МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.54

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ ПРОТОКОЛА АУТЕНТИФИКАЦИИ УШАКОВА — ШПИЛЬРАЙНА, ОСНОВАННОГО НА ПРОБЛЕМЕ БИНАРНО СКРУЧЕННОЙ СОПРЯЖЁННОСТИ[1]

М. Н. Горнова, Е. Г. Кукина, В. А. Романьков

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

Приводится криптографический анализ протокола аутентификации Ушакова — Шпильрайна, базирующегося на проблеме бинарно скрученной сопряжённости относительно пары эндоморфизмов полугруппы 2×2-матриц над кольцом срезанных многочленов с коэффициентами из поля $\mathbb{F}_2$. Показано, что закрытый ключ протокола может быть вычислен путём решения системы линейных уравнений над полем $\mathbb{F}_2$. Представлена теоретическая оценка сложности алгоритма данного криптографического анализа и дано краткое описание практических результатов, полученных с помощью подготовленной программы. Анализ показывает, что рассматриваемый протокол аутентификации является теоретически и практически нестойким.

Ключевые слова: *криптография, аутентификация, эндоморфизм, скрученная сопряжённость, срезанные многочлены.*

DOI 10.17223/20710410/28/5

CRYPTANALYSIS OF USHAKOV — SHPILRAIN'S AUTHENTICATION PROTOCOL BASED ON THE TWISTED CONJUGACY PROBLEM

M. N. Gornova, E. G. Kukina, V. A. Romankov

Omsk State University, Omsk, Russia

E-mail: romankov48@mail.ru

We give a cryptanalysis of Ushakov — Shpilrain's authentication protocol based on the twisted conjugacy problem for a pair of endomorphisms on the semigroup of all 2×2 matrices over the ring of truncated one-variable polynomials over the field $\mathbb{F}_2$. It is shown that the private key of the protocol can be computed by solving the system of linear equations over $\mathbb{F}_2$. We present a theoretical estimation for the complexity of this cryptanalysis and describe practical results obtained in a computer experiment. It is shown that the protocol is theoretically and practically vulnerable.

Keywords: *cryptography, authentication, endomorphism, twisted conjugacy, truncated polynomials.*

[1]Работа выполнена при финансовой поддержке РФФИ, проекты № 13.01.00239-а и Р. Сибирь 15-41-04312-а.

Введение

В современной алгебраической криптографии примитивы, схемы, протоколы и системы строятся на алгебраических структурах (платформах). Наиболее развита в этом смысле криптография на бесконечных группах (см. работы [1, 2]). Предположения секретности при этом, как правило, базируются на трудноразрешимых и неразрешимых алгоритмических проблемах. Среди последних чаще всего фигурирует проблема сопряжённости, но встречаются также схемы, использующие проблемы равенства, вхождения и т. п. Анализ таких схем ведётся с точки зрения теории сложности. При этом кроме классического понятия «сложности в худшем случае» используются понятия «сложности в среднем» и «генерической сложности» [1 – 4].

В настоящей работе рассматривается протокол аутентификации из [5], для которого в качестве платформы предлагается использовать полугруппу 2×2-матриц над срезанными многочленами от одной переменной над полем $\mathbb{F}_2$, состоящим из двух элементов. В качестве базовой трудноразрешимой проблемы фигурирует проблема бинарно скрученной сопряжённости. Перейдём к определениям.

Пусть G — (полу)группа, ψ — её эндоморфизм. Говорят, что элементы $u, v \in G$ *скрученно сопряжены* относительно ψ, или, более кратко, ψ-*сопряжены*, если существует элемент $s \in G$, такой, что выполняется равенство

$$\psi(s)u = vs.$$

Легко проверить, что свойство *быть* ψ-*сопряжёнными* является отношением эквивалентности на основном множестве G. Понятие скрученной сопряжённости в случае, когда G — группа, обобщает понятие сопряжённости, соответствующее тождественному эндоморфизму $\psi = id$. Его появление в начале XX столетия мотивировано топологической теорией фиксированных точек отображений Нильсена — Райдемайстера. Впоследствии это понятие нашло применение в различных областях математики: теории представлений бесконечных групп, теории динамических систем, алгебраической геометрии и т. п. Свойство скрученной сопряжённости интересно и с чисто алгебраической точки зрения (см. по этому поводу работы [6 – 11]). Имеются попытки использовать понятие скрученной сопряжённости для алгебраических приложений. Рассмотрим одну из таких попыток [5], в которой фигурирует даже более общее понятие бинарно скрученной сопряжённости.

Пусть G — (полу)группа, ψ, φ — её эндоморфизмы. Говорят, что элементы $u, v \in G$ *скрученно сопряжены* относительно ψ, φ, или, более кратко, ψ-,φ-*сопряжены*, если существует элемент $s \in G$, такой, что выполняется равенство

$$\psi(s)u = v\varphi(s).$$

Свойство *быть* ψ-,φ-*сопряжёнными* также является отношением эквивалентности на основном множестве G. Понятие бинарно скрученной сопряжённости обобщает понятие скрученной сопряжённости, в котором энодоморфизм ψ произвольный, а φ — тождественный.

Говорят, что в G разрешима *проблема скрученной сопряжённости*, если существует алгоритм, определяющий для любого эндоморфизма ψ и любой пары элементов u, v из G, является ли элемент u ψ-сопряжённым элементу v. Аналогично определяется *проблема бинарно скрученной сопряжённости*. В [8] установлена разрешимость проблемы скрученной сопряжённости в произвольной полициклической группе P относительно любого её эндоморфизма ψ. В [9] доказана разрешимость проблемы скрученной сопряжённости в произвольной конечно порождённой метабелевой группе M

относительно любого её эндоморфизма ψ, тождественного по модулю коммутанта M' группы M. Конечно, существуют группы, в которых указанные проблемы алгоритмически неразрешимы. Например, такова конечно определённая группа с неразрешимой классической проблемой сопряжённости. Относительно примеров таких групп см., например, [12, 13].

В криптографии на бесконечных группах предположения секретности обычно связывают с *поисковой* алгоритмической проблемой. Например, известно, что два элемента u, v сопряжены в группе G. Требуется найти (хотя бы один) сопрягающий элемент $f \in G$, такой, что $fuf^{-1} = v$. Если проблема сопряжённости в группе G алгоритмически неразрешима, то время решения соответствующей проблемы поисковой сопряжённости не может быть ограничено сверху никакой рекурсивной функцией от параметров проблемы. Например, если на группе заданы длины элементов, то мы не можем ограничить сверху минимальную длину сопрягающего элемента f рекурсивной функцией от длин элементов u и v. Обычно в качестве длины выступает длина кратчайшего группового слова от фиксированного конечного множества порождающих элементов группы G, представляющего данный элемент. Считается, что трудноразрешимым алгоритмическим проблемам для данной группы соответствуют трудноразрешимые поисковые алгоритмические проблемы. Нахождение и интерпретация таких проблем и соответствующих групп является одной из основных проблем криптографии на бесконечных группах. В этой связи следует заметить, что в [4, 14] приведены многочисленные примеры раскрытия передаваемых секретных сообщений без вычисления закрытых ключей шифрования, т. е. без решения поисковых алгоритмических проблем, на трудности решения которых базируются предположения секретности. Это заставляет пересмотреть общее мнение о построении систем такого вида. Дальнейший криптографический анализ, основанный на разработанном в [4] методе линейного разложения, можно найти в [15 – 17].

В [5] в качестве платформы для построения протокола аутентификации предлагается использовать полугруппу 2×2-матриц над кольцом K_n n-срезанных многочленов от одной переменной x с коэффициентами из поля $\mathbb{F}_2$. Здесь n — натуральное число. Более точно, $K_n = \mathbb{F}_2[x]/I_n$ означает фактор-кольцо кольца многочленов $\mathbb{F}_2[x]$ по идеалу $I_n = \mathrm{ideal}(x^n)$, порождённому элементом x^n. Произвольный элемент $f(x)$ кольца K_n однозначно записывается в виде $a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$, где $a_i \in \mathbb{F}_2$. При этом a_0 называется *свободным членом* данного многочлена. Здесь и в дальнейшем мы опускаем слово n-срезанный. Сложение таких нормальных форм обычное, умножение отличается от обычного тем, что все степени x^k при $k \geqslant n$ равны нулю в K_n, поэтому они не фигурируют в нормальной форме.

1. Протокол аутентификации Ушакова — Шпильрайна

Приведём описание протокола аутентификации Ушакова — Шпильрайна из [5]. Заметим, что в указанной работе приведена общая версия протокола, в которой фигурирует антиэндоморфизм полугруппы. Один из основных частных случаев связан с выбором в качестве такого антиэндоморфизма операции взятия обратного элемента; мы рассматриваем и анализируем именно эту версию протокола.

Подобно классической схеме Фиата — Шамира, предполагается k-кратное повторение раундов при одной сессии аутентификации. В каждом из этих раундов вероятность правильного прохождения при незнании секретного ключа равна $1/2$. Значит, вероятность прохождения при незнании секретного ключа в k последовательных раундах не больше $(1/2)^k$.

Перейдём к описанию протокола. Предположим, что один из корреспондентов (Алиса) доказывает своё право на аутентификацию, а другой (Боб) осуществляет проверку её права на аутентификацию. При этом они открыто договариваются о выборе полугруппы G в качестве платформы для протокола аутентификации и двух эндоморфизмов ψ и φ полугруппы G, участвующих в установке этого протокола.

В процессе установки Алиса выбирает в качестве закрытого ключа обратимый элемент s полугруппы G. Затем она выбирает элемент $w \in G$ и вычисляет $t = \psi(s^{-1})w\varphi(s)$. Открытым ключом Алисы служит пара (t, w).

Каждый раунд аутентификации описывается следующим образом:

1) При очередной сессии аутентификации Алиса выбирает сессионный закрытый ключ r, с помощью которого она вычисляет $u = \psi(r^{-1})t\varphi(r)$, после чего посылает u Бобу.
2) Боб выбирает с вероятностью $1/2$ один из битов $b = 0$ или $b = 1$ и посылает его Алисе.
3) Если Алиса получает $b = 0$, она должна отправить Бобу сессионный ключ $v = r$. При его получении Боб проверяет выполнимость равенства $u = \psi(v^{-1})t\varphi(v)$. Условием прохождения раунда является справедливость этого равенства.
   Если Алиса получает $b = 1$, она должна вычислить и отправить Бобу элемент $v = sr$. При его получении Боб проверяет выполнимость равенства $u = \psi(v^{-1})w\varphi(v)$. Условием прохождения раунда является справедливость этого равенства.

Непосредственно проверяется, что при правильном элементе v указанные равенства действительно справедливы. В то же время любой, кто захочет выдать себя за Алису, сможет это сделать в случае, если угадает значение ответного бита Боба.

Действительно, если он угадает ответ $b = 0$, то ему достаточно выбрать произвольный ключ r, а затем вычислить и передать элемент $u = \psi(r^{-1})t\varphi(r)$. При угаданном ответе $b = 0$ передаётся $v = r$. Но если ответ $b = 1$, необходимо передать элемент $v = rs$, что равносильно раскрытию закрытого ключа s.

Если обманщик угадает ответ $b = 1$, он также может успешно завершить данный раунд процесса аутентификации. Для этого он должен выбрать любой элемент $z \in G$, вычислить и передать Бобу элемент $u = \psi(z^{-1})w\varphi(z)$. При ответе $b = 1$ он просто отправляет Бобу элемент $v = z$ и таким образом проходит проверку. Но при ответе $b = 0$ ему для прохождения проверки нужно передать такой элемент v, что выполнено равенство $u = \psi(v^{-1})t\varphi(v)$. Подходит элемент $v = s^{-1}z$, знание которого позволяет раскрыть s.

Криптостойкость приведённого протокола обеспечивается трудноразрешимостью проблемы бинарно скрученной сопряжённости в выбранной полугруппе G. Действительно, если кому-либо удалось бы найти по элементам t и w закрытый ключ s, то таким образом был бы раскрыт весь протокол. Если по элементам u и t удалось бы вычислить сессионный ключ r, то при ответе $b = 1$ также удалось бы вычислить закрытый ключ s.

Заметим, что достаточно было бы вычислить такой элемент s', для которого выполнено равенство $t = \psi((s')^{-1})w\varphi(s')$. С помощью s' так же можно проходить аутентификацию, как и с оригинальным закрытым ключом s. Если вычислить элемент $r' \in G$, такой, что $\psi((r')^{-1})t\varphi(r') = u$, то можно, зная sr, определить элемент $s' = (sr)(r')^{-1}$.

Тогда

$$\psi((s')^{-1})w\varphi(s') = \psi(r'r^{-1})(\psi(s^{-1})w\varphi(s))\varphi(r(r')^{-1}) =$$
$$= \psi(r')(\psi(r^{-1})t\varphi(r))\varphi((r')^{-1}) = \psi(r')u\varphi((r')^{-1}) = t.$$

Таким образом, s' также играет роль закрытого ключа s. Вычислить s' можно, наблюдая передаваемый Алисой элемент $v = sr$ при ответе Боба $b = 1$.

В [5] в качестве платформы протокола предлагается использовать полугруппу G всех 2×2-матриц над кольцом срезанных многочленов K_n, где n — число порядка 300. Любое отображение $\phi : K_n \to K_n$, для которого $\phi(x) = h$, где $h = h(x)$ — многочлен с нулевым свободным членом, однозначно продолжается до эндоморфизма кольца K_n, рассматриваемого как алгебра над $\mathbb{F}_2$. Обозначим такой эндоморфизм через ϕ_h. Действительно, $\mathbb{F}_2[x]$ — свободная коммутативная ассоциативная алгебра над $\mathbb{F}_2$ размерности один со свободным порождающим x. Поэтому любое отображение $x \mapsto h$, где h — произвольный многочлен из $\mathbb{F}_2[x]$, однозначно продолжается до её эндоморфизма. Если h — многочлен с нулевым свободным членом, то идеал I_n инвариантен относительно этого эндоморфизма. В этом случае данный эндоморфизм индуцирует эндоморфизм ϕ_h кольца K_n. Любой эндоморфизм кольца K_n естественным образом распространяется на полугруппу G, действуя соответствующим образом на элементы матриц. В [5] в качестве фигурирующих в протоколе аутентификации φ и ψ предлагается выбирать соответствующие распространения на G эндоморфизмов кольца K_n вида ϕ_h, где $h \in K_n$ имеет нулевой свободный член. Для этих распространений сохраняются обозначения ϕ_h.

Параметр n определяет размер ключевого пространства для закрытых ключей. При $n = 300$ имеется 2^{300} многочленов степени $\leqslant 300$ над $\mathbb{F}_2$, следовательно, полугруппа G содержит 2^{1200} элементов, что также является размером ключевого пространства. В то же время вычисления в кольце K_n эффективны [18]. Сложение $p(x) + q(x)$ элементов $p(x), q(x) \in K_n$ осуществляется за время $\mathrm{O}(n)$, умножение $p(x)q(x)$ — за время $\mathrm{O}(n \log_2 n)$, композиция $p(q(x))$ — за время $\mathrm{O}(n \log_2 n)$. Отюда получаем оценку времени работы одного раунда алгоритма протокола, которая определяется как $\mathrm{O}(n \log_2 n)^{3/2}$.

Открытыми ключами системы служат пары эндоморфизмов кольца K_n указанного вида. Всего таких пар эндоморфизмов при произвольном параметре $2^{2(n-1)}$. Для $n = 300$ их 2^{598}.

2. Криптографический анализ протокола аутентификации Ушакова — Шпильрайна

Рассмотрим уравнение

$$t = \psi(s^{-1})w\varphi(s), \tag{1}$$

в котором неизвестной является матрица $s = (s(ij))$, $s(ij) \in K_n$, $i, j = 1, 2$. Считаем, как это предлагается авторами протокола в [5], что каждый из эндоморфизмов ψ и φ имеет вид ϕ_h для соответствующих многочленов без свободных членов $h \in K_n$, как это объяснено выше. Умножим уравнение (1) слева на $\psi(s)$. В результате получим равносильное уравнение

$$\psi(s)t = w\varphi(s). \tag{2}$$

Запишем элементы матрицы s в нормальной форме с неопределёнными коэффициентами из поля $\mathbb{F}_2$:

$$s(ij) = s(ij)_0 + s(ij)_1 x + \ldots + s(ij)_{n-1} x^{n-1}.$$

Применив к матрице s эндоморфизмы φ и ψ, получим из уравнения (2) равносильную ему систему линейных уравнений от $4n$ переменных $s(ij)_l$ $(i,j = 1,2;$ $l = 0,1,\ldots,n-1)$ над полем $\mathbb{F}_2$. Остаётся найти такое решение данной системы линейных уравнений, для которого соответствующая ему матрица s обратима. Значительно облегчает эту задачу то обстоятельство, что матрица s обратима тогда и только тогда, когда обратима матрица s_1 свободных членов её элементов, являющаяся образом s относительно гомоморфизма специализации, при котором x отображается в ноль. Действительно, имеется всего шесть обратимых 2×2-матриц над $\mathbb{F}_2$. Следовательно, достаточно рассмотреть шесть различных случаев и хотя бы в одном из них найти обратимое решение s. Каждая частная задача при этом имеет $r = 4(n-1)$ переменных.

3. Алгоритм дешифрования протокола аутентификации Ушакова — Шпильрайна

На входе алгоритма имеем два элемента t и w из полугруппы G матриц размера 2×2 над кольцом K_n, а также два эндоморфизма ψ и φ, имеющие вид ϕ_h, предложенный в протоколе Ушакова — Шпильрайна. Их можно считать эндоморфизмами линейного пространства всей алгебры матриц. Известно, что элементы t и w ψ-,φ-сопряжены, но мы не знаем сопрягающий элемент s. Наша задача — найти любой обратимый элемент s, такой, что $\psi(s)t - w\varphi(s) = 0$. Преобразование $s \mapsto \psi(s)t - w\varphi(s)$ является линейным. Все элементы s, переходящие в ноль (ядро преобразования) образуют подпространство, базис которого находится алгоритмом Гаусса.

Ш а г 1. Получение системы линейных уравнений (СЛУ).

Рассмотрим линейное преобразование $\psi(s)t-w\varphi(s)$ в каждом из шести случаев, отвечающих различным обратимым матрицам специализации s_1, о чём говорилось выше. Каждый такой случай соответствует выбору свободных членов элементов матрицы s. Строим матрицу этого линейного преобразования, выбрав естественный базис полугруппы G. Матрице соответствует СЛУ, состоящая из $4(n-1)$ уравнений от $4(n-1)$ неизвестных. Хорошо известно, что число операций над элементами любого поля для решения такой системы оценивается как $\mathrm{O}(4^3(n-1)^3) \sim \mathrm{O}(n^3)$.

Ш а г 2. Нахождение решения s.

Полученные в шести случаях СЛУ решаем методом Гаусса. По условию хотя бы в одном из этих случаев СЛУ имеет решение. Ему соответствует искомая обратимая матрица s.

Ш а г 3. Проверка.

Считаем s^{-1} и затем $t' = \varphi(s^{-1})w\psi(s)$. Сравниваем t' с t.

Как уже отмечалось, число операций над элементами поля для решения каждой из рассматриваемых СЛУ оценивается как $\mathrm{O}(4^3(n-1)^3) \sim \mathrm{O}(n^3)$. Для получения общей оценки сложности следует учесть сложность элементарных операций в поле $\mathbb{F}_2$. Заметим, что возникающие СЛУ имеют специальный вид, при котором неизвестные коэффициенты при больших степенях переменной x в K_n не участвуют (присутствуют с нулевыми коэффициентами) в уравнениях, соответствующих меньшим степеням переменной x. Система, таким образом, имеет ступенчатый вид, значит, соответствующие вычисления упрощаются.

В соответствии с полученным алгоритмом написана программа на языке Java. Программа запускалась на оборудовании с двухъядерным процессором частоты 2,6 ГГц и 8 Гб оперативной памяти.

Для степени срезанных многочленов порядка 300 программа работает в среднем 7 мин 40 с, причём это время можно сократить, если оптимизировать некоторые шаги и запустить её на более мощном оборудовании.

ЛИТЕРАТУРА

1. *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.
2. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative Cryptography and Complexity of Group-Theoretic Problems. Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2011. 385 p.
3. *Романьков В. А.* Диофантова криптография на бесконечных группах // Прикладная дискретная математика. 2012. № 2(16). С. 15–42.
4. *Романьков В. А.* Алгебраическая криптография. Омск: ОмГУ, 2013. 135 с.
5. *Shpilrain V. and Ushakov A.* An authentication scheme based on the twisted conjugacy problem // ACNS'2008. LNCS. 2008. V. 5037. P. 366–372.
6. *Fel'shtyn A. and Troitsky E.* Twisted Burnside — Frobenius theory for discrete groups // J. Reine Angew. Math. 2007. V. 613. P. 193–210.
7. *Goncalves D. and Wong P.* Twisted conjugacy classes in nilpotent groups // J. Reine Angew. Math. 2009. V. 633. P. 11–27.
8. *Roman'kov V.* The twisted conjugacy problem in polycyclic groups // J. Group Theory. 2010. V. 13. No. 3. P. 353–364.
9. *Вентура Э., Романьков В. А.* Проблема скрученной сопряжённости для эндоморфизмов метабелевых групп // Алгебра и логика. 2009. Т. 48. № 2. С. 157–173.
10. *Roman'kov V.* Twisted conjugacy classes in nilpotent groups // J. Pure Appl. Algebra. 2011. V. 215. No. 4. P. 664–671.
11. *Fel'shtyn A. and Goncalves D. L.* Reidemeister spectrum for metabelian groups // Int. J. Algebra Comput. 2011. V. 21. No. 3. P. 1–16.
12. *Ремесленников В. Н., Романьков В. А.* Теоретико-модельные и алгоритмические проблемы теории групп // Итоги науки и техн. Сер. Алгебра. Геометрия. Топология. Т. 21. М.: ВИНИТИ, 1983. С. 3–79.
13. *Miller C. F.* Decision problems for groups: survey and reflections // Algorithms and Classification in Combinatorial Group Theory /eds. G. Baumslag and C. F. Miller III. MSRI Publications, 1992. V. 23. P. 1–59.
14. *Романьков В. А.* Криптографический анализ некоторых схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 36–51.
15. *Roman'kov V. and Myasnikov A.* A linear decomposition attack. `arXiv:1412.6401v1[math.GR]`. 19 Dec. 2014.
16. *Roman'kov V.* A polynomial time algorithm for the braid double shielded public key cryptosystem. `arXiv:1412.5277v1[math.GR]`. 17 Dec. 2014.
17. *Roman'kov V.* Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups. `arXiv:1501.0052v1[cs.CR]`. 15 Jan. 2015.
18. *Bürgisser P., Clausen M., and Shokrollalu M. A.* Algebraic Complexity Theory. Berlin: Springer, 1997.

REFERENCES

1. *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.

2. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative Cryptography and Complexity of Group-Theoretic Problems. Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2011. 385 p.
3. *Roman'kov V A.* Diofantova kriptografiya na beskonechnykh gruppakh [Diophantine cryptography over infinite groups.] Prikladnaya Diskretnaya Matematika, 2012, no. 2(16), pp. 15–42. (in Russian)
4. *Roman'kov V. A.* Algebraicheskaya kriptografiya [Algebraic Cryptography]. Omsk: OmSU Publ., 2013. 135 p. (in Russian)
5. *Shpilrain V. and Ushakov A.* An authentication scheme based on the twisted conjugacy problem. ACNS'2008. LNCS, 2008, vol. 5037, pp. 366–372.
6. *Fel'shtyn A. and Troitsky E.* Twisted Burnside — Frobenius theory for discrete groups. J. Reine Angew. Math., 2007, vol. 613, pp. 193–210.
7. *Goncalves D. and Wong P.* Twisted conjugacy classes in nilpotent groups. J. Reine Angew. Math., 2009, vol. 633, pp. 11–27.
8. *Roman'kov V.* The twisted conjugacy problem in polycyclic groups. J. Group Theory, 2010, vol. 13, no. 3, pp. 353–364.
9. *Ventura E. and Roman'kov V. A.* The twisted conjugacy problem for endomorphisms of metabelian groups. Algebra and Logic, 2009, vol. 48, iss. 2, pp. 89–98.
10. *Roman'kov V.* Twisted conjugacy classes in nilpotent groups. J. Pure Appl. Algebra, 2011, vol. 215, no. 4, pp. 664–671.
11. *Fel'shtyn A. and Goncalves D. L.* Reidemeister spectrum for metabelian groups. Int. J. Algebra Comput., 2011, vol. 21, no. 3, pp. 1–16.
12. *Remeslennikov V N., Roman'kov V. A.* Teoretiko-model'nye i algoritmicheskie problemy teorii grupp [Model-theoretic and algorithmic problems in group theory]. Itogi Nauki i Tekhn. Ser. Algebra. Geometriya. Topologiya, vol. 21. Moscow, VINITI Publ., 1983. pp. 3–79. (in Russian)
13. *Miller C. F.* Decision problems for groups: survey and reflections. Algorithms and Classification in Combinatorial Group Theory (eds. G. Baumslag and C. F. Miller III). MSRI Publications, 1992, vol. 23, pp. 1–59.
14. *Roman'kov V A.* Kriptograficheskiy analiz nekotorykh skhem shifrovaniya, ispol'zuyushchikh avtomorfizmy [Cryptanalysis of some schemes applying automorphisms]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 36–51. (in Russian)
15. *Roman'kov V. and Myasnikov A.* A linear decomposition attack. `arXiv:1412.6401v1[math.GR]`. 19 Dec. 2014.
16. *Roman'kov V.* A polynomial time algorithm for the braid double shielded public key cryptosystem. `arXiv:1412.5277v1[math.GR]`. 17 Dec. 2014.
17. *Roman'kov V.* Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups. `arXiv:1501.0052v1[cs.CR]`. 15 Jan. 2015.
18. *Bürgisser P., Clausen M., and Shokrollalu M. A.* Algebraic Complexity Theory. Berlin, Springer, 1997.