Криптографические алгоритмы на группах и алгебрах

А. С. КУЗЬМИН
Академия криптографии Российской Федерации

В. Т. МАРКОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vtmarkov@yandex.ru

А. А. МИХАЛЁВ
Московский государственный университет им. М. В. Ломоносова

А. В. МИХАЛЁВ
Московский государственный университет им. М. В. Ломоносова

А. А. НЕЧАЕВ

УДК 512.624.95+512.552.12+512.8

Ключевые слова: теория кодирования, криптография, алгебраические структуры, ассоциативные алгебры, спрятанные матрицы, алгоритмы факторизации алгебр.

Аннотация

В статье проводится анализ алгоритмов открытого построения ключа на некоммутативной группе. Рассмотрены алгоритмы факторизации и разложения ассоциативных алгебр (малой размерности). Дан обзор приложений (в том числе в криптографии) так называемых «спрятанных матриц».

Abstract

A. S. Kuzmin, V. T. Markov, A. A. Mikhalev, A. V. Mikhalev, A. A. Nechaev, Cryptographic algorithms on groups and algebras, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 205—222.

We analyze algorithms for open construction of a key on some noncommutative group. Algorithms of factorization and decomposition for associative algebras (of small dimension) are considered. A survey of applications (in particular, in cryptography) of so-called “hidden matrices” is given.

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 205—222.

1. Об алгоритмах открытого построения ключа на некоммутативной группе

1.1. Описание алгоритма

В [34] предлагается новый алгоритм открытого формирования секретного ключа, основанный на использовании некоммутативной группы $(\Gamma, \cdot)$ большого порядка.

Предполагается, что в группе Γ существуют элемент Q большого простого порядка $\operatorname{ord} Q = t$ (в [34] $t = q$, у нас параметр q используется как мощность поля, см. ниже) и коммутативная подгруппа $C = \Gamma_{\mathrm{comm}}$ со свойством

$$WQ \neq QW \quad \text{для каждого} \quad W \in C \setminus \{e\}. \tag{1}$$

Последнее условие означает, что группа C имеет тривиальное пересечение с нормализатором $N_\Gamma(Q)$ элемента Q в группе Γ:

$$C \cap N_\Gamma(Q) = e. \tag{2}$$

Параметры Q, t, C известны всем. Каждый из абонентов $i \in \overline{0,1}$ вырабатывает свой секретный ключ (W_i, z_i), $W_i \in C$, $z_i \in \overline{1, t-1}$, затем абоненты обмениваются посылками

$$W_i^{-1} Q^{z_i} W_i, \quad i \in \overline{0,1}, \tag{3}$$

и вычисляют общий ключ

$$K = (W_1 W_0)^{-1} Q^{z_1 z_0} W_1 W_0 = W_{1-i}^{-1} (W_i^{-1} Q^{z_i} W_i)^{z_{1-i}} W_{1-i}, \quad i \in \overline{0,1}. \tag{4}$$

При такой процедуре сложность вычисления общего секретного ключа оценивается сверху сложностью решения уравнения с двумя неизвестными

$$Y^{-1} Q^z Y = K, \quad z \in \overline{1, t-1}, \quad Y \in C. \tag{5}$$

Последнюю задачу можно назвать задачей *конгруэнц-логарифмирования*.

Сложность решения этой задачи, как и задачи дискретного логарифмирования, определяют прежде всего два фактора:

1) *выбор алгебраического носителя алгоритма* (группы Γ, основного элемента Q и подгруппы C), обеспечивающий стойкость алгоритма по отношению к методам, связанным с факторизацией и перебором;
2) *выбор способа представления алгебраического носителя*, делающий функцию $Y^{-1} Q^z Y$ однонаправленной.

Известно, что оптимизация по этим двум факторам алгоритма Диффи—Хеллмана на циклической группе порядка n даёт оценку стойкости $O(\sqrt{n})$ (оценка стойкости по отношению к методу согласования [1, 20]). Следует отметить, что последняя оценка является классическим примером экспертной оценки, т. е. она не доказана как нижняя оценка, но многочисленные усилия криптографов не дали более низкой оценки при хорошем выборе способа представления алгебраического носителя (см. 2)).

Изложенный алгоритм представляется, в принципе, интересным, и возможно, при удачной реализации решение задачи конгруэнц-логарифмирования может оказаться более сложным, чем решение задачи логарифмирования. Однако предлагаемый в [34] способ представления группы Γ (выбор способа представления алгебраического носителя) позволяет использовать алгоритм, имеющий сложность $O(\sqrt{t})$, равную сложности логарифмирования.

Заметим, что во всех реально предложенных в [34] вариантах выбора алгебры A параметр t существенно меньше мощности $|A|$ алфавита, в котором строится общий ключ (см. раздел 1.3), и оценка сложности $O(\sqrt{t})$ существенно меньше величины $O(\sqrt{|A|})$, а именно эта величина является оценкой сложности алгоритма восстановления ключа в процедуре Диффи—Хеллмана.

1.2. Слабости алгоритма, связанные с выбором представления алгебраического носителя

Авторы предлагают выбирать группу Γ как мультипликативную группу некоторой алгебры A размерности 4 над полем $F = \mathrm{GF}(q)$. Рассмотрим две несколько более общие ситуации.

1.2.1. Случай, когда A — простая алгебра, $\Gamma = A^*$

В этой ситуации $A = \mathrm{M}_m(P)$ — полное кольцо матриц над некоторым полем P, содержащим F, $|P| = \pi$ (см., например, [35]); Q — матрица простого порядка t над полем P; C — абелева подгруппа группы $\Gamma = A^*$ со свойством (2).

Решение уравнения (5) можно разбить на два независимых этапа.

I. Определение параметра $z \in \overline{1, t-1}$.

II. Определение значения $Y \in C$ при известном значении z.

Простое число t может появиться в качестве порядка матрицы Q в одном из следующих случаев (см. [8]):

а) $t = p = \mathrm{char}\, P$, матрица Q подобна жордановой матрице, каждая клетка которой имеет размер, не превосходящий p, и корень e (если $m = 2$, то Q подобна клетке второго порядка);

б) $t \mid \pi - 1$, $\pi = |P|$, матрица Q подобна диагональной матрице, на диагонали которой стоят элементы поля P порядка t;

в) $t \mid \frac{(\pi^m-1)}{\pi-1} \frac{(\pi^{m-1}-1)}{\pi-1} \dots \frac{(\pi^2-1)}{\pi-1}$, $m = kl$, матрица Q подобна распавшейся на клетки размеров $k \times k$ матрице,

$$Q \sim \mathrm{Diag}(Q_1, \dots, Q_l),$$

у которой минимальный многочлен каждой клетки $\mu_{Q_i}(z)$ есть неприводимый над P многочлен степени k и периода t (если $m = 2$, то $l = 1$ и $\mu_Q(x) = \chi_Q(x)$ — неприводимый многочлен).

Здесь мы рассмотрим наиболее интересный, на наш взгляд, с точки зрения стойкости алгоритма случай в).

Будем полагать, что $m \geqslant 2$ и $\mu_Q(x) = \chi_Q(x) = f(x)$ — неприводимый многочлен простого периода t. Покажем, что в этом случае этап I можно реализовать со сложностью $O(\sqrt{t})$.

Изложению алгоритма вычисления параметра z предпошлём несколько замечаний.

Пусть P' — минимальное поле разложения многочлена $f(x)$ над P и $\vartheta \in P'$ — корень этого многочлена. Можно считать, что этот корень нам известен. Например, если поле P' представлено в виде $P' = P[x]/f(x)P[x]$, то $\vartheta = x + f(x)P[x]$. Тогда $\operatorname{ord}\vartheta = \operatorname{ord} Q = t$ — простое число, $[P' : P] = m = \deg\mu_Q(x)$, $m = \operatorname{ord}\pi \pmod t$, $|P'| = \pi^m$. Отсюда следует, что для любого $s \in \overline{1, t-1}$ выполняются соотношения $\operatorname{ord}\vartheta^s = t$, $P' = P(\vartheta^s)$, и если $\mu_{\vartheta^s,P}(x)$ — минимальный многочлен элемента ϑ^s над P, то

$$\mu_{Q^s}(x) = \mu_{\vartheta^s,P}(x) = (x - \vartheta^s)(x - \vartheta^{s\pi})\cdots(x - \vartheta^{s\pi^{m-1}}) — \tag{6}$$

неприводимый многочлен степени m над P и для любого $r \in \overline{1, t-1}$ $\mu_{Q^r}(x) = \mu_{Q^s}(x)$, если и только если $r \in \{s, s\pi, \ldots, s\pi^{m-1}\} \pmod t$. Набор коэффициентов $(c_0, c_1, \ldots, c_{m-1})$ многочлена

$$\mu_{Q^s}(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1x - c_0$$

вычисляется как решение $c^{\downarrow} = (c_0, c_1, \ldots, c_{m-1})^{\mathrm{T}}$ системы линейных уравнений

$$(a^{\downarrow}, Q^s a^{\downarrow}, \ldots, Q^{(m-1)s}a^{\downarrow})c^{\downarrow} = Q^{ms}a^{\downarrow}$$

при любом $a^{\downarrow} \in P^{(m)} \setminus 0^{\downarrow}$.

Теперь можно предложить следующий алгоритм.

Алгоритм согласования для вычисления неизвестного z в уравнении (5).

Вход: матрицы Q и K из уравнения (5).
Выход: значение неизвестного z в m вариантах.
Параметр алгоритма: $d = [\sqrt{t}] + 1$.
Шаг 1: вычислить многочлен $\mu_K(x)$.
Шаг 2: найти корень α многочлена $\mu_K(x)$ в поле $P' = P(\vartheta)$.
Шаг 3: найти решение y_0 уравнения $\vartheta^y = \alpha$ методом согласования с шагом d.
Ответ: параметр z из уравнения (5) удовлетворяет условию

$$z \in \{y_0, y_0\pi, \ldots, y_0\pi^{m-1}\}.$$

Наиболее трудоёмким в алгоритме является шаг 3, и сложность алгоритма можно оценить величиной $O(\sqrt{t})$.

Определение параметра Y в уравнении (5) при известном значении z (этап II) проводится по следующему алгоритму.

Шаг 1: для произвольного $a^{\downarrow} \in P^{(m)} \setminus 0^{\downarrow}$ вычислить матрицу

$$U = (a^{\downarrow}\, Q^z a^{\downarrow} \ldots Q^{z(m-1)} a^{\downarrow}).$$

(Тогда $U^{-1}Q^zU = S\big(g(x)\big) = S$ — сопровождающая матрица для многочлена $\mu_{Q^z}(x)$.)

Шаг 2: вычислить матрицу $V = (a^{\downarrow}\, Ka^{\downarrow} \ldots K^{m-1}a^{\downarrow})$. (Тогда $V^{-1}KV = S$, матрица $\tilde{Y} = U^{-1}YV$ удовлетворяет соотношению $\tilde{Y}^{-1}S\tilde{Y} = S$, и следовательно, ввиду неприводимости многочлена $g(x)$ $\tilde{Y}$ есть ненулевой элемент поля

$$P(S) = \{c_0E + c_1S + \ldots + c_{m-1}S^{m-1} \colon c_i \in P\}.$$

Теперь, пользуясь условием $Y \in UP(S)V^{-1}$, матрицу Y можно представить в виде линейной комбинации известных матриц с неопределёнными коэффициентами

$$Y = \sum_{i=0}^{m-1} y_i U S^i V^{-1}$$

и далее находить эти коэффициенты, решая систему линейных уравнений $Q^zY = YK$.)

Шаг 3: найти ненулевое решение $\vec{c}$ системы однородных линейных уравнений с m неизвестными

$$\sum_{i=0}^{m-1} (Q^z U S^i V^{-1} - U S^i V^{-1} K) y_i = 0.$$

Шаг 4: вычислить

$$Y_0 = \sum_{i=0}^{m-1} c_i U S^i V^{-1}.$$

(Тогда множество всех решений уравнения (5) есть $Y_0P(Q^z)^*$, где $P(Q^z)^* = P(Q^z) \setminus 0$ — мультипликативная группа поля

$$P(Q^z) = \{a_0E + a_1Q^z + \ldots + a_{m-1}Q^{z(m-1)} \colon a_i \in P\};$$

другими словами, множество всех решений $Y \in \mathrm{M}_m(P)^*$ уравнения (5) (при заданном значении z) есть множество всех ненулевых векторов m-мерного подпространства $\mathcal{Y} = Y_0P(Q^z)$.)

Шаг 5: вычислить множество всех решений уравнения (5), принадлежащих подгруппе C:

$$Y_0P(Q^z)^* \cap C. \tag{7}$$

Если последнее пересечение пусто, то значение $z = y_0\pi^i$ на выходе алгоритма, реализующего этап I, выбрано неверно; если $Y \in Y_0P(Q^z)^* \cap C$, то (Y, z) — один из криптографически эквивалентных секретных ключей абонента.

Сложность вычислений на шагах 1—3 последнего алгоритма, сводящихся к решению линейных задач, можно оценить величиной $O(m^3)$ операций поля P. В контексте [34] это вообще константа, так как $m \leqslant 2$.

Менее понятна сложность вычисления пересечения (7), поскольку авторы не указывают конкретных способов построения группы C. Можно лишь сказать, что если группа C принадлежит некоторому линейному многообразию $\mathcal{M}$ пространства ${}_P\mathrm{M}_m(P)$, сравнимому по мощности с $|C|$, то задача сводится практически к линейной задаче вычисления базиса пересечения $\mathcal{Y} \cap \mathcal{M}$ двух линейных многообразий.

1.2.2. Случай, когда алгебра A не является простой

Факторизацией алгебры A по её радикалу и применением теоремы Молина—Веддербёрна—Артина этот случай сводится к рассмотренному выше случаю, причём получающееся кольцо матриц имеет мощность, существенно меньшую мощности исходной алгебры (см. ниже).

1.3. Алгебраические свойства обобщённых алгебр кватернионов над конечными полями

Рассмотрим алгебры A, которые были предложены в [34] в качестве алгебраических носителей алгоритма.

Пусть $F = \mathrm{GF}(q)$ — поле из $q = p^s$ элементов. В этом разделе всюду предполагается, что $p \neq 2$. Рассмотрим алгебру A с базисом $\{\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$, причём умножение в ней определено таблицей операции $x * y$:

x \ y	$\boldsymbol{e}$	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{e}$	$\boldsymbol{e}$	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}$	$\boldsymbol{i}$	$-\varepsilon\boldsymbol{e}$	$\varepsilon\boldsymbol{k}$	$-\boldsymbol{j}$
$\boldsymbol{j}$	$\boldsymbol{j}$	$-\varepsilon\boldsymbol{k}$	$-\varepsilon\boldsymbol{e}$	$\boldsymbol{i}$
$\boldsymbol{k}$	$\boldsymbol{k}$	$\boldsymbol{j}$	$-\boldsymbol{i}$	$-\boldsymbol{e}$

Предложение 1.3.1. *Если алгебра A полупроста, то она изоморфна полной матричной алгебре* $\mathrm{M}_2(F)$.

Доказательство. По теореме Молина—Веддербёрна—Артина и теореме Веддербёрна

$$A \cong \bigoplus_{i=1}^{n} \mathrm{M}_{d_i}(P_i),$$

где P_i — некоторые расширения поля F. Сравнивая размерности левой и правой части, получаем, что

$$4 = \sum_{i=1}^{n} d_i^2 \dim_F(P_i),$$

причём, в силу того что алгебра A некоммутативна, хотя бы одно из чисел d_i больше 1. Значит, $n = 1$, $d_1 = 2$ и $P_1 = F$. □

Предложение 1.3.2. *При $\varepsilon \neq 0$ алгебра A полупроста.*

Доказательство. Прежде всего для общего элемента

$$\boldsymbol{g} = a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$$

вычислим произведения

$$\boldsymbol{g}\boldsymbol{i} = -\varepsilon b\boldsymbol{e} + a\boldsymbol{i} + d\boldsymbol{j} - \varepsilon c\boldsymbol{k}, \tag{8}$$

$$\boldsymbol{g}\boldsymbol{j} = -\varepsilon c\boldsymbol{e} - d\boldsymbol{i} + a\boldsymbol{j} + \varepsilon b\boldsymbol{k}, \tag{9}$$

$$\boldsymbol{g}\boldsymbol{k} = -d\boldsymbol{e} + c\boldsymbol{i} - b\boldsymbol{j} + a\boldsymbol{k}. \tag{10}$$

С помощью этих выражений легко найти общий вид квадрата элемента алгебры A:

$$\begin{aligned}\boldsymbol{g}^2 = (a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k})^2 &= a\boldsymbol{g} + b\boldsymbol{g}\boldsymbol{i} + c\boldsymbol{g}\boldsymbol{j} + d\boldsymbol{g}\boldsymbol{k} = \\ &= a(a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}) + b(-\varepsilon b\boldsymbol{e} + a\boldsymbol{i} + d\boldsymbol{j} - \varepsilon c\boldsymbol{k}) + \\ &+ c(-\varepsilon c\boldsymbol{e} - d\boldsymbol{i} + a\boldsymbol{j} + \varepsilon b\boldsymbol{k}) + d(-d\boldsymbol{e} + c\boldsymbol{i} - b\boldsymbol{j} + a\boldsymbol{k}) = \\ &= (a^2 - \varepsilon b^2 - \varepsilon c^2 - d^2)\boldsymbol{e} + 2ab\boldsymbol{i} + 2ac\boldsymbol{j} + 2ad\boldsymbol{k}. \end{aligned} \tag{11}$$

Предположим теперь, что алгебра A не полупроста. Тогда существует элемент $\boldsymbol{g} \in A$, такой что $\boldsymbol{g} \neq 0$, но $(\boldsymbol{g}A)^2 = 0$. Последнее условие равносильно тому, что $\boldsymbol{g}^2 = (\boldsymbol{g}\boldsymbol{i})^2 = (\boldsymbol{g}\boldsymbol{j})^2 = (\boldsymbol{g}\boldsymbol{k})^2 = 0$. Пусть $a \neq 0$. Тогда из (11) вытекает, что $b = c = d = 0$, но тогда и $a^2 = 0$. Противоречие показывает, что $a = 0$ при условии, что $\boldsymbol{g}^2 = 0$. Комбинируя (8) и (11), аналогично получаем, что $\varepsilon b = 0$, откуда следует, что $b = 0$. Применяя то же рассуждение к $\boldsymbol{g}\boldsymbol{j}$ и $\boldsymbol{g}\boldsymbol{k}$, получаем, что $c = d = 0$. Итак, $\boldsymbol{g} = 0$, противоречие. □

Следствие 1.3.3. *При $\varepsilon \neq 0$ алгебра A изоморфна матричной алгебре $\mathrm{M}_2(F)$ и число обратимых элементов алгебры A равно $(q^2 - 1)(q^2 - q)$.*

Доказательство. Утверждение вытекает из предложений 1.3.1, 1.3.2 и хорошо известной формулы для порядка группы $\mathrm{GL}_n(F)$. □

Следующее утверждение показывает, как явно построить систему матричных единиц в алгебре A при некотором дополнительном условии.

Предложение 1.3.4. *Пусть $\varepsilon \neq 0$ и $q \equiv 1 \pmod 4$ (т. е. $p \equiv 1 \pmod 4$ или s чётно). Тогда в качестве системы матричных единиц можно взять элементы*

$$e_{11} = \frac{1}{2}(\boldsymbol{e} + \alpha\boldsymbol{k}),$$
$$e_{22} = \frac{1}{2}(\boldsymbol{e} - \alpha\boldsymbol{k}),$$
$$e_{12} = -\frac{1}{2\varepsilon}(\boldsymbol{i} + \alpha\boldsymbol{j}),$$
$$e_{21} = \frac{1}{2}(\boldsymbol{i} - \alpha\boldsymbol{j}),$$

где α — элемент порядка 4 группы F^*.

Доказательство. Легко убедиться, что $\alpha^2 = -1$. Рассмотрим элементы

$$e_{11} = \frac{1}{2}(\boldsymbol{e} + \alpha\boldsymbol{k}), \quad e_{22} = \frac{1}{2}(\boldsymbol{e} - \alpha\boldsymbol{k}).$$

Очевидно, что тогда $e_{11}^2 = e_{11}$, $e_{22}^2 = e_{22}$ и $e_{11}e_{22} = e_{22}e_{11} = 0$. Вычислим элементы

$$\begin{aligned}
u_{12} &= e_{11}\boldsymbol{i}e_{22} = \\
&= \frac{1}{4}(\boldsymbol{e} + \alpha\boldsymbol{k})(\boldsymbol{i} - \alpha\boldsymbol{i}\boldsymbol{k}) = \frac{1}{4}(\boldsymbol{e} + \alpha\boldsymbol{k})(\boldsymbol{i} + \alpha\boldsymbol{j}) = \frac{1}{4}(\boldsymbol{i} + \alpha\boldsymbol{k}\boldsymbol{i} + \alpha\boldsymbol{j} + \alpha^2\boldsymbol{k}\boldsymbol{j}) = \\
&= \frac{1}{4}\big(\boldsymbol{i} + \alpha\boldsymbol{j} + \alpha\boldsymbol{j} + \alpha^2(-\boldsymbol{i})\big) = \frac{1}{4}(2\boldsymbol{i} + 2\alpha\boldsymbol{j}) = \frac{1}{2}(\boldsymbol{i} + \alpha\boldsymbol{j}), \\
u_{21} &= e_{22}\boldsymbol{i}e_{11} = \\
&= \frac{1}{4}(\boldsymbol{e} - \alpha\boldsymbol{k})(\boldsymbol{i} + \alpha\boldsymbol{i}\boldsymbol{k}) = \frac{1}{4}(\boldsymbol{e} - \alpha\boldsymbol{k})(\boldsymbol{i} - \alpha\boldsymbol{j}) = \frac{1}{4}(\boldsymbol{i} - \alpha\boldsymbol{k}\boldsymbol{i} - \alpha\boldsymbol{j} + \alpha^2\boldsymbol{k}\boldsymbol{j}) = \\
&= \frac{1}{4}\big(\boldsymbol{i} - \alpha\boldsymbol{j} - \alpha\boldsymbol{j} + \alpha^2(-\boldsymbol{i})\big) = \frac{1}{4}(2\boldsymbol{i} - 2\alpha\boldsymbol{j}) = \frac{1}{2}(\boldsymbol{i} - \alpha\boldsymbol{j}).
\end{aligned}$$

Непосредственно проверяется, что

$$\begin{aligned}
u_{12}u_{21} &= \frac{1}{4}(\boldsymbol{i} + \alpha\boldsymbol{j})(\boldsymbol{i} - \alpha\boldsymbol{j}) = \frac{1}{4}(\boldsymbol{i}^2 + \alpha\boldsymbol{j}\boldsymbol{i} - \alpha\boldsymbol{i}\boldsymbol{j} - \alpha^2\boldsymbol{j}^2) = \\
&= \frac{1}{4}(-\varepsilon\boldsymbol{e} - \alpha\varepsilon\boldsymbol{k} - \alpha\varepsilon\boldsymbol{k} - \varepsilon\boldsymbol{e}) = -\varepsilon\frac{1}{2}(\boldsymbol{e} + \alpha\boldsymbol{k}) = -\varepsilon e_{11}, \\
u_{21}u_{12} &= \frac{1}{4}(\boldsymbol{i} - \alpha\boldsymbol{j})(\boldsymbol{i} + \alpha\boldsymbol{j}) = \frac{1}{4}(\boldsymbol{i}^2 - \alpha\boldsymbol{j}\boldsymbol{i} + \alpha\boldsymbol{i}\boldsymbol{j} - \alpha^2\boldsymbol{j}^2) = \\
&= \frac{1}{4}(-\varepsilon\boldsymbol{e} + \alpha\varepsilon\boldsymbol{k} + \alpha\varepsilon\boldsymbol{k} - \varepsilon\boldsymbol{e}) = -\varepsilon\frac{1}{2}(\boldsymbol{e} - \alpha\boldsymbol{k}) = -\varepsilon e_{22}.
\end{aligned}$$

Остаётся взять

$$e_{12} = -\frac{1}{\varepsilon}u_{12} = -\frac{1}{2\varepsilon}(\boldsymbol{i} + \alpha\boldsymbol{j}), \quad e_{21} = u_{21}$$

и убедиться, что $\{e_{ij}\colon 1 \leqslant i, j \leqslant 2\}$ — система матричных единиц в A. □

В случае когда -1 не является квадратом в F, явной формулы для нетривиального идемпотента получить не удалось, однако мы приведём некоторый вероятностный алгоритм, подходящий для этого случая. При этом будет удобно

воспользоваться свойствами квадратичного характера поля F, т. е. гомоморфизма $\eta\colon F^* \to \{1,-1\}$ с ядром $(F^*)^2$.

Предложение 1.3.5. *Элемент $\boldsymbol{g} = a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ является нетривиальным идемпотентом тогда и только тогда, когда*

$$a = \frac{1}{2}, \quad \frac{1}{4} + \varepsilon(b^2 + c^2) + d^2 = 0. \tag{12}$$

Доказательство. Заметим, что

$$\begin{aligned}\boldsymbol{g}^2 - \boldsymbol{g} &= (a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k})^2 - (a\boldsymbol{g} + b\boldsymbol{g}\boldsymbol{i} + c\boldsymbol{g}\boldsymbol{j} + d\boldsymbol{g}\boldsymbol{k}) = \\ &= (a^2 - \varepsilon b^2 - \varepsilon c^2 - d^2)\boldsymbol{e} + 2\,ab\boldsymbol{i} + 2\,ac\boldsymbol{j} + 2\,ad\boldsymbol{k} - a\boldsymbol{e} - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k} + \\ &+ (a^2 - \varepsilon b^2 - \varepsilon c^2 - d^2 - a)\boldsymbol{e} + (2a-1)b\boldsymbol{i} + (2a-1)c\boldsymbol{j} + (2a-1)d\boldsymbol{k}. \end{aligned} \tag{13}$$

Если $2a - 1 \neq 0$, то $b = c = d = 0$ и $a^2 = a$, поэтому $\boldsymbol{g} = 0$ или $\boldsymbol{g} = \boldsymbol{e}$, т. е. $\boldsymbol{g}$ — тривиальный идемпотент. Если же $a = \frac{1}{2}$, то, подставляя a в (13), получаем (12). □

Следствие 1.3.6. *При $-\varepsilon \in (F^*)^2$ нетривиальный идемпотент находится с помощью одного логарифмирования в поле F.*

Доказательство. Достаточно взять $b = d = 0$ в (12) и решить уравнение $c^2 = -\frac{1}{4\varepsilon}$. □

Следствие 1.3.7. *При $-\varepsilon \notin (F^*)^2$ и $-1 \notin (F^*)^2$ нетривиальный идемпотент можно найти в среднем с помощью одного логарифмирования в поле F и $\frac{2(p-1)}{p+1}$ логарифмирований в поле* $\mathrm{GF}(p)$.

Доказательство. Положим $d = 0$ и $x = c/b$ в (12). Получится уравнение $1 + x^2 = -\frac{1}{4b^2\varepsilon}$. Оно имеет решение относительно b тогда и только тогда, когда $\eta(1 + x^2) = -1$, и это решение можно найти с помощью одного логарифмирования в F. Значение x, для которого $\eta(1 + x^2) = -1$, можно найти с помощью нескольких опробований, причём достаточно выбирать x из простого подполя $\mathbb{F}_p = GF(p) \subseteq F$. Известно [9, теорема 5.48], что

$$\sum_{x \in \mathbb{F}_p} \eta(1 + x^2) = -1. \tag{14}$$

Пусть $U = \{x \in \mathbb{F}_p^*\colon \eta(1 + x^2) = 1$, $V = \{x \in \mathbb{F}_p^*\colon \eta(1 + x^2) = -1$, $u = |U|$, $v = |V|$. Тогда $u + v = p - 1$, а $u - v = -2$ в силу 14 и того, что $\eta(1) = 1$. Следовательно, $u = \frac{p-3}{2}$, $v = \frac{p+1}{2}$. Это означает, что при случайном выборе $x \in \mathbb{F}_p^*$ вероятность события $\eta(1 + x^2) = -1$ равна $\frac{p+1}{2(p-1)}$. Хорошо известно (см., например, [7, пример 3, с. 100]), что при заданной вероятности $\mathfrak{p}$ успеха в одном испытании математическое ожидание числа испытаний до первого успеха равно $\frac{1}{\mathfrak{p}}$, что и доказывает приведённую среднюю оценку. □

Рассмотрим оставшийся случай $\varepsilon = 0$.

Лемма 1.3.8. *Положим $B = F\boldsymbol{e} + F\boldsymbol{k}$. Тогда отображение*

$$a\boldsymbol{e} + b\boldsymbol{k} \mapsto \overline{a\boldsymbol{e} + b\boldsymbol{k}} = a\boldsymbol{e} - b\boldsymbol{k}$$

является инволюцией (автоморфизмом порядка 2) алгебры B.

Доказательство. Утверждение проверяется непосредственным вычислением. □

Предложение 1.3.9. *Пусть $\varepsilon = 0$. Тогда алгебра A изоморфна алгебре матриц вида*

$$\begin{pmatrix} u & v \\ 0 & \overline{u} \end{pmatrix}, \quad u, v \in B,$$

и

$$|A^*| = q^2|B^*| = \begin{cases} q^2(q-1)^2 & \text{при } q \equiv 1 \pmod 4, \\ q^2(q^2-1) & \text{при } q \equiv 3 \pmod 4. \end{cases}$$

Доказательство. Очевидно, что в рассматриваемом случае

$$A = B\boldsymbol{e} \dotplus B\boldsymbol{i}$$

(прямая сумма левых B-модулей). Определим отображение $\varphi\colon A \to \mathrm{M}_2(B)$:

$$\varphi(u\boldsymbol{e} + v\boldsymbol{i}) = \begin{pmatrix} u & v \\ 0 & \overline{u} \end{pmatrix} \quad \text{для любых} \quad u, v \in B.$$

Линейность отображения φ очевидна. Проверим, что

$$\varphi\big((u\boldsymbol{e} + v\boldsymbol{i})(u'\boldsymbol{e} + v'\boldsymbol{i})\big) = \begin{pmatrix} u & v \\ 0 & \overline{u} \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & \overline{u'} \end{pmatrix} \quad \text{для любых} \quad u, v, u', v' \in B.$$

Заметим, что если $u = a\boldsymbol{e} + b\boldsymbol{k} \in B$, то $u\boldsymbol{i} = a\boldsymbol{i} + b\boldsymbol{j}$, а $\boldsymbol{i}u = a\boldsymbol{i} - b\boldsymbol{j} = \overline{u}i$. Следовательно,

$$\begin{aligned} \varphi\big((u\boldsymbol{e} + v\boldsymbol{i})(u'\boldsymbol{e} + v'\boldsymbol{i})\big) &= \varphi(uu'\boldsymbol{e} + uv'\boldsymbol{i} + v\boldsymbol{i}u') = \varphi(uu'\boldsymbol{e} + vu'\boldsymbol{i} + \overline{u'}v\boldsymbol{i}) = \\ &= \begin{pmatrix} uu' & vu' + \overline{u'}v \\ 0 & \overline{uu'} \end{pmatrix} = \begin{pmatrix} u & v \\ 0 & \overline{u} \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & \overline{u'} \end{pmatrix} = \varphi(u\boldsymbol{e} + v\boldsymbol{i})\varphi(u'\boldsymbol{e} + v'\boldsymbol{i}). \end{aligned}$$

Осталось заметить, что матрица

$$\begin{pmatrix} u & v \\ 0 & \overline{u} \end{pmatrix}$$

обратима тогда и только тогда, когда обратим элемент $u \in B$. Следовательно, $|A^*| = |B^*|\,|B|$. Но при $q \equiv 1 \pmod 4$ поле F содержит элемент α порядка 4, поэтому $B = Fe_1 + Fe_2$, где $e_1 = \frac{1}{2}(\boldsymbol{e} + \alpha\boldsymbol{k})$ и $e_2 = \frac{1}{2}(\boldsymbol{e} - \alpha\boldsymbol{k})$ — нетривиальные идемпотенты алгебры B. Значит, в этом случае $|B^*| = |F^*|^2 = (q-1)^2$. С другой стороны, при $q \equiv 3 \pmod 4$ многочлен $x^2 + 1$ неприводим над F, поэтому алгебра B изоморфна полю $F[x]/(x^2+1)$, и $|B^*| = q^2 - 1$. □

2. Алгоритмы факторизации и разложения ассоциативных алгебр малой размерности

2.1. Введение

При рассмотрении различных криптографических схем, основанных на вычислениях в заданной ассоциативной алгебре, факторизация алгебры по её радикалу и последующее разложение алгебры в прямую сумму простых алгебр сводит задачу к аналогичной задаче для алгебр меньшей размерности, тем самым уменьшая её сложность. Известны алгоритмы, позволяющие для ассоциативной алгебры, заданной структурными константами относительно некоторого базиса, получить описание её радикала (при условии, что характеристика основного поля F больше размерности алгебры), а для полупростой алгебры — её разложение в прямую сумму матричных алгебр над полями. Все алгоритмы, рассмотренные далее в этом разделе, имеют полиномиальную сложность относительно $\log|F|$ при постоянной размерности алгебры. Приведём сводку полученных результатов.

Пусть A — ассоциативная алгебра размерности n над конечным полем F характеристики p и мощности $q = p^s$, $Z(A)$ — её центр, $\mathrm{rad}(A)$ — её радикал, т. е. наибольший нильпотентный идеал алгебры A. Предположим, что алгебра A задана структурными константами относительно некоторого фиксированного базиса $e_1, \ldots, e_n$ (т. е. известны координаты тензора (τ_{ij}^k), такого что $e_i e_j = \sum\limits_{k=1}^{n} \tau_{ij}^k e_k$, $i, j \in \overline{1,n}$).

Для любого подмножества $S \subseteq A$ пусть $l_A(S)$ обозначает левый аннулятор множества S, т. е.

$$l_A(S) = \{a \in A \colon aS = 0\}.$$

Аналогично определяется правый аннулятор $r_A(S)$ множества S. Если $l_A(S) = r_A(S)$, то мы будем также использовать обозначение $\mathrm{Ann}_A(S) = l_A(S) = r_A(S)$.

2.2. Радикал и центр алгебры

Следующее утверждение проверяется с помощью функции «след».

Предложение 2.2.1. *При условии $p > n$ для описания радикала (в частности, для проверки полупростоты) алгебры A достаточно решить систему из n линейных уравнений над полем F.*

Следующее утверждение проверяются непосредственно.

Предложение 2.2.2. *Задача о нахождении центра алгебры размерности n сводится к решению системы n линейных уравнений.*

2.3. Распознавание строения полупростой коммутативной алгебры

Следующее утверждение вытекает из хорошо известного факта, что элементы поля из q^l элементов удовлетворяют уравнению $x^{q^l} - x = 0$, решение которого в алгебре над полем $\mathbb{F}_q$ сводится к решению системы линейных уравнений.

Предложение 2.3.1. *Предположим, что алгебра A коммутативна и полупроста. Тогда*

$$A = \bigoplus_{l=1}^{m} (\mathbb{F}_{q^l})^{r_l}, \tag{15}$$

где $\mathbb{F}_{q^l}$ — поле из q^l элементов,

$$P^r = \underbrace{P \oplus P \oplus \ldots \oplus P}_{r \text{ раз}},$$

знак $\oplus$ обозначает прямую сумму алгебр. Решая не более n систем линейных однородных уравнений, каждая из которых содержит не более n уравнений, можно найти все компоненты (15) *вида $A_l = (\mathbb{F}_{q^l})^{r_l}$. Для построения этой системы достаточно выполнить $O(\log_2 q)$ операций в алгебре A. Количество слагаемых вида $\mathbb{F}_{q^l}$ в каждой из алгебр A_l можно найти из равенства*

$$r_l = \frac{\dim_F(A_l)}{l}.$$

2.4. Выделение прямых сумм алгебр матриц одного размера

Следующее предложение вытекает из хорошо известной теоремы Амицура—Левицкого [12, § 20.4].

Предложение 2.4.1. *Пусть R — полупростая конечномерная алгебра над полем F, $A = Z(R)$. Известно, что R — прямая сумма матричных алгебр над некоторыми расширениями поля F:*

$$R = \bigoplus_{i,j} \mathrm{M}_i(P_j), \tag{16}$$

где пара индексов (i, j) пробегает некоторое конечное множество. Соответственно,

$$A = \bigoplus_{i,j} P_j.$$

Применяя к A предложение 2.3.1*, можно без ограничения общности считать все расширения P_j одним и тем же полем P известного порядка q^l и записать* (16) *в виде*

$$R = \bigoplus_{i=1}^{r} \big(\mathrm{M}_{k_i}(P)\big)^{t_i}, \tag{17}$$

группируя прямые слагаемые, изоморфные алгебрам матриц одного порядка. Тогда компоненты вида $R_i = \big(\mathrm{M}_i(P)\big)^{t_i}$ *в разложении* (17) *можно найти, решая не более* n *систем линейных однородных уравнений, каждая из которых содержит не более* n *уравнений. Для построения этой системы достаточно выполнить* $O\left(\frac{n!}{(n-2[\sqrt{n}])!}\right)$ *операций в алгебре* A. *Количество слагаемых вида* $\mathrm{M}_i(P)$ *в каждой из алгебр* R_i *можно найти из равенства*

$$t_i = \frac{\dim_F R_i}{i^2 \dim_F P}.$$

Нам не удалось найти алгоритма такой же сложности для нахождения компонент прямой суммы матричных алгебр одинаковых порядков над изоморфными полями. Однако ниже мы предлагаем вероятностный алгоритм для решения этой задачи.

2.5. Разложение прямой суммы изоморфных полей

Пусть алгебра A над полем F — прямая сумма m копий известного расширения P основного поля F, $\dim_F P = t$:

$$A = \bigoplus_{j=1}^{m} P_j, \quad P_j \cong P, \quad j \in \overline{1,n}. \tag{18}$$

Задача состоит в нахождении базисов компонент этого разложения. Естественно, при $m = 1$ задача тривиальна. В общем случае, зная ненулевой идеал I алгебры A, имеющий ненулевой аннулятор, легко получить разложение $A = I \oplus l_A(I)$ и рассматривать далее алгебры I и $l_A(I)$. Итак, достаточно при $m > 1$ найти пару делителей нуля алгебры A.

Очевидна следующая лемма.

Лемма 2.5.1. *Пусть* a *— элемент алгебры* A, $a = \sum\limits_{j=1}^{m} a_j$, *где* $a_j \in P_j$. *Тогда минимальный многочлен элемента* a *— наименьшее общее кратное минимальных многочленов элементов* $a_1, \ldots, a_m$ *как элементов поля* P.

Таким образом, вероятность при случайном выборе получить делитель нуля равна $1 - \left(\frac{|P|-1}{|P|}\right)^m$.

3. Спрятанные матрицы

В теории колец и её приложениях (в том числе криптографических, см. [29, 37, 42]) часто важным оказывается следующий вопрос: является ли данное кольцо кольцом матриц над некоторым кольцом?

Классический ответ на этот вопрос даёт следующая теорема.

Теорема 3.1. *Пусть A — кольцо и $n \geqslant 2$. Тогда следующие условия эквивалентны*:

1) $A \cong \mathrm{M}_n(R)$ *для некоторого кольца* R;
2) *в кольце* A *существует система матричных единиц* $\{E_{ij} \in A \mid 1 \leqslant i, j \leqslant n\}$, *для которой* $E_{ij}E_{kl} = \delta_{jk}E_{il}$, $E_{11} + \ldots + E_{nn} = 1$;
3) $A_A = I_1 \oplus \ldots \oplus I_n$, *где* $I_1, \ldots, I_n$ — *изоморфные* (*как правые модули*) *правые идеалы кольца* A.

Если $A = \mathrm{M}_n(R)$, $a = E_{1n}$, $b = E_{21} + E_{32} + \ldots + E_{n,n-1}$, то

$$b^n = 0, \quad ab^{n-1} + bab^{n-2} + \ldots + b^{n-1}a = 1. \tag{19}$$

Теорема 3.2 [38]. *Кольцо A является кольцом $(n \times n)$-матриц тогда и только тогда, когда в кольце A найдутся два элемента a и b, удовлетворяющие условиям* (19).

Теорема 3.3 [13]. *Для данных натуральных чисел m, n кольцо A является кольцом $\big((m+n)\times(m+n)\big)$-матриц в том и только в том случае, когда найдутся такие элементы $a, b, c \in A$, что $b^{m+n} = 0$ и $ab^m + b^n c = 1$.*

Если $n = 1$ и $m = n - 1$, то получим следующий результат.

Следствие 3.4. *Кольцо A является кольцом $(n \times n)$-матриц тогда и только тогда, когда найдутся такие элементы $a, b, c \in A$, что $b^n = 0$ и $ab^{n-1} + bc = 1$.*

Пример 3.5 [17,18,38]. Пусть $H = Z \oplus Zi \oplus Zj \oplus Zk$ — кольцо кватернионов с целыми коэффициентами,

$$A = \begin{pmatrix} H & 3H \\ H & H \end{pmatrix} -$$

подкольцо кольца матриц $\mathrm{M}_2(H)$. Тогда A — полное матричное кольцо (2×2)-матриц.

Действительно, пусть $\alpha = i + j + k$,

$$a = \begin{pmatrix} i & 0 \\ 1 & -i \end{pmatrix}, \quad b = \begin{pmatrix} \alpha & 3 \\ 1 & -\alpha \end{pmatrix}.$$

Тогда $b^2 = 0$ и $ab + ba = 1$ в кольце A. Следовательно, $A \cong \mathrm{M}_2(R)$ для некоторого кольца R. В нашем случае кольцо R изоморфно идеализатору $I_H(\alpha H)$, являющемуся подкольцом кольца H.

Более того, в [18] показано, что кольца

$$A_n = \begin{pmatrix} H & nH \\ H & H \end{pmatrix}, \quad B_n = \begin{pmatrix} H & nH \\ nH & H \end{pmatrix}$$

являются кольцами (2×2)-матриц в том и только в том случае, когда n нечётно.

Для натурального числа n подкольцо $T_n = H + \mathrm{M}_2(nH)$ кольца $\mathrm{M}_2(H)$ является кольцом (2×2)-матриц тогда и только тогда, когда любой простой делитель числа n сравним с 1 по модулю 4 (см. [31,32]).

Имеются соответствующие результаты для косых колец Оре (см. [13,31]).

Приведём некоторые другие характеризации матричных колец.

Теорема 3.6 [31]. *Кольцо A является кольцом $(n \times n)$-матриц тогда и только тогда, когда для некоторого (следовательно, для всех) $r \geqslant 2$ матрица $F_r = E_{21} + E_{12} + \ldots + E_{r,r-1}$ размера $r \times r$ имеет корень степени n в кольце $\mathrm{M}_r(A)$.*

Теорема 3.7 [28,31]. *Для $n \geqslant 2$ кольцо A является кольцом $(n \times n)$-матриц в том и только в том случае, когда существуют такие элементы $f, g \in A$, что $f^n = g^n = 0$ и $f^{n-1} + gf^{n-2} + \ldots + g^{n-1} \in U(A)$.*

Теорема 3.8 [27]. *Кольцо A изоморфно кольцу $\mathrm{M}_n(R)$ для некоторого кольца R в том и только в том случае, когда существуют такие элементы $x, y \in A$, что $x^n = y^2 = 0$, $x^{n-1} \neq 0$, элемент $x + y$ обратим и $I_R(x^{n-1}) \cap Ry = 0$, где $I_R(x^{n-1})$ — левый аннулятор элемента x^{n-1}.*

Некоторые из критериев матричности колец имеют аналоги для полуколец (см. [6]).

Конечно, необходимо отметить классические теоремы Молина—Веддербёрна—Артина и Голди (если A — первичное кольцо, в котором каждый односторонний идеал главный, то $A \cong \mathrm{M}_n(R)$ для некоторых n и области R).

Алгоритмам построения разложений ассоциативных конечномерных алгебр в прямую сумму матричных алгебр (в том числе для алгебр над конечным полем, для конечных алгебр) посвящены работы [15,21—26,39,40]. Особо отметим свежий обзор [15].

В [16, 36, 41] получены теоретико-решёточные результаты характеризации колец матриц.

Критерии для распознавания колец суперматриц $\mathrm{Mat}(p, q)$, $\mathrm{Mat}(p, 0 \mid \Lambda)$, $\mathrm{Mat}(p, 1 \mid \Lambda)$ были получены в [11].

Изоморфизмы колец матриц $\Delta\colon \mathrm{M}_m(R) \to \mathrm{M}_n(S)$ над ассоциативными кольцами описаны (теорема Боллы [14], а также более общая теорема А. В. Михалёва [10,33] об изоморфизмах колец эндоморфизмов модулей, близких к свободным, градуированный случай см. в [2]). Строение антиизоморфизмов колец матриц над кольцами описывается теоремой К. И. Бейдара и А. В. Михалёва [4, 5, 33] (такие антиизоморфизмы индуцируются антиэквивалентностями Мориты, градуированный случай см. в [3]).

Конечно, если R и S — коммутативные кольца, то из существования изоморфизма $\Delta\colon \mathrm{M}_m(R) \to \mathrm{M}_n(S)$ следует, что кольца R и S изоморфны.

Довольно много статей содержат конкретные примеры, когда $\mathrm{M}_m(R) \cong \mathrm{M}_n(S)$, но $R \ncong S$, а также соответствующие рассмотрения для подколец колец матриц, в частности для треугольных матриц (см., например, статью [19], в которой $m = n = 2$ и кольца R и S являются некоммутативными нётеровыми областями).

Пример 3.9. Рассмотрим, как можно использовать условия (19) для распознавания матричной структуры алгебры A, предложенной в [34] в качестве возможного алгебраического носителя большой некоммутативной группы. Эта алгебра имеет базис e, i, j, k над некоторым конечным полем P, а умножение

в ней задаётся соотношениями

$$ei = ie = i, \quad ej = je = j, \quad ek = ke = k,$$
$$i^2 = j^2 = -\varepsilon e, \quad k^2 = -e,$$
$$ij = -ji = \varepsilon k, \quad ik = -ki = -j, \quad jk = -kj = i.$$

При этом $\operatorname{char} P = p > 2$, иначе алгебра A коммутативна. Из соображений размерности ясно, что указанная алгебра не может быть алгеброй матриц порядка $n > 2$, а при $n = 2$ соотношения (19) принимают вид $b^2 = 0$, $ab + ba = e$. Полагая $b = xe + yi + zj + wk$ и $a = x'e + y'i + z'j + w'k$, после несложных преобразований получаем, что $x = x' = 0$, а остальные переменные удовлетворяют уравнениям

$$w^2 = -\varepsilon(y^2 + z^2), \quad \varepsilon(yy' + zz') + ww' = \frac{1}{2}.$$

Легко убедиться, что при $\varepsilon = 0$ эта система уравнений несовместна, т. е. алгебра A не является матричной алгеброй. Напротив, при $\varepsilon \neq 0$ первое уравнение имеет решение с $w \neq 0$ (причём это решение можно найти непосредственно при $-\varepsilon \in (P^*)^2$ или с помощью в среднем около двух опробований случайно выбранных элементов простого подполя поля P, как показано в предыдущем разделе). Тогда второе уравнение линейно относительно y', z', w' и коэффициент при w' не равен 0, значит, оно имеет хотя бы одно решение. Итак, получен ещё один способ представления алгебры A в виде алгебры матриц.

Литература

[1] Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии. — М.: Гелиос АРВ, 2002.

[2] Балаба И. Н., Михалёв А. В. Изоморфизмы градуированных колец эндоморфизмов градуированных модулей, близких к свободным // Фундамент. и прикл. матем. — 2007. — Т. 13, вып. 5. — С. 3—18.

[3] Балаба И. Н., Михалёв А. В. Антиизоморфизмы градуированных колец эндоморфизмов градуированных модулей, близких к свободным // Фундамент. и прикл. матем. — 2008. — Т. 14, вып. 7. — С. 23—36.

[4] Бейдар К. И., Михалёв А. В. Антиизоморфизмы колец эндоморфизмов модулей и антиэквивалентности Мориты // УМН. — 1995. — Т. 50, № 1. — С. 191—192.

[5] Бейдар К. И., Михалёв А. В. Антиизоморфизмы колец эндоморфизмов модулей, близких к свободным, индуцированные антиэквивалентностями Мориты // Тр. семинара им. И. Г. Петровского. — 1996. — Вып. 19. — С. 338—344.

[6] Богданов И. И. Скрытые матричные полукольца // Фундамент. и прикл. матем. — 2003. — Т. 9, вып. 3. — С. 13—19.

[7] Вентцель Е. С. Теория вероятностей. — М.: Наука, 1969.

[8] Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Т. II. — М.: Гелиос АРВ, 2003.

[9] Лидл Р., Нидеррайтер Г. Конечные поля. — М.: Мир, 1988.

[10] Михалёв А. В. Изоморфизмы колец эндоморфизмов модулей, близких к свободным // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 1989. — № 2. — С. 20—27.

[11] Новиков М. И. Распознавание суперматриц: Курсовая работа студента 4-го курса механико-математического факультета МГУ (научный руководитель: проф. А. В. Михалёв). — М., 2009.

[12] Пирс Р. Ассоциативные алгебры. — М.: Мир, 1986.

[13] Agnarson G., Amitsur S. A., Robson J. C. Recognition of matrix rings. II // Israel J. Math. — 1966. — Vol. 96. — P. 1—13.

[14] Bolla M. L. Isomorphisms between endomorphism rings of progenerators // J. Algebra. — 1984. — Vol. 87. — P. 261—281.

[15] Bremmer M. R. How to compute the Wedderburn decomposition of a finite-dimensional associative algebra // Groups, Complexity, Cryptology. — 2011. — Vol. 3. — P. 47—66.

[16] Camillo V. P. Inducing lattice maps by semilinear isomorphisms // Rocky Mountain J. Math. — 1984. — Vol. 14. — P. 475—486.

[17] Chatters A. W. Representations of tiled matrix rings as full matrix rings // Math. Proc. Cambridge Phil. Soc. — 1989. — Vol. 105. — P. 67—72.

[18] Chatters A. W. Matrices, idealizers, and integer quaternions // J. Algebra. — 1992. — Vol. 150. — P. 45—56.

[19] Chatters A. W. Non-isomorphic rings with isomorphic matrix rings // Proc. Edinburgh Math. Soc. — 1993. — Vol. 36. — P. 339—348.

[20] Diffie W., Hellman M. E. New directions in cryptography // IEEE Trans. Inf. Theory. — 1976. — IT-22, No. 6. — P. 644—654.

[21] Eberly W. Decompositions of algebras over finite fields and number fields // Comput. Complexity. — 1991. — Vol. 1. — P. 183—210.

[22] Eberly W. Decompositions of algebras over R and C // Comput. Complexity. — 1991. — Vol. 1. — P. 214—234.

[23] Eberly W., Giesbrecht M. Efficient decomposition of associative algebras over finite fields // J. Symbolic Comput. — 2000. — Vol. 29. — P. 441—458.

[24] Eberly W., Giesbrecht M. Efficient decomposition of separable algebras // J. Symbolic Comput. — 2004. — Vol. 37. — P. 35—81.

[25] Eberly W., Giesbrecht M. Efficient decomposition of associative algebras // Proc. ISSAC '96. — New York: ACM, 1996. — P. 170—178.

[26] Friede K., Ronyai L. Polynomial time solutions of some problems in computational algebra // Proc. 17th Ann. ACM Symp. Theory Comp. — New York: ACM, 1985. — P. 153—162.

[27] Fuchs P. R. A characterization result for matrix rings // Bull. Austral. Math. Soc. — 1991. — Vol. 43. — P. 265—267.

[28] Fuchs P. R., Maxson C. J., Pilz G. F. On rings for which homogeneous maps are linear // Proc. Amer. Math. Soc. — 1991. — Vol. 112. — P. 1—7.

[29] Imai H., Matsumoto T. Algebraic methods for constructing asymmetric cryptosystems // Proc. of the 3rd Int. Conf. on Algebraic Algorithms and Error-Correcting Codes. — Berlin: Springer, 1985. — (Lect. Notes Comput. Sci.; Vol. 229). — P. 108—119.

[30] Lam T. Y. Modules with Isomorphic Multiples and Rings with Isomorphic Matrix Rings. A Survey. — Kundig, 1999. — (L'Enseignement Mathématique, No. 35).

[31] Lam T. Y., Leroy A. Recognition amd computations of matrix rings // Israel J. Math. — 1996. — Vol. 96. — P. 379—397.

[32] Levy I. S., Robson J. S., Stafford T. Hidden matrices // Proc. London Math. Soc. (2). — 1994. — Vol. 69. — P. 277—308.

[33] Mikhalev A. V. Isomorphisms and antiisomorphisms of endomorphism rings of modules // First Int. Tainan—Moscow Algebra Workshop. — Berlin: Walter de Gruyter, 1996. — P. 70—122.

[34] Moldovyan N. A., Moldovyan D. N. A new hard problem over non-commutative finite groups for cryptographic protocols // Computer Network Security, Proc. 5th Int. Conf. MMM-ACNS 2010. — Berlin: Springer, 2010. — (Lect. Notes Comput. Sci.; Vol. 6258). — P. 183—194.

[35] Nechaev A. A. Finite rings with applications // Handbook of Algebra. Vol. 5 / M. Hazewinkel, ed. — Elsevier, 2008. — P. 213—320.

[36] Von Neumann J. Continuous Geometry. — Princeton Univ. Press, 1960.

[37] Patarin J., Goubin L., Courtois N. C^*_{-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai // Advances in Cryptology — ASIACRYPT '98. — Berlin: Springer, 1998. — (Lect. Notes Comput. Sci.; Vol. 1514). — P. 35—50.

[38] Robson J. C. Recognition of matrix rings // Commun. Algebra. — 1991. — Vol. 19. — P. 2113—2124.

[39] Ronyai L. Simple algebras are difficult // Proc. 19th Ann. ACM Symp. Theory Comp. — New York: ACM, 1987. — P. 398—408.

[40] Ronyai L. Computing the structure of finite algebras // J. Symbolic Comput. — 1990. — Vol. 9. — P. 355—373.

[41] Stephenson W. Lattice isomorphisms between modules. I. Endomorphism rings // J. London Math. Soc. (2). — 1969. — Vol. 1. — P. 177—183.

[42] Wu Z., Ding J., Gower J. E., Ye D. Perturbed hidden matrix cryptosystems // Computational Science and Its Applications — ICCSA 2005. — Berlin: Springer, 2005. — (Lect. Notes Comput. Sci.; Vol. 3481). — P. 595—602.