УДК 512.74; 512.76; 681.3

Казакова О.Н., Пихтилькова О.А., Пихтильков С.А.
Оренбургский государственный университет
E-mail: olnikka@yandex.ru, OPikhtilkova@mail.ru, pikhtilkov@mail.ru

ОБ ОДНОЙ РЕАЛИЗАЦИИ ТОРИЧЕСКОЙ КРИПТОГРАФИИ

Наиболее популярными криптосистемами с открытым ключом являются: RSA-коды, шифросистема Эль-Гамаля, шифросистема Мак-Элиса и криптосистемы на эллиптических кривых.

В настоящее время эллиптическая криптография считается наиболее удачной системой, обеспечивающей хорошую криптостойкость при меньшей длине ключа.

Недавно появились работы по торической криптографии, где предложена новая шифросистема CEILIDH, основанная на алгебраических торах.

Групповой схемой называется группа в категории S-схем Гротендика.

Алгебраическая группа G над полем k – это групповая k-схема, гладкая и конечного типа над полем k.

Алгебраический тор – это алгебраическая группа над полем F_q, который над некоторым расширением поля изоморфен $(G_m)^d$, где G_m – мультипликативная группа поля $F_{q^n}^*$, и d является размерностью T. Если T изоморфно $(G_m)^d$ над полем F_{q^n}, говорят, что T разложимо над полем F_{q^n}.

Тор $T_n(F_q)$ имеет такую же криптостойкость, как мультипликативная группа $F_{q^n}^*$.

В работе рассмотрена шифросистема Эль-Гамаля для алгебраического тора $T_2(F_q)$.

Предположим, что целое число d является квадратичным невычетом в поле F_q. Тогда $F_{q^2} = F_q(\sqrt{d})$.

Определим отображение $\psi : A^1(F_q) \to T_2(F_q)$ одномерного аффинного пространства в мультипликативную группу $F_{q^2}^*$.

Положим $\psi(a) = \frac{a+\sqrt{d}}{a-\sqrt{d}}$. Обратное отображение определяется по формуле $\rho(\beta_1 + \beta_2\sqrt{d}) = \frac{1+\beta_1}{\beta_2}$.

Отображения ρ и ψ осуществляют рациональную параметризацию тора $T_2(F_q)$. С помощью них осуществляется кодирование и декодирование сообщений.

Ключевые слова: алгебраическая группа, алгебраический тор, торическая криптография.

1. Алгебраические группы

В этом разделе излагается теория групповых схем по Гротендику, которая обобщает хорошо известное определение группы в алгебре [5].

Для полноты изложения можно также ознакомиться с работами [8-15].

Пусть E – категория с нулевыми морфизмами. Ядром морфизма $f : A \to B$ называется морфизм $k : K \to A$ такой, что $f \circ k$ – нулевой морфизм и для любого морфизма $k' : K \to A$, удовлетворяющего условию $f \circ k'$ – нулевой, существует единственный морфизм $u : K' \to K$ такой, что $k \circ u = k'$.

Морфизм называется нормальным, если он является ядром некоторого морфизма.

Категория называется абелевой, если:

– в ней существует нулевой объект;

– существуют все бинарные произведения и копроизведения;

– все мономорфизмы и эпиморфизмы являются нормальными.

Абелева категория, обладающая семейством образующих и удовлетворяющая условиям:

– в категории существуют копроизведения (суммы) любых семейств объектов;

– для каждого направленного по возрастанию семейства подобъектов $(U_i, \mu_i), i \in I$ произвольного объекта A и подобъекта (V, σ) выполнено равенство

$$(\cup_{i \in I}(U_i, \mu_i)) \cap (V, \sigma) = \cup_{i \in I}((U_i, \mu_i) \cap (V, \sigma)),$$

– называется категорией Гротендика.

Ковариантный функтор $F : C \to D$ из категории C в категорию D – это отображение, которое

– сопоставляет каждому объекту $X \in C$ объект $F(X) \in D$,

– сопоставляет каждому морфизму $f : X \to Y$ в категории C морфизм $F(f) : F(X) \to F(Y)$.

Это сопоставление должно обладать следующими свойствами:

$$F(id_A) = id_{F(A)};$$
$$F(g \circ f) = F(g) \circ F(f).$$

Аналогичным образом определяется контравариантный функтор – это отображение объектов категорий, обращающее стрелки, то есть морфизму $f: X \to Y$ ставится в соответствие морфизм $F(f): F(Y) \to F(X)$, сохраняющее тождественные морфизмы и удовлетворяющее равенству

$$F(g \circ f) = F(f) \circ F(g).$$

Пусть E – некоторая категория, X – ее объект. Определим контравариантный функтор (предпучок) h_x на категории E со значениями в категории множеств, полагая $h_x(Y) = Hom(Y, X)$ – гомоморфизм из Y в X.

Множество $h_x(Y)$ также называется множеством точек объекта X и обозначается $X(Y)$.

Функтор h_x удовлетворяет следующим свойствам.

1) Всякий морфизм $f: X \to X'$ определяет естественное преобразование функтора h_x в функтор $h_{x'}$, то есть для каждого Z на E определено отображение $F(Z): X(Z) \to X'(Z)$ по правилу: пусть $\varphi \in Hom_E(Z, X)$, тогда $F(z)(\varphi) = f \circ \varphi$ и для каждого морфизма $g: Z \to Z'$ выполнено

$$h_{X'}(g) \circ f(Z) = f(Z') \circ h_X(g).$$

2) Всякое естественное преобразование функтора $h_x \to h_y$ определяется однозначно некоторым морфизмом $X \to Y$.

Следующие примеры указывают путь к определению групповой структуры на объектах произвольной категории.

Пример 1 ([5]). Объект X категории E, обладающий свойством, что множество $X(Y)$ состоит из одного элемента для любого Y, является аналогом «одной точки» (одноэлементного множества) категории E. Такой объект, если он существует, называется конечным или финальным объектом категории E.

Пример 2 ([5]). Пусть E – категория множеств и G – абстрактная группа. Множество G(Y) всех отображений Y в G снабдим структурой группы, полагая $(f \circ g)(y) = f(y)g(y)$ для всех $y \in Y, f, g \in G(Y)$.

Легко проверить, что множество $G(Y)$ является группой по отношению к операции «о».

Роль нейтрального элемента играет отображение e, определенное по правилу $e(y)=e$ для всех $y \in Y$, где e – нейтральный элемент группы G.

Обратный элемент определяется следующим образом $f^{-1}(y) = f(y)^{-1}$ для всех $y \in Y$.

Пусть $\varphi: Z \to Y$ – произвольное отображение множеств. Тогда отображение $\psi: G(Y) \to G(Z)$, определенное по правилу $\psi(f)(z) = (f \circ \varphi)(z)$, является групповым гомоморфизмом.

Функтор h_G обладает следующими двумя важными свойствами:

а) для любого множества Y объект $h_G(Y)$ есть группа;

б) для любого отображения $Z \to Y$ отображение $h_G(Z) \to h_G(Z)$ является гомоморфизмом групп.

Функтор h_G определяет также исходную групповую структуру. Если Y – одноточечное множество, то группа $G(Y)$ изоморфна группе G.

Пусть X – произвольное топологическое пространство, и пусть любому его открытому множеству U сопоставлено некоторое его множество $F(U)$, и для любых открытых множеств $U \subset V$ задано отображение $\rho_U^V: F(V) \to F(U)$. Эта система множеств и отображений называется предпучком, если выполнены следующие условия:

1) ρ_U^V – тождественное отображение;

2) для любых открытых множеств $U \subset V \subset W$ выполняется равенство $\rho_U^W = \rho_U^V \cdot \rho_V^W$;

3) $F(\varnothing)$ состоит из одного символа.

Пусть E – категория и F – контравариантный функтор на E со значениями в категории множеств.

Будем называть F предпучком групп на E, если для всех $y \in E$ множества $F(Y)$ снабжены групповой структурой так, что для всякого морфизма $f: X \to Y$ индуцированное отображение $F(f): F(Y) \to F(X)$ является групповым гомоморфизмом.

Если F и H – два предпучка групп на E, то назовем гомоморфизмом предпучка F в

H всякий морфизм $u: F \to H$ такой, что для каждого $y \in E$ отображение множеств $u(y): F(y) \to H(y)$ является гомоморфизмом групп.

Гомоморфизм предпучков F в H будем обозначать $Hom_{E-gr}(F,H)$.

Объект G категории E называется группой в E или групповым объектом, если функтор h_G есть предпучок групп в E.

Предпучок F на топологическом пространстве X называется пучком, если для любого открытого подмножества U в X и любого его открытого покрытия $U = \bigcup U_\alpha$ удовлетворяются следующие условия:

1) если $\rho^U_{U_\alpha} s_1 = \rho^U_{U_\alpha} s_2$ для $s_1, s_2 \in F(U)$ и для всех U_α, то $s_1 = s_2$.

2) если $s_\alpha \in F(U_\alpha)$ таковы, что $\rho^{U_\alpha}_{U_\alpha \cap U_\beta} s_\alpha = \rho_{U_\alpha \cap U_\beta} s_\beta$, то существует элемент $s \in F(U)$, для которого $s_\alpha = \rho^U_{U_\alpha} s$ для всех U_α.

Окольцованным пространством называется пара (X, O_X), состоящая из топологического пространства X и пучка колец O_X. Пучок O_X называется структурным пучком окольцованного пространства.

Пусть (X, O_X) и (Y, O_Y) – окольцованные пространства. Морфизмом $\varphi: (X, O_X) \to (Y, O_Y)$ окольцованных пространств называется совокупность, состоящая из непрерывного отображения $\varphi: X \to Y$ и гомоморфизмов колец $\psi_U : O_Y(U) \to O_X(U^*)$, где $U^* = \varphi^{-1}(U), U \subset Y$.

Схемой называется окольцованное пространство (X, O_X), любая точка которого имеет такую окрестность U, что окольцованное пространство (U, O_U), изоморфно *Spec A*, где *Spec A* – спектр некоторого коммутативного кольца.

Пусть S – фиксированная схема. Схемой над S или S-схемой Гротендика называется схема X, снабженная морфизмом $q: X \to S$.

Групповой схемой называется группа в категории S-схем Гротендика (см. [5], [6]).

Пусть R – коммутативное кольцо с 1, $S = Spec\ R$. Групповая S-схема G называется аффинной S-группой или R-группой, если $G = Spec\ A$, где A есть R-алгебра. Аффинную R-группу G можно также определить как групповой объект в категории R-схем.

Пример (мультипликативная группа G_m). Для всякого коммутативного кольца B положим $G_m(B) = G^*$, где B^* – мультипликативная группа обратимых элементов в B. Функтор G_m представим аффинной схемой $SpecZ[T, T^{-1}]$, так как

$$Hom_{ring}(Z[T, T^{-1}], B) = B^*.$$

Алгебраическая группа G над полем k – это групповая k-схема, гладкая и конечного типа над полем k.

Примеры.

Все классические группы матриц являются алгебраическими:

1. $GL_n(R)$, $GL_n(C)$ – невырожденные матрицы порядка $n \times n$;

2. $SL_n(R)$, $SL_n(C)$ – матрицы с определителем, равным единице;

3. $SO_n(R)$ – ортогональные матрицы, то есть матрицы, удовлетворяющие условию $UU^T = E$.

2. Алгебраические торы

Определение 1 ([5]). Групповая k-схема T называется алгебраическим тором, если $T \otimes_k \bar{k} = D_{\bar{k}}(Z^n)$.

Пусть T – k-тор, разложимый над расширением Галуа L/k, $\Pi = \mathrm{Gal(L/k)}$, $(\mathrm{L{:}k}) < \infty$. Тогда для всякой k-алгебры A выполнено

$$T(A) = Hom(T, (A \otimes_k L)^*) =$$

$$= [Hom(T, Z) \otimes_Z (A \otimes_k L)^*]^\Pi.$$

Следующее определение алгебраического тора эквивалентно определению 1.

Определение 2 ([4]). Алгебраический тор – это алгебраическая группа над полем F_q, которая над некоторым расширением поля изоморфен $(G_m)^d$, где G_m – мультипликативная группа поля $F^*_{q^n}$, и d является размерностью T. Если T изоморфно $(G_m)^d$ над полем F_{q^n}, говорят, что T разложимо над полем F_{q^n}.

Примеры.

1. Если $d=1$, то тор T изоморфен мультипликативной группе $G_m = K^*_V$ для некоторого поля K. Следовательно, мультипли-

кативная группа K^* является тором размерности 1. В частности, торами размерности 1 являются группы R^* и C^*.

2. Группы целочисленных автоморфизмов квадратичных форм над Z являются алгебраическими торами размерности 4 [7]:

$$C_4 : x_1^2 + x_2^2 + x_3^2 + x_4^2;$$

$$S_4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 - x_1x_2 - x_2x_3 - x_3x_4.$$

Пусть k= F_q и L= F_{q^n}. Обозначим через $\mathrm{Re}s_{L/k}$ ограничения Вейля скаляров из L на k. Тогда $\mathrm{Re}s_{L/k}G_m$ является тором.

Имеет место следующий изоморфизм

$$(\mathrm{Re}s_{L/k}G_m)(k) \cong G_m(L) = L^*,$$

где L^* – мультипликативная группа поля L.

Если $k \subset F \subset L$ – расширения полей, получаем следующее нормальное отображение $\mathrm{Re}s_{L/k}G_m \to \mathrm{Re}s_{F/k}G_m$, которое обозначается $N_{L/F}$.

Определим алгебраический тор T_n как пересечение ядер нормальных отображений $N_{L/F}$ для всех подполей $k \subset F \subsetneq L$.

Размерность T_n равна $\varphi(n)$, где $\varphi(n)$ – функция Эйлера.

Группа $T_n(F_q)$ – это подгруппа мультипликативной группы $F_{q^n}^*$. Следующая лемма отождествляет группу $T_n(F_q)$ с циклическими подгруппами $G_{q,n} \subset F_{q^n}^*$ порядка $\Phi_n(q)$, где $\Phi_n(q)$ – многочлен деления круга, и показывает, что секретность криптографических систем, построенных на группе T_n основана на мультипликативной группе $F_{q^n}^*$, а не на группе меньшего поля.

Лемма 1.2.1 ([4]).

i) $T_n(F_q) \approx G_{q,n}$.

ii) $\left|T_n(F_q)\right| = \Phi_n(q)$.

iii) Если $h \in T_n(F_q)$ – элемент простого порядка, не делящего n, то тогда h не лежит в собственном подполе расширения F_{q^n}/F_q.

3. Рациональная параметризация алгебраических торов

Определение. Пусть T – алгебраический тор над F_q размерности d. Тор T называется рациональным, если существует бирациональное отображение $\rho : T \to A^d$. Другими словами, тор T – рационален, если существуют открытые множества $W \subset T$ и $U \subset A^d$ и рациональные функции

$$\rho_1,...,\rho_d \in F_q(x_1,...,x_t) \text{ и } \psi_1,...,\psi_t \in F_q(y_1,...,y_d)$$

такие, что отображения

$$\rho = (\rho_1,...,\rho_d) : W \to U \text{ и } \psi = (\psi_1,...,\psi_t) : U \to W$$

являются обратными гомеоморфизмами.

Гипотеза Воскресенского ([5]). Тор T_n является рациональным.

Гипотеза справедлива, если n является степенью простого числа или произведением двух степеней простых чисел [5].

Пример ([3]). Рассмотрим рациональную параметризацию тора $T_6(F_q)$.

Зафиксируем $x \in F_{q^2}/F_q$.

Тогда $F_{q^2} = F_q(x)$. Выберем базис $\alpha_1,\alpha_2,\alpha_3$ поля F_{q^3}.

Тогда множество

$$\{\alpha_1,\alpha_2,\alpha_3,x\alpha_1,x\alpha_2,x\alpha_3\}$$

является базисом F_{q^6}.

Пусть $\sigma \in Gal(F_{q^6}/F_q)$ является элементом порядка 2.

Определим взаимно однозначное отображение $\psi_0 : A^3(F_q) \to F_{q^6}^*$ по формуле

$$\psi_0(u_1,u_2,u_3) = \frac{\gamma + x}{\gamma + \sigma(x)},$$

где $\gamma = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3$.

Тогда $N_{F_{q^6}/F_{q^3}}(\psi_0(u)) = 1$ для всех $u = (u_1,u_2,u_3)$.

Из теоремы Гильберта следует, что отображение ψ_0 является гомеоморфизмом.

Рассмотрим рационализацию для конкретного q.

Пример ([5]). Пусть $q \equiv 2 (\mathrm{mod}\, 9)$. Выберем $x = \zeta_3$ и $y = \zeta_9\zeta_9^{-1}$.

Тогда

$$F_{q^6} = F_q(\zeta_9), F_{q^2} = F_q(x), F_{q^3} = F_q(y).$$

Возьмем базис $\{1, y, y^2 - 2\}$ для F_{q^3}.

Пусть $\alpha = (0,0,0)$.

Значит, $\psi_0(\alpha) = \zeta_3^2$.

Рассмотрим отображение

$$f(v_1,v_2) = 1 - v_1^2 - v_2^2 + v_1v_2.$$

Следовательно,

$$\psi(v_1,v_2) = \frac{1 + v_1y + v_2(y^2-2) + f(v_1,v_2)x}{1 + v_1y + v_2(y^2-2) + f(v_1,v_2)x^2}.$$

Для $\beta=\beta_1+\beta_2 x\in T_6(F_q)/\{1,\zeta_3^2\}$ получим

$$\rho(\beta)=\left(\frac{u_2}{u_1},\frac{u_3}{u_1}\right),$$

где $\frac{1+\beta_1}{\beta_2}=u_1+u_2y+u_3(y^2-2)$.

Отображения ρ и ψ являются обратными бирациональными отображениями между T_6 и A^2.

4. Криптография, основанная на алгебраических торах

Криптосистема основанная на алгебраических торах T_6, называется CEILIDH [4].

Согласно лемме 1.2.1, тор $T_n(F_q)$ имеет такую же криптостойкость, как мультипликативная группа $F_{q^n}^*$.

Обозначим через F_{q^r} конечное поле из q^r, где q – простое. В работе рассмотрена шифросистема Эль-Гамаля для алгебраического тора $T_2(F_q)$.

Эта шифросистема реализована на компьютере на алгоритмическом языке C#. Простое число q выбирается так, чтобы $2\ln q\approx 1024$ и $(q+1)$ имело простой делитель порядка 160 бит.

Предположим, что целое число d является квадратичным невычетом в поле F_q. Тогда $F_{q^2}=F_q(\sqrt{d})$.

Определим отображение

$$\psi: A^1(F_q)\to T_2(F_q)$$

одномерного аффинного пространства в мультипликативную группу $F_{q^2}^*$.

Положим $\psi(a)=\frac{a+\sqrt{d}}{a-\sqrt{d}}$. Обратное отображение определяется по формуле $\rho(\beta_1+\beta_2\sqrt{d})=\frac{1+\beta_1}{\beta_2}$.

Отображения ρ и ψ являются взаимообратными отображениями множеств $A^1\setminus\{0\}$ и $T_2\setminus\{\pm1\}$.

Для q=2081 порядок группы T_2 равен $\Phi_2(2081)=2082=2\cdot3\cdot347$, где $\Phi_n(n)$ – многочлен деления круга на n частей.

Пусть α – элемент порядка $l=347$ в T_2. Для его нахождения обычно достаточно возвести элемент T_2 в степень $\frac{q^2-1}{l}$. В нашем примере это элемент $\psi(1)^{12480}$.

Абонент А выбирает число a: $1\le a<l-1$ и вычисляет $\beta=a^\alpha$.

Абонент Б выбирает случайное число $1\le k<l-1$.

Пусть M – сообщение, M –целое число и $1\le M<q-1$. Абонент Б вычисляет $\gamma=\rho(\alpha^k)$, $\delta=\rho(\psi(M))$ и посылает шифротекст (γ,δ).

Нетрудно понять, что посылаемый шифротекст в 2 раза длиннее исходного сообщения. В этом состоит особенность шифросистемы Эль-Гамаля, которая компенсируется тем, что торическая криптосистема предлагает меньшую длину ключа по сравнению с другими системами с открытым ключом, за исключением эллиптической криптографии.

Открытым ключом является набор (q,α,β), секретным ключом является a.

Абонент А декодирует сообщение по формуле $\rho(\psi(\delta)\psi(\gamma)^{-a}$.

В работе указано, в отличие от [4], явное преобразование сообщения M в элемент группы T_2.

В программе описан следующий класс, реализующий элементы поля $F_{q^2}=F_q(\sqrt{d})$.

```
public class Fq
{
private int a, b, q = 2081;
public Fq(int a, int b)
{
this.a = a; this.b = b;
}
public string ToString (string format)
{
return Convert.ToString(a) + «+sqr(3)»
+ Convert.ToString(b);
}
```

С помощью перегрузки операторов реализованы операции сложения, умножения и деления классов.

```
public static Fq operator + (Fq x, Fq y)
{
int c=(x.a+y.a)%x.q;
int d=(x.b+y.b)%x.q;
return new Fq(c,d);
}
public static Fq operator *(Fq x, Fq y)
{
```

```
int c = (x.a * y.a + 3 * x.b * y.b + x.q * x.q) %
x.q;
int d = (x.a * y.b + x.b * y.a + x.q * x.q) %
x.q;
return new Fq(c, d);
}
public static Fq operator /(Fq x, Fq y)
{
Fq ys = new Fq(y.a, -y.b);
int Dn = (y.a * y.a – 3 * y.b * y.b + x.q * x.q)
% x.q;
Fq Nm = x * ys;
int c = (Nm.a * MultObr(Dn, x.q)+x.q *
x.q) % x.q;
int d = (Nm.b * MultObr(Dn, x.q)+x.q *
x.q) % x.q;
return new Fq(c, d);
}
```

Использован стандартный алгоритм нахождения линейного представления наибольшего общего делителя, с помощью которого находится мультипликативный обратный.

Следующие программы реализуют операторы $\rho(\beta_1+\beta_2\sqrt{d})=\frac{1+\beta_1}{\beta_2}$ и $\psi(a)=\frac{a+\sqrt{d}}{a-\sqrt{d}}$.

```
public static int Rho(Fq x)
{
int y = ((1 + x.a) * MultObr(x.b, x.q)+ x.q
* x.q) % x.q;
return y;
}
public static Fq Psi(int a)
{
Fq x = new Fq(a,1);
Fq y = new Fq(a, -1);
Fq z = x / y;
return z;
}
```

Для возведения класса в степень используется стандартный алгоритм.

Следующие операторы осуществляют кодирование-декодирование сообщения.

```
Fq s = Psi(1);
Fq alpha = Form1.Pow(s, 12480);
Fq st = Form1.Pow(alpha, 347);
int a = 5;
int Pa = Fq.Rho(Form1.Pow(alpha, a));
Random rnd = new Random();
int k = rnd.Next(0,2080);
int gamma = Fq.Rho(Form1.Pow(alpha,
k));
byte[] bytes = System.Text.Encoding.
ASCII.GetBytes(textBox1.Text);
n = bytes.Length;
int M = 0;
for (i = 0; i < n; i++)
{
if (bytes[i] == Convert.ToByte(48))
M = 2 * M;
if (bytes[i] == Convert.ToByte(49))
M = 2 * M+1;
};
Fq MFq = Psi(M);
int delta = Fq.Rho(MFq*Form1.Pow
(Psi(Pa), k));
Fq DMFq = Psi(delta) * Form1.Pow(Psi
(gamma), 347 – a);
int DM = Fq.Rho(DMFq).
```

18.01.2015

Список литературы:

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. Учебное пособие. 2-е изд. исправленное и дополненное.– М.: Гелиос АРВ.– 2002. 480 с.
2. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы.– М.: КомКнига.– 2006. 328 с.
3. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых.– М.: КомКнига.– 2006. 280 с.
4. Rubin K., Silverberg A. Torus-based cryptography // Advances of Cryptology.– 2003.– P. 349-365.
5. *Воскресенский В.Е.* Алгебраические торы.– М.: Наука.– 1977. 223 с.
6. *Воскресенский В.Е.* Бирациональная геометрия линейных алгебраических групп. – М. : МЦНМО.– 2009. 404 с.
7. *Крутиков Ю.Ю., Попов С.Ю.* Когомологические бирациональные инварианты четырехмерных алгебраических торов// Вестник СамГУ – естественнонаучная серия.– 2011.– № 2.– С. 26-37.
8. *Грехов М.В.* Модель Нерона двумерных анизотропных алгебраических торов над локальными полями // Вестник СамГУ – естественнонаучная серия.– 2012.– № 9.– С. 31-40.
9. Исковских В.А., Куликов В.С., Прохоров Ю.Г., Чельцов И.А. Алгебраические поверхности: геометрия и арифметика. – М. : МЦНМО.– 2012. 356 с.
10. Итоги науки и техники / Рос. акад. наук, Всесоюз. ин-т науч. и техн. информ . – М. : ВИНИТИ, 2001. – (Современная математика и ее приложение / под ред. Р. В. Гамкрелидзе). Т. 70 : Алгебраическая геометрия. – 2001. – 264 с.

11. Итоги науки и техники / Рос. акад. наук, ВИНИТИ . – М. : ВИНИТИ, 2002– (Современная математика и ее приложения / ред. Р. В. Гамкрелидзе). Т. 100 : Алгебраическая геометрия.– 2006. – 248 с.
12. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. – М. : Мир.– 2000. 687 с.
13. Харрис Д. Алгебраическая геометрия.– М.: МЦНМО.– 2005. – 400 с.
14. Хартсхорн Р. Алгебраическая геометрия.– Новокузнецк: Изд-во НФМИ.– 2000. – Т. 1 . 368 с.
15. Шафаревич И. Р. Основы алгебраической геометрии.– М.: МЦНМО.– 2007. 589 с.

Сведения об авторах

Казакова Ольга Николаевна, доцент кафедры геометрии и компьютерных наук Оренбургского государственного университета, кандидат педагогических наук
460018, г. Оренбург, пр. Победы, 13, ауд. 1503; тел.: (3532)37-25-39; e-mail: ais@mail.osu.ru

Пихтилькова Ольга Александровна, доцент кафедры алгебры и математической кибернетики, Оренбургского государственного университета, кандидат физико-математических наук, доцент.
460018, г. Оренбург, пр. Победы, 13, ауд. 1410; тел.: (3532)37-25-35; e-mail: mathcyb@mail.osu.ru.

Пихтильков Сергей Алексеевич, профессор кафедры алгебры и математической кибернетики Оренбургского государственного университета, доктор физико-математических наук, профессор.
460018, г. Оренбург, пр. Победы, 13, ауд. 1410; тел.: (3532)37-25-35; e-mail: mathcyb@mail.osu.ru.