автоморфизм $\alpha \in S$, вычисляет и публикует элемент $\alpha(h)$ для Боба.
2) Боб выбирает случайным образом автоморфизм $\beta \in S$, вычисляет и публикует элемент $\beta(\alpha(h))$ для Алисы.
3) Алиса вычисляет элемент $\alpha^{-1}(\beta(\alpha(h))) = \beta(h)$, затем выбирает случайным образом автоморфизм $\gamma \in S$, вычисляет и публикует элемент $\gamma(\beta(h))$ для Боба.
4) Боб вычисляет элемент $\beta^{-1}(\gamma(\beta(h))) = \gamma(h)$, являющийся переданным ему ключом.

Криптоанализ.

Предположим, что можно эффективно выбрать из элементов вида $s(f)$, $s \in S$, где $f \in G$ — фиксированный элемент, конечное множество порождающих элементов $\{\lambda_i(f) : \lambda_i \in S,\ i = 1, \ldots, k\}$ подгруппы $Sf = \mathrm{gp}(sf : s \in S)$, а также эффективно записать через эти порождающие элементы любой элемент группы Sf.

Пусть $f = \beta(\alpha(h))$. Тогда можно найти выражение открытого элемента $\gamma(\beta(h)) = \beta(\gamma(h))$ в виде значения некоторого слова $u(\lambda_1(f), \ldots, \lambda_k(f))$. Вынося за значение слова u автоморфизм β и сокращая на него обе части, получим требуемое значение $\gamma(h) = u(\lambda_1(\alpha(h)), \ldots, \lambda_k(\alpha(h))$. Значит, это значение можно вычислить по слову u, автоморфизмам λ_i, $i = 1, \ldots, k$, и открытому элементу $\alpha(h)$.

2. Способы защиты от атак, использующих линейную алгебру

Данный раздел основан на работе автора [33]. Далее введено понятие множества маргинальных наборов, соответствующих выражению и значению группового слова w в группе G, существенно обобщающему понятие маргинальной подгруппы $w^*(G)$, определяемой w в G. На основе этого понятия вводится новая улучшенная версия знаменитого AAG-протокола Аншель — Аншеля — Гольдфельда [34]. Улучшенная версия, в отличие от оригинальной, оказывается защищённой относительно span-метода. Она основана на смешанной проблеме вхождения-сопряжённости, в то время как оригинальная версия базируется на трудной разрешимости проблемы поиска сопрягающего элемента.

Дадим краткое описание оригинальной версии AAG -протокола. Рассматривается группа G, для которой фиксируются открытые наборы элементов $\bar{a} = (a_1, \ldots, a_k)$ и $\bar{b} = (b_1, \ldots, b_l)$. Алиса выбирает закрытый элемент $u \in \mathrm{gp}(a_1, \ldots, a_k)$ и публикует набор $\bar{b}^u = (b_1^u, \ldots, b_l^u)$. Боб выбирает закрытый элемент $v \in \mathrm{gp}(b_1, \ldots, b_l)$ и публикует набор $\bar{a}^v = (a_1^v, \ldots, a_k^v)$. Затем каждый из корреспондентов вычисляет элемент

$$u^{-1}u(a_1^v, \ldots, a_k^v) = v(b_1^u, \ldots, b_l^u)^{-1}v = [u, v],$$

являющийся распределённым ключом.

2.1. Маргинальные множества

Определение 1. Пусть $w = w(x_1, \ldots, x_n)$ обозначает групповое слово от n переменных, G — группа и $\bar{g} = (g_1, \ldots, g_n)$ — набор её элементов. Говорим, что набор $\bar{c} = (c_1, \ldots, c_n) \in G^n$ является *маргинальным набором*, определяемым w и $\bar{g}$, если имеет место равенство

$$w(c_1 g_1, \ldots, c_n g_n) = w(g_1, \ldots, g_n).$$

Будем писать $\bar{c} \perp w(\bar{g})$ в этом случае. Множество $\bar{C} \subseteq G^n$ называется *маргинальным* по отношению к w и $\bar{g}$ ($\bar{C} \perp w(\bar{g})$), если $\bar{c} \perp w(\bar{g})$ для любого набора $\bar{c} \in \bar{C}$.

В общем случае маргинальное множество $\bar{C}$, $\bar{C} \perp w$, не является подгруппой. Оно может быть выбрано как множество без всякой структуры, в случае бесконечной группы оно может быть выбрано нерекурсивным.

Дадим простой и эффективный способ построения маргинального множества $\bar{C}$ по слову w. Этот способ универсален, так как он не зависит от структуры группы $\bar{G}$.

Пусть $w = w(a_1, \ldots, a_k) = a_1 a_2 \ldots a_k$, $a_i \in G$, $i = 1, \ldots, k$, — выражение через произведение элементов произвольного слова $f \in G$, при этом допускаются равенства $a_i = a_j$ или $a_i = a_j^{-1}$ для $i \neq j$. Выражение не обязано быть редуцированным. Рассмотрим уравнение

$$x_1 a_1 x_2 a_2 \ldots x_k a_k = f. \tag{1}$$

Любое решение этого уравнения может быть включено в маргинальное множество $\bar{C}$, $\bar{C} \perp w$. Зафиксировав какое-то i и выбрав произвольные значения $x_j = c_j$, $j \neq i$, $c_j \in G$, можно получить решение уравнения (1), полагая

$$x_i = a_{i-1}^{-1} c_{i-1}^{-1} \ldots a_1^{-1} c_1^{-1} f a_k^{-1} c_k^{-1} \ldots a_{i+1}^{-1} c_{i+1}^{-1}. \tag{2}$$

Улучшенная версия AAG-протокола

Предположим, что два корреспондента, Алиса и Боб, хотят распределить между собой ключ. Они выбирают открытую группу G, эффективно заданную порождающими элементами и определяющими соотношениями. Группа G используется как платформа

для распределения ключа. Как обычно, предполагаем, что операции в группе вычисляются эффективно и что в группе G эффективно разрешима проблема равенства.

Для распределения ключа корреспонденты действуют следующим образом.

Алиса выбирает натуральное число k и набор элементов $\bar{a} = (a_1, \ldots, a_k)$. Эти данные открыты. Затем она выбирает секретное групповое слово $u = u(x_1, \ldots, x_k)$ и вычисляет его значение $u(\bar{a}) = u(a_1, \ldots, a_k)$ в группе G. Она строит также маргинальное множество $\bar{C} \subseteq G^k$, $\bar{C} \perp u(\bar{a})$. Боб фиксирует натуральное число l и выбирает открытый набор элементов $\bar{b} = (b_1, \ldots, b_l)$. Затем он выбирает секретное слово $v = v(y_1, \ldots, y_l)$ и вычисляет его значение $v(\bar{b}) = v(b_1, \ldots, b_l)$ в группе G. Далее он строит открытое маргинальное множество $\bar{D} \subseteq G^l$, $\bar{D} \perp v(\bar{b})$. Всё это составляет установку системы для распределения секретного ключа между корреспондентами. Впрочем, она может быть измененена, как объясняется далее.

Замечание 1. Алиса публикует элементы $a_1, \ldots, a_k$ как $a_{\pi(1)}, \ldots, a_{\pi(k)}$, где $\pi \in \in \mathbb{S}_k$ — случайная подстановка. Та же самая подстановка применяется к элементам набора $\bar{c} \in \bar{C}$. Боб действует аналогичным образом.

Виртуальные и скрытые элементы. Алиса может ввести виртуальные элементы h, не задействованные в записи $u(\bar{a})$. Затем она может присоединить соответствующие виртуальные компоненты к $\bar{c} \in \bar{C}$, $\bar{C} \perp w$. Например, она может присоединить ряд виртуальных элементов и соответствующих компонент с целью скрыть длину слова u, или завуалировать уравнение (2), или выбрать элемент h с большим централизатором, или, наоборот, с малым централизатором, чтобы сделать решение проблемы более затруднительным для потенциального взломщика систем. Боб действует аналогично.

Алиса может также скрыть некоторые элементы a_i следующим образом. Пусть $a_i = a_j$ и соответствующие им компоненты любого из элементов маргинального множества равны между собой, то есть $c_i = c_j$ для всех $\bar{c} \in \bar{C}$. Тогда Алиса может не публиковать некоторые a_j, исключая соответствующие j-компоненты из $\bar{c}$. Необходимая информация восстанавливается очевидным образом. Боб может действовать аналогично.

Эти операции рекомендуются. После их выполнения параметры k и l заменяются на новые параметры k' и l'.

Алгоритм.

1) Алиса выбирает набор $\bar{d} = (d_1, \ldots, d_{l'}) \in \bar{D}$ и вычисляет $\bar{d}\bar{b} = (d_1 b_1, \ldots, d_{l'} b_{l'})$. Затем она посылает набор $\bar{d}\bar{b}^{u(\bar{a})} = ((d_1 b_1)^{u(\bar{a})}, \ldots, (d_{l'} b_{l'})^{u(\bar{a})})$ Бобу.
2) Боб выбирает набор $\bar{c} = (c_1, \ldots, c_{k'}) \in \bar{C}$ и вычисляет $\bar{c}\bar{a} = (c_1 a_1, \ldots, c_k a_k)$. Затем он посылает набор $\bar{c}\bar{a}^{v(\bar{b})} = ((c_1 a_1)^{v(\bar{b})}, \ldots, (c_{k'} a_{k'})^{v(\bar{b})})$ Алисе.
3) Алиса, используя скрытые компоненты, вычисляет значение

$$u(\bar{a})^{-1} u((c_1 a_1)^{v(\bar{b})}, \ldots, (c_k a_k)^{v(\bar{b})} = u(\bar{a})^{-1} u(c_1 a_1, \ldots, c_k a_k)^{v(\bar{b})} = [u(\bar{a}), v(\bar{b})].$$

4) Боб аналогично вычисляет

$$v((d_1 b_1)^{u(\bar{a})}, \ldots, (d_l b_l)^{u(\bar{a})})^{-1} v(\bar{b}) = (v(d_1 b_1, \ldots, d_l b_l)^{u(\bar{a})})^{-1} v(\bar{b}) = [u(\bar{a}), v(\bar{b})].$$

Коммутатор $K = [u(\bar{a}), v(\bar{b})]$ является секретным распределённым ключом.

Криптоанализ.

Определение 2. *Проблема вхождения-сопряжённости* разрешима в G по отношению к $\bar{C} \subseteq G^k$, если существует алгоритм, решающий для двух любых наборов

$\bar{a} = (a_1, \ldots, a_k)$ и $\bar{f} = (f_1, \ldots, f_k)$ элементов группы G, существует или нет элемент $y \in G$, такой, что $(f_1^y a_1^{-1}, \ldots, f_k^y a_k^{-1}) \in \bar{C}$. Короче говоря, существует ли $y \in G$, для которого $\bar{f}^y \bar{a}^{-1} \in \bar{C}$? Соответствующая проблема поиска — это вопрос о существовании алгоритма, находящего решение указанной проблемы, если такое решение существует.

Предложенная версия AAG-протокола основывается на трудной разрешимости поисковой проблемы вхождения-сопряжённости в случае, когда $\bar{C}$ — маргинальное множество, $\bar{C} \perp u(a_1, \ldots, a_k)$, для неизвестного слова $u(x_1, \ldots, x_n)$ (или аналогично, когда $\bar{D}$ — маргинальное множество, $\bar{D} \perp v(b_1, \ldots, b_l)$). В самом деле, предположим, что взломщик находит $\bar{c}' \in \bar{C}$ и $y \in G$, такие, что $\bar{c}\bar{a}^{v(\bar{b})} = \bar{c}'a^y$, и аналогично находит $\bar{d}' \in \bar{D}$ и $x \in G$, такие, что $\bar{d}\bar{b}^{u(\bar{a})} = \bar{d}'b^x$. Тогда он может вычислить распределяемый ключ $K = [x, y] = [u(\bar{a}), v(\bar{b})]$, как в оригинальной версии AAG.

Существуют также другие проблемы, которые следует решить перед тем, как пытаться взломать предложенный алгоритм. Присутствие виртуальных и скрытых элементов не позволяет вычислить длины слов u и v. Заметим, что каждое решение уравнения (1) является решением уравнения вида $a_i a_{i+1} \ldots a_k a_1 \ldots a_{i-1} = f$, $i = 2, \ldots, k$, а также ряда других уравнений. Следовательно, открытые данные не позволяют определить $f^{v(\bar{b})}$, даже если взломщик знает длину v и все буквы $v(\bar{b})$ вместе с их кратностью.

ЛИТЕРАТУРА

1. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.
2. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013.
3. *Myasnikov A. and Roman'kov V.* A linear decomposition attack // Groups, Complexity, Cryptology. 2015. V. 7. P. 81–94.
4. *Романьков В. А., Обзор А. А.* Общая алгебраическая схема распределения криптографических ключей и её криптоанализ // Прикладная дискретная математика. 2017. № 37. С. 52–61.
5. *Романьков В. А., Обзор А А.* Метод нелинейного разложения для анализа криптографических схем, использующих автоморфизмы групп // Прикладная дискретная математика. 2018. № 41. С. 38–45.
6. *Roman'kov V. A.* Essays in Algebra and Cryptology. Algebraic Cryptanalysis. Omsk: OmSU, 2018.
7. *Tsaban B.* Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography // J. Cryptology. 2015. V. 28. P. 601–622.
8. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans // CRYPTO 2018. LNCS. 2018. V. 10991. P. 1–20.
9. *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.
10. *Tsaban B.* The Conjugacy Problem: Cryptoanalytic Approaches to a Problem of Dehn. Minicourse, Dusseldorf University, Germany, July–August 2012. `http://reh.math.uni-duesseldorf.de/gagta/slides/Tsabanminicourses.pdf`.
11. *Roman'kov V.* A non-linear decomposition attack // Groups, Complexity, Cryptology. 2015. V. 8. P. 197–207.
12. *Романьков В. А.* Криптографический анализ модифицированной матричной модулярной криптосистемы // Вестник Омского ун-та. 2018. Т. 23. С. 44–50.
13. *Roman'kov V.* Two general schemes of algebraic cryptography // Groups, Complexity, Cryptology. 2018. V. 10. P. 83–98.

14. *Roman'kov V. A.* A Polynomial Time Algorithm for the Braid Double Shielded Public Key Cryptosystems. Bulletin of the Karaganda University. Mathematics Ser. 2016. No. 4(84). P. 110–115. arXiv math.:1412.5277v1 [math.GR], 17 Dec. 2014. 7 p.
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. *Романьков В. А.* Метод линейного разложения анализа протоколов скрытой информации на алгебраических платформах // Алгебра и логика. 2015. Т. 54. № 1. С. 119–128.
17. *Roman'kov V. A. and Menshov A. V.* Cryptanalysis of Andrecut's Public Key Cryptosystem. arXiv math.: 1507.01496v1 [math.GR], 6 Jul 2015, 5 p.
18. *Andrecut M.* A Matrix Public Key Cryptosystem. arXiv math.:1506.00277v1 [cs.CR], 31 May 2015. 11 p.
19. *Gu L., Wang L., Ota K., et al.* New public key cryptosystems based on non-abelian factorization problems // Security and Communication Networks. 2013. V. 6. P. 912–922.
20. *Gu L. and Zheng S.* Conjugacy systems based on nonabelian factorization problems and their applications in cryptography // J. Appl. Math. 2014. Article ID 630607. 10 p.
21. *Hurley B. and Hurley T.* Group Ring Cryptography. arXiv math.: 1104.17.24v1 [math.GR] 9 Apr 2011. 20 p.
22. *Hurley T.* Cryptographic schemes, key exchange, public key. arXiv math.: 1305.4063v1 [cs.CR] May 2013. 19 p.
23. *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.
24. *Stickel E.* A new method for exchanging secret keys // Proc. Third Intern. Conf. ICITA 05. Contemp. Math. 2005. V. 2. P. 426–430.
25. *Wang X., Xu C., Li G., et al.* Double shielded public key cryptosystems. Cryptology ePrint Archive. Report 2014/558. Version 20140718:185200, 2014. P. 1–14. `https://eprint.iacr.org/2014/558`.
26. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-Based Cryptography. Barselona, Basel: CRM, 2008 (Advances Courses in Math.).
27. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. Math. Surveys and Monographs. V. 177. Providence RI: AMS, 2011.
28. *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.
29. *Романьков В. А.* Введение в криптографию. М.: Форум, 2012.
30. *Bigelow S.* Braid groups are linear // J. Amer. Math. Soc. 2001. V. 14. P. 471–486.
31. *Krammer D.* Braid groups are linear // Ann. Math. 2002. V. 155. P. 131–156.
32. *Mahalanobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. 2008. V. 165. P. 161–187.
33. *Roman'kov V. A.* An improved version of the AAG cryptographic protocol // Groups, Complexity, Cryptology. 2019. V. 11.
34. *Anshel I., Anshel M., and Goldfeld D.* An algebraic method for public-key cryptography // Math. Res. Lett. 1999. V. 6. P. 287–291.