УДК 003.26; 004.056.55; 512.54

МЕТОД НЕЛИНЕЙНОГО РАЗЛОЖЕНИЯ ДЛЯ АНАЛИЗА КРИПТОГРАФИЧЕСКИХ СХЕМ, ИСПОЛЬЗУЮЩИХ АВТОМОРФИЗМЫ ГРУПП[1]

В. А. Романьков, А. А. Обзор

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

Показано применение метода нелинейного разложения для криптографического анализа на примере двух схем, которые используют автоморфизмы группы. При некоторых ограничениях на группу, выбранную в качестве платформы шифрования, данный метод работает эффективно и позволяет раскрывать секретную информацию (распределяемый ключ или пересылаемое сообщение) без решения алгоритмически сложных проблем, заложенных в основу схемы. Такими являются нетеровы группы, для которых эффективно решается проблема поиска вхождения элемента в заданную подгруппу. В частности, этим свойством обладают конечно порожденные нильпотентные или, более общо, полициклические группы, часто рекомендуемые в качестве платформ в современной алгебраической криптографии.

Ключевые слова: *криптография, криптоанализ, распределение ключа, нелинейное разложение, проблема поиска вхождения.*

DOI 10.17223/20710410/41/4

A NONLINEAR DECOMPOSITION METHOD IN ANALYSIS OF SOME ENCRYPTION SCHEMES USING GROUP AUTOMORPHISMS

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

Dostoevskii Omsk State University, Omsk, Russia

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

This paper shows how the nonlinear decomposition method, that had been invented by the first author, works against two cryptographic schemes based on group automorphisms. In some cases we can find the secret data and break the scheme without solving the algorithmic problem on which scheme is based. More exactly, let G be a group and A be a finitely generated subgroup of the automorphism group $\mathrm{Aut}(G)$. Suppose, that the membership search problem for G is efficiently solvable for any subgroup of the form $\langle g^A\rangle$ generated by the all images of g under automorphisms of A, and every subgroup $\langle g^A\rangle$ is finitely generated. Then there exists an efficient algorithm to construct a finite generating set of $\langle g^A\rangle$ and the nonlinear decomposition method can be applied. In particular, if the elements $g, f = g^\alpha, h = f^\beta \in G$ are public, $\alpha, \beta \in \mathrm{Aut}(G)$, $\alpha\beta = \beta\alpha$, and α, β are private, then one can efficiently compute h^α without computing α or β. The method efficiently works for a Noetherian group with efficiently solvable membership search problem. In particular, finitely generated nilpotent (more generally, polycyclic) groups, that are frequently used in the modern algebraic cryptography, share this property.

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

Keywords: *cryptography, cryptanalysis, key exchange, nonlinear decomposition, membership search problem.*

Введение

В данной работе рассматривается применение метода нелинейного разложения, предложенного первым автором в [1], на примере двух схем: схемы передачи ключа Махалонобиса [2], являющейся алгебраическим аналогом классической схемы Масси — Омуры, и алгебраического аналога классического протокола Эль-Гамаля, использующего автоморфизмы [3, 4] (относительно классических версий см., например, [5]). В отличие от метода линейного разложения, теоретические основы которого изложены в [6] (см. также [7, 8]), метод нелинейного разложения не предполагает наличия структуры векторного пространства у платформы, на которой строится схема.

В [2] А. Махалонобис предложил два протокола распределения ключа, один из которых является алгебраической версией протокола Диффи — Хеллмана, другой — алгебраической версией протокола Масси — Омуры. В качестве платформы шифрования предлагались конечно порождённые нильпотентные группы и их автоморфизмы специального вида. Оба протокола проанализированы в [6] в предположении, что используемая группа линейна. Методом линейного разложения установлено, что в этом случае протоколы уязвимы. Конечно порождённые нильпотентные группы всегда допускают точное представление матрицами, но размерность матриц может оказаться слишком большой для проведения такого анализа. Поэтому возникла потребность поиска других методов.

В [1] первым автором дан криптографический анализ первого из этих протоколов (аналога протокола Диффи — Хеллмана), показана его уязвимость. При этом не была использована детализация групп и автоморфизмов из [2]. Применён новый метод нелинейного анализа, основанный на эффективной разрешимости в группе проблемы вхождения элемента в подгруппу. Отмечено, что такая проблема эффективно разрешима в полициклических, а значит, и в конечно порождённых нильпотентных группах. В последнем классе большинство основных алгоритмических проблем разрешаются алгоритмами с низкой сложностью. Об этом говорится далее более подробно. В том числе существует алгоритм низкой сложности, решающий проблему поиска вхождения элемента в подгруппу.

В настоящей работе представлен криптографический анализ второго из протоколов работы [2] — алгебраической версии протокола Масси — Омуры. В предположениях автора протокола он оказывается уязвимым относительно анализа методом нелинейного разложения. Аналогичный анализ проведён также для алгебраической версии протокола Эль-Гамаля.

Метод нелинейного разложения используется также для криптографического анализа алгебраической версии протокола Эль-Гамаля и алгебраической версии системы MOR, предложенной в [3, 4]. Доказано, что эти версии также уязвимы.

Через $\langle g_1, \ldots, g_n \rangle$ будем обозначать подгруппу рассматриваемой группы, порождённую элементами $g_1, \ldots, g_n$. Выражение $H \leqslant G$ означает, что H — подгруппа группы G.

Напомним, что проблема поиска, соответствующая классической проблеме вхождения (поиска вхождения элемента в подгруппу), ставится следующим образом: для данной группы G, её подгруппы $H = \langle h_1, \ldots, h_k \rangle$ и заданного элемента $g \in H$ найти слово $u(x_1, \ldots, x_k)$, такое, что $g = u(h_1, \ldots, h_k)$. Если подгруппа H фиксирована, рассматриваем соответствующую проблему поиска вхождения элемента $g \in H$ в H.

Здесь и далее предполагается, что используется язык комбинаторной теории групп, в котором группы задаются своими представлениями через порождающие элементы и определяющие соотношения, элементы записываются словами от порождающих элементов. Допустимы также матричные задания групп и их подгрупп над полями, в которых основные операции эффективно выполнимы. Почти во всех известных случаях группы, предлагаемые как платформы для криптографических схем, задаются именно таким способом. Как правило, требуется наличие в группах нормальных форм записи элементов, операции над которыми также должны быть эффективными.

Пусть G — алгебраическая система (группа, полугруппа, кольцо и т. п.), $\mathrm{Aut}(G)$ — её группа автоморфизмов. Через g^α будем обозначать образ элемента $g \in G$ относительно автоморфизма $\alpha \in \mathrm{Aut}(G)$. Другими словами, $g^\alpha = \alpha(g)$. В данной работе мы ограничиваемся рассмотрением групп, но предлагаемый метод криптографического анализа при соответствующих условиях может быть применён и к произвольным алгебраическим системам.

Если A — подгруппа группы автоморфизмов $\mathrm{Aut}(G)$ группы G и $v \in G$, то $v^A = \{v^\alpha | \alpha \in A\}$ обозначает орбиту относительно A, порождённую элементом v.

1. Лемма о построении порождающего множества

Пусть G — группа, $A = \langle \alpha_1, \ldots, \alpha_n \rangle$ — подгруппа группы автоморфизмов $\mathrm{Aut}(G)$.

Лемма 1. Если в группе G эффективно разрешима проблема поиска вхождения элемента в подгруппу $\langle g^A \rangle$ и подгруппа $\langle g^A \rangle$ конечно порождена, то существует алгоритм построения её конечного порождающего множества.

Доказательство. Считаем для простоты, что множество $\{\alpha_1, \ldots, \alpha_n\}$ замкнуто относительно взятия обратных элементов. Упорядочим все конечные наборы вида $\alpha_{i_1} \ldots \alpha_{i_t}$, $t = 0, 1, \ldots$, в соответствии с длиной и лексикографическим порядком. Полученная последовательность содержит записи всех элементов множества g^A. Элемент 1 соответствует набору длины 0. Через L_i обозначим часть полученной последовательности, соответствующую наборам длины i; $M_i = g^{L_i}$ — индуцированно упорядоченный набор элементов вида g^α, $\alpha \in L_i$. Последовательность множеств M_i, $i = 0, 1, \ldots$, очевидно, содержит все элементы множества g^A, а значит, и какое-то конечное порождающее множество подгруппы $\langle g^A \rangle$.

Опишем процесс построения конечного порождающего множества. Положим $K_0 = M_0 = \{g\}$. Добавляем к K_0 по очереди элементы $g^{\alpha_j} \in M_1$, для которых $g^{\alpha_j} \notin \langle g, g^{\alpha_1}, \ldots, g^{\alpha_{j-1}} \rangle$. Другими словами, добавляем элементы, не принадлежащие подгруппе, порождённой ранее выбранными элементами. Шаг заканчивается, когда будут просмотрены все элементы из M_1. В результате получим эффективно построенное подмножество $K_1 = \{g, g^{\alpha_{l_1}}, \ldots, g^{\alpha_{l_s}} : l_1 < \ldots < l_s\}$ множества $K_0 \cup M_1$. При этом $\langle g^A \rangle = \langle K_1, \bigcup_{i=2}^{\infty} M_i \rangle$.

Если $K_0 = K_1$, то алгоритм завершает свою работу, констатируя, что $\langle g^A \rangle = \langle K_0 \rangle = \langle g \rangle$ — циклическая группа. Действительно, в этом случае подгруппа $\langle g \rangle$ очевидно инвариантна относительно любого автоморфизма α_i, $i = 1, \ldots, n$, значит, и любого автоморфизма из A.

Если $K_0 \neq K_1$, продолжаем описанный процесс, добавляя к K_1 поочередно элементы из M_2, не входящие в подгруппу, порождённую уже выбранными элементами. При этом можно сразу убрать из рассмотрения элементы вида $g^{\alpha_i \alpha_j}$, где g^{α_i} не является выбранным элементом. Это может значительно ускорить процесс. В итоге построим множество K_2, равное объединению K_1 с выбранными на этом шаге элементами из M_2.

Если ни один элемент не выбран, то $\langle g^A \rangle = \langle K_1 \rangle$. Это также следует из того, что группа $\langle K_1 \rangle$ в этом случае инвариантна относительно действия A.

Далее аналогично строим множества K_r для $r = 3, \ldots$, просматривая и поочередно добавляя элементы из соответствующего множества M_r. Заметим, что на каждом шаге $\langle g^A \rangle = \langle K_r, \bigcup\limits_{i=r+1}^{\infty} M_i \rangle$.

На каком-то шаге получим $K_t = K_{t+1}$, так как группа $\langle g^A \rangle$ по сделанному предположению конечно порождена. Тогда получаем равенство $\langle g^A \rangle = \langle K_t \rangle$. Заметим также, что если подгруппа $\langle g^A \rangle$ имеет s порождающих, то процесс обязательно закончится не позднее чем при рассмотрении K_s. Описанный процесс находит наименьшее по мощности множество порождающих элементов группы $\langle g^A \rangle$. Это позволяет в ряде случаев дать очевидную оценку сверху на число шагов алгоритма. ■

Замечание 1. Если A — коммутативная подгруппа, как далее в протоколе из [2], то рассматриваем не все конечные наборы вида $\alpha_{i_1} \ldots \alpha_{i_t}$, $t = 0, 1, \ldots$, а только те, для которых индексы не убывают.

2. Эффективность метода

Метод нелинейного разложения применим, если в группе G, используемой в качестве платформы шифрования, эффективно решается проблема поиска вхождения элемента в подгруппу, соответствующая классической проблеме вхождения, а также если можно эффективно построить порождающие множества элементов для некоторых конечно порождённых подгрупп, использующихся при шифровании. Пример такого построения указан в лемме 1.

Метод хорошо работает на ряде схем, построенных на полициклических группах, которые сейчас часто предлагаются в качестве платформ [9 – 11]. В полициклических группах любая подгруппа конечно порождена, причем количество её порождающих элементов оценивается сверху длиной полициклического ряда всей группы. Это позволяет дать верхнюю оценку времени работы алгоритма, описанного в лемме 1. В [12] показано, что основные алгоритмические проблемы (построения нормальной формы элемента, определения сопряжённости двух элементов, проблемы вхождения и др.) могут быть решены алгоритмами, работающими в логарифмическом пространстве за квазилинейное время. Более того, если рассматривать постановку проблемы в сжатом виде, причем каждое вхождение слова представлять как strait-line программу, то эти проблемы решаются за полиномиальное время. В [13] использование так называемых TC^0-схем позволило авторам понизить оценки сложности проблем. Наконец, в [14] авторы расширили список алгоритмических проблем для конечно порождённых нильпотентных групп, решаемых алгоритмами с низкой сложностью, включив в него ряд проблем для подгрупп.

3. Примеры криптографического анализа алгебраических схем с использованием метода нелинейного разложения

3.1. Пример 1

Опишем протокол распределения ключа Махалонобиса [2] — аналога классического протокола Масси — Омуры.

Пусть G — группа и $g \in G$. Предположим, что Φ и Ψ — два конечных подмножества группы автоморфизмов $\mathrm{Aut}(G)$, причём элементы из Φ попарно перестановочны с элементами из Ψ. Пусть A и B — подгруппы группы $\mathrm{Aut}(G)$, порождённые множествами Φ и Ψ соответственно.

Алгоритм распределения ключа работает следующим образом:

1) Алиса выбирает случайный автоморфизм $\alpha \in A$, вычисляет g^α и посылает результат Бобу.
2) Боб выбирает случайным образом автоморфизм $\beta \in B$, вычисляет и посылает $(g^\alpha)^\beta$ Алисе.
3) Затем Алиса вычисляет α^{-1} и получает $((g^\alpha)^\beta)^{\alpha^{-1}} = g^\beta$. После этого она выбирает еще один случайный автоморфизм $\gamma \in A$, вычисляет $(g^\beta)^\gamma$ и передаёт его Бобу.
4) Боб находит β^{-1} и получает ключ $K = ((g^\beta)^\gamma)^{\beta^{-1}} = g^\gamma$.
5) Алиса в свою очередь, зная g и γ, тоже вычисляет ключ K.

Криптографический анализ. Заметим, что в алгоритме подгруппы $A, B \leqslant \leqslant \mathrm{Aut}(G)$ конечно порождены.

Предположим, что для группы G эффективно решается проблема поиска вхождения элемента в подгруппу $\langle v^A \rangle$, где $v = (g^\alpha)^\beta$. Пусть известно, что подгруппа $\langle v^A \rangle$ s-порождена для некоторого s.

Замечание 2. В [2] в качестве платформы шифрования предлагается использовать конечно порождённую p-группу, более того, конечную p-группу специального вида. Приведённые условия криптографического анализа в этом случае выполнены. Значение оценочного параметра в оригинальном протоколе очевидно (в общем случае s не больше, чем полициклический ранг группы).

Заметим также, что выше приведён несколько более общий вариант оригинального протокола: автор брал в качестве A и B общую коммутативную подгруппу S группы автоморфизмов $\mathrm{Aut}(G)$. Мы не даём и не используем детали выбора групп и автоморфизмов из [2], так как криптоанализ от них не зависит. Детали только упрощают его реализацию.

Перейдём непосредственно к криптографическому анализу.

По лемме 1 можно эффективно найти порождающее множество элементов для группы $\langle v^A \rangle$. Обозначим эти элементы как $\langle v^{\alpha_1}, \ldots, v^{\alpha_t} \rangle$. Далее отметим, что $(g^\beta)^\gamma \in v^A$, поэтому можно найти его представление вида

$$g^{\beta\cdot\gamma} = V(v^{\alpha_1}, \ldots, v^{\alpha_t}),$$

где $V(x_1, \ldots, x_t)$ — групповое слово от t переменных. Затем в правую часть данного представления вместо $v = (g^\alpha)^\beta$ подставим $g^\alpha = (g^{\alpha\cdot\beta})^{\beta^{-1}}$. Получим

$$V((g^\alpha)^{\alpha_1}, \ldots, (g^\alpha)^{\alpha_t}) = V((v^{\beta^{-1}})^{\alpha_1}, \ldots, (v^{\beta^{-1}})^{\alpha_t}) =$$
$$= V((v^{\alpha_1})^{\beta^{-1}}, \ldots, (v^{\alpha_t})^{\beta^{-1}}) = (V(v^{\alpha_1}, \ldots, v^{\alpha_t}))^{\beta^{-1}} = g^\gamma.$$

Таким образом, не вычисляя ни один из закрытых элементов α, β и γ, можно эффективно найти распределяемый (передаваемый) секретный элемент (ключ или сообщение) g^γ. Это означает, что данная схема является уязвимой.

3.2. Пример 2

В качестве второго примера рассмотрим алгебраический аналог классического протокола Эль-Гамаля, использующий автоморфизмы. Имеется несколько алгебраических версий как самого протокола Эль-Гамаля, так и его обобщения — так называемой системы MOR, относительно которых см. [3, 4].

Алгебраическая версия системы Эль-Гамаля. Соглашения о группе G, элементе $g \in G$ и подгруппах $A, B \leqslant \mathrm{Aut}(G)$ те же, что и в предыдущем примере.

Алгоритм работает следующим образом:

1) Алиса случайным образом выбирает автоморфизм $\alpha \in A$, вычисляет элемент g^α и отправляет его Бобу.
2) Боб хочет послать сообщение m Алисе. Для этого он выбирает случайный автоморфизм $\beta \in B$ и посылает по сети сообщение $(g^\beta, m \cdot g^{\alpha\cdot\beta})$.
3) После этого Алиса вычисляет элемент $(g^\beta)^\alpha = g^{\alpha\cdot\beta}$, находит к нему обратный и получает сообщение $m = m \cdot g^{\alpha\cdot\beta}(g^{\alpha\cdot\beta})^{-1}$.

Криптографический анализ. Пусть для группы G эффективно решается проблема поиска вхождения элемента в подгруппу $\langle g^A\rangle$. Тогда по лемме 1, аналогично примеру 1, найдём порождающее множество для группы $\langle g^A\rangle$, скажем, $\{g^{\alpha_1}, \ldots, g^{\alpha_k}\}$. Из того, что Алиса выбирала автоморфизм $\alpha \in A$, следует, что $g^\alpha \in g^A$, а значит, можно найти представление этого элемента через порождающие:

$$g^\alpha = V(g^{\alpha_1}, \ldots, g^{\alpha_k}).$$

Заменив в правой части g на g^β, получим

$$V((g^\beta)^{\alpha_1}, \ldots, (g^\beta)^{\alpha_k}) = V((g^{\alpha_1})^\beta, \ldots, (g^{\alpha_k})^\beta) = (V(g^{\alpha_1}, \ldots, g^{\alpha_k}))^\beta = g^{\alpha\cdot\beta}.$$

Далее, действуя аналогично Алисе, вычисляем обратный элемент к $g^{\alpha\cdot\beta}$ и расшифровываем сообщение $m = m \cdot g^{\alpha\cdot\beta}(g^{\alpha\cdot\beta})^{-1}$.

Алгебраическая версия системы MOR. Пусть $G = \langle g_1, \ldots, g_n\rangle$ — конечно порождённая группа. Алгоритм распределения ключа работает следующим образом:

1) Алиса выбирает случайный автоморфизм $\varphi \in \mathrm{Aut}(G)$ и случайное натуральное число k, вычисляет значения g_i^φ и $g_i^{\varphi^k}$ для $i = 1, \ldots, n$, которые считаются открытыми. Другими словами, Алиса объявляет открытыми автоморфизмы φ и φ^k. При этом k — закрытый параметр.
2) Боб хочет послать Алисе сообщение m, закодированное как элемент группы G. Для этого Боб выбирает случайное натуральное число l, вычисляет и посылает Алисе набор значений $g_i^{\varphi^l}$ для $i = 1, \ldots, n$, а также элемент $m^{\varphi^{kl}}$. Другими словами, Боб посылает Алисе пару $(\varphi^k, m^{\varphi^{kl}})$.
3) Затем Алиса, зная k, вычисляет $(\varphi^{kl})^{-1}$ и раскрывает сообщение m, подействовав этим автоморфизмом на $m^{\varphi^{kl}}$.

Криптографический анализ. Повторяем рассуждения предыдущего криптографического анализа, позволяющие вычислить по значениям $g_i^{\varphi^k}$ и $g_i^{\varphi^l}$ значение $g_i^{\varphi^{kl}}$ для любого $i = 1, \ldots, n$. Тем самым мы найдём автоморфизм φ^{kl}, вычислим к нему обратный, а затем по элементу $m^{\varphi^{kl}}$ получим сообщение m.

Замечание 3. Для эффективности алгоритма проведённого криптографического анализа необходимо уметь решать проблему поиска вхождения элемента в подгруппу. В [3] в качестве платформы предложено выбирать группу унитреугольных матриц над конечным полем (конечную нильпотентную p-группу, где p — характеристика поля), в которой эта проблема решается легко. В [4] предлагается брать специальную линейную группу над конечным полем, которая, очевидно, сама конечна. Вопрос о сложности алгоритма, решающего в такой группе проблему вхождения элемента в подгруппу, как и вопрос об эффективности построения порождающего множества для подгруппы ещё должен быть изучен. Заметим, что при том и другом предложении для

криптоанализа лучше использовать метод линейного разложения, уже неоднократно упомянутый в данной работе.

Заключение

В работе показано, как метод нелинейного разложения может быть эффективно применен для криптографического анализа ряда схем алгебраической криптографии, использующих автоморфизмы, в частности, для алгебраических аналогов схем Масси — Омуры, Эль-Гамаля и системы MOR. Для его реализации необходимо и достаточно, чтобы в группе, выбранной в качестве платформы шифрования, эффективно решалась проблема вхождения элемента в подгруппу определённого вида, а также можно было бы эффективно построить систему порождающих элементов такой подгруппы. Объяснено, что конечно порождённые и полициклические группы, часто предлагаемые в качестве платформ в современной алгебраической криптографии (в том числе в приведённых в работе примерах криптографического анализа), удовлетворяют этим условиям. Алгоритм построения системы порождающих элементов для таких групп описан в работе.

Выводы. Приведённый криптографический анализ позволяет заключить, что рассматриваемые схемы при определённых естественных и часто предлагаемых условиях оказываются уязвимыми, следовательно, они не могут считаться надёжными.

ЛИТЕРАТУРА

1. *Roman'kov V. A.* A nonlinear decomposition attack // Groups Complexity Cryptology. 2017. V. 8. P. 197–207.
2. *Mahalanobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. 2008. V. 165. P. 161–187.
3. *Mahalanobis A.* A simple generalization of El-Gamal cryptosystem to non-abelian groups // Communications in Algebra. 2008. V. 36. P. 3878–3889.
4. *Mahalanobis A.* A simple generalization of El-Gamal cryptosystem to non-abelian groups II // Communications in Algebra. 2012. V. 40. P. 171–186.
5. *Романьков В. А.* Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.
6. *Романьков В. А.* Алгебраическая криптография. Омск: Изд-во ОмГУ, 2013. 135 с.
7. *Романьков В. А.* Криптографический анализ некоторых известных схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.
8. *Myasnikov A. G. and Roman'kov V. A.* A linear decomposition attack // Groups Complexity Cryptology. 2015. V. 7. P. 81–94.
9. *Eick B. and Kahrobaei D.* Polycyclic groups: A new platform for cryptology? arXiv math.: 0411.077v1 [math.GR].
10. *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.
11. *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. P. 1–14.
12. *Macdonald J., Miasnikov A., Nikolaev A., and Vassileva S.* Logspace and compressed-word computations in nilpotentgroups. arXiv math.:1503.03888 [math.GR]. 2015.
13. *Macdonald J., Miasnikov A., and Ovchinnikov D.* Low-complexity computations for nilpotent subgroup theorem. arXiv math.: 1706.01092v2 [math. GR] 4 Jul 2017. 23 p.
14. *Miasnikov A. and Weiβ A.* TC^0 circuits for algorithmic problems in nilpotent groups // 42nd Intern. Symp. MFCS. 2017. Article No. 23.

REFERENCES

1. *Roman'kov V. A.* A nonlinear decomposition attack. Groups Complexity Cryptology, 2017, vol. 8, pp. 197–207.
2. *Mahalonobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups. Israel J. Math., 2008, vol. 165, pp. 161–187.
3. *Mahalanobis A.* A simple generalization of El-Gamal cryptosystem to non-abelian groups. Communications in Algebra, 2008, vol. 36, pp. 3878–3889.
4. *Mahalanobis A.* A simple generalization of El-Gamal cryptosystem to non-abelian groups II. Communications in Algebra, 2012, vol. 40, pp. 171–186.
5. *Roman'kov V. A.* Vvedenie v kriptografiyu. Kurs lektsiy [Introduction to Cryptography. Lecture Course]. Moscow, Forum Publ., 2012. 240 p. (in Russian)
6. *Roman'kov V. A.* Algebraicheskaya kriptografiya [Algebraic Cryptography]. Omsk, Dostoevsky Omsk State University Publ., 2013. 135 p. (in Russian)
7. *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)
8. *Myasnikov A. G. and Roman'kov V. A.* A linear decomposition attack. Groups Complexity Cryptology, 2015, vol. 7, pp. 81–94.
9. *Eick B. and Kahrobaei D.* Polycyclic groups: A new platform for cryptology? arXiv math.: 0411.077v1 [math.GR].
10. *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.
11. *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, pp. 1–14.
12. *Macdonald J., Miasnikov A., Nikolaev A., and Vassileva S.* Logspace and compressed-word computations in nilpotentgroups. arXiv math.:1503.03888 [math.GR], 2015.
13. *Macdonald J., Miasnikov A., and Ovchinnikov D.* Low-complexity computations for nilpotent subgroup theorem. arXiv math.: 1706.01092v2 [math. GR], 4 Jul 2017. 23 p.
14. *Miasnikov A. and Weiβ A.* TC^0 circuits for algorithmic problems in nilpotent groups. 42nd Intern. Symp. MFCS, 2017. Article no. 23.