**УДК 511.6**

# ОБ АЛГОРИТМИЧЕСКИХ И ВЫЧИСЛИТЕЛЬНЫХ АСПЕКТАХ ОДНОГО МЕТОДА ТЕОРИИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

***Виноградова Т.А.***

*Воронежский институт МВД России, Воронеж, Россия*

В работе рассмотрен метод комплексного умножения Дойринга. В его рамках приведён алгоритм генерации эллиптических кривых, на использовании которых основаны многие методы современной криптографии. Рассмотрено обобщение метода комплексного умножения и разработан общий алгоритм для случая гиперэллиптических кривых рода 2. Основной результат состоит в обосновании выбора одного из параметров алгоритма – подходящего простого числа по методу Вейля.

*КЛЮЧЕВЫЕ СЛОВА*: эллиптические кривые, комплексное умножение, метод Дойринга, криптография.

# ПРО АЛГОРИТМІЧНІ І ОБЧИСЛЮВАЛЬНІ АСПЕКТИ ОДНОГО МЕТОДУ ТЕОРІЇ ЕЛІПТИЧНИХ КРИВИХ

***Віноградова Т.А.***

В роботі розглянуто метод комплексного множення Дойрінга. В його рамках приведений алгоритм генерації еліптичних кривих, на використанні яких засновані багато методів сучасної криптографії. Розглянуто узагальнення методу комплексного множення і розроблений загальний алгоритм для випадку гіпереліптичних кривих роду 2. Основний результат полягає в обгрунтуванні вибору одного з параметрів алгоритму - підходящого простого числа за методом Вейля.

*КЛЮЧОВІ СЛОВА*: еліптичні криві, комплексне множення, метод Дойрінга, криптографія.

# ON ALGORITHMIC AND COMPUTATIONAL ASPECTS OF THE THEORY OF ELLIPTIC CURVES METHOD

***Vinogradova T.A.***

The paper presents the Deuring method of complex multiplication. Within its frameworks the algorithm for generating elliptic curves which are used in many techniques of modern cryptography is given. A generalization of the method of complex multiplication is considered and a general algorithm for the case of hyper elliptic curves of kind 2 is developed. The main result is the justification for choosing one of the parameters of the algorithm - a suitable prime Weil method.

*KEY WORDS*: elliptic curves, complex multiplication method Deuring, cryptography.

**1. Введение. Анализ наиболее существенных результатов и публикаций по теме работы.** В настоящее время продолжает расти спрос на эффективные методы защиты передаваемых данных [1–18]. Начиная с 1976 года, в котором У. Диффи и М. Хеллман опубликовали работу «Новые направления в криптографии», положившую начало криптографии с открытым ключом (асимметричным методам шифрования), было разработано множество алгоритмов генерации, обмена и хранения ключей. Один из подходов к созданию таких процедур состоит в использовании проблемы факторизации больших целых чисел. Другой способ основан на проблеме дискретного логарифма (*DL*), состоящей в том, что в некоторых группах при относительно легком осуществлении операции возведения в степень (нахождения $b = a^n$, $a \in G$, $n \in \mathbb{Z}$), обратная операция логарифмирования (отыскания числа $n = log_a(b)$) достаточно трудоемка. Для стойкости *DL*-криптосистемы в конечной абелевой группе требуется, чтобы порядок группы был либо простым, либо «почти простым» (произведением достаточно большого простого числа и небольшого целого).

В качестве исходной конечной группы можно взять множество точек абелева многообразия над конечным полем (это конечная абелева группа, сложение в которой задаётся посредством рациональных функций). Если группа $\mathcal{A}(\mathbb{F}_q)$ абелева многообразия $\mathcal{A}$ является подходящей для *DL*-систем, то $\mathcal{A}$ также называется подходящим. Для применения таких многообразий в криптографии необходимы методы их генерации, а также наличие процедур быстрого сложения на них. Подходящим

абелево многообразие будет в случае, когда оно является многообразием Якоби $J_C$ некоторой кривой $C$. Тогда группа $J_C(\mathbb{F}_q)$ совпадает с группой классов $\mathbb{F}_q$-рациональных дивизоров кривой, и сложение на $J_C(\mathbb{F}_q)$ задается посредством сложения в группе классов дивизоров, тогда как в общем случае сложение на абелевом многообразии осуществляется достаточно сложно. Поэтому проблема реализации подходящего многообразия трансформируется в задачу реализации соответствующей кривой. В [13] выведены формулы быстрого сложения на многообразиях Якоби кривых рода 2.

Таким образом, возникает необходимость в методах построения эллиптических и гиперэллиптических кривых, заведомо обладающих требуемыми свойствами, например, имеющих подходящий порядок многообразия Якоби. Метод комплексного умножения Дойринга (*CM*-метод) является более выигрышным по времени в сравнении со случайным выбором кривой. Он позволяет построить кривую с заданным порядком группы точек (в случае рода 1) или многообразия Якоби (в случае рода 2).

В работе рассмотрен метод комплексного умножения Дойринга. В его рамках приведён алгоритм генерации эллиптических кривых, на использовании которых основаны многие методы современной криптографии. Рассмотрено обобщение метода комплексного умножения и разработан общий алгоритм для случая гиперэллиптических кривых рода 2. Основной результат состоит в обосновании выбора одного из параметров алгоритма – подходящего простого числа по методу Вейля.

**2. Метод Дойринга.** *CM*-метод Дойринга (*M. Deuring*) основан на теории комплексного умножения и теории полей классов мнимых квадратичных полей. Он позволяет построить эллиптическую кривую с заданным порядком группы точек, определённую над конечным полем.

Пусть $E$: $y^2=x^3 + ax + b$; $a, b \in K$ – эллиптическая кривая над $K$, где $K$ – числовое поле. Применим к $E$ отображение редукции по модулю простого $\mathfrak{p} \in \mathcal{O}_K$, лежащего над $p$. Пусть $\tilde{a}, \tilde{b}$ – образы чисел $a, b$, лежащие в конечном поле $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Если при этом выполняется условие $\Delta = -16(4\tilde{a}^3 + 27\tilde{b}^2) \neq 0$, то редуцированная кривая $\tilde{E}: y^2 = x^3 + \tilde{a}x + \tilde{b}$ является эллиптической над $\mathbb{F}_\mathfrak{p}$. В данном случае говорят, что кривая $E$ обладает «хорошей редукцией».

**Теорема** (Дойринга о подъёме). *Пусть $E$ – эллиптическая кривая, определённая над простым полем $\mathbb{F}_p$ и обладающая нетривиальным эндоморфизмом $\psi$. Тогда найдутся эллиптическая кривая $E'$, определённая над числовым полем $K$, эндоморфизм $\psi'$ и хорошая редукция $\tilde{E}$ кривой $E'$ в точке $\mathfrak{p}$, лежащей над $p$, такие, что $\tilde{E}' \cong E$, и $\tilde{\psi}'$ под действием изоморфизма переходит в $\psi$.*

Таким образом, отображение редукции индуцирует изоморфизм $End_K(E) \cong End_{\mathbb{F}_p}(E)$. Поэтому каждую эллиптическую кривую над конечным полем $\mathbb{F}_p$ можно рассмотреть как редукцию некоторой эллиптической кривой, определённой над заданным алгебраическим числовым полем $K$ и обладающей тем же самым кольцом эндоморфизмов.

Из теоремы Дойринга (с учётом свойств эндоморфизма Фробениуса) следует, что если $E$ – эллиптическая кривая с комплексным умножением на $\mathcal{O}_D$ (здесь $\mathcal{O}_D$ – порядок в числовом поле $K$), то для группы точек редуцированной кривой выполняется соотношение $|E(\mathbb{F}_p)| = p + 1 - (\omega + \bar{\omega})$, где простое число $p = \omega\bar{\omega}$ разлагается в произведение двух простых элементов из $\mathcal{O}_D$.

**3. Алгоритм генерации эллиптических кривых.** В 1986 году Эткин (*A.O.L.Atkin*) предложил алгоритм нахождения конечной группы, заведомо подходящей для применения в криптографических алгоритмах, взяв за основу *CM*-метод Дойринга [2].

Идея алгоритма состоит в следующем: выбирается мнимое квадратичное числовое поле $K$ и целое число $\omega \in \mathcal{O}_K$, такое, чтобы выполнялось $\omega\bar{\omega} = p$ для некоторого подходящего простого $p$ (здесь $\mathcal{O}_K$ – максимальный порядок в $K$). В этом случае $\omega$ соответствует эндоморфизму Фробениуса $\pi_p$ эллиптической кривой $E$ с комплексным умножением и кольцом эндоморфизмов $\mathcal{O}_K$. При подстановке $x = 1$ в характеристический многочлен эндоморфизма Фробениуса $f_p(x) = (x - \omega)(x - \bar{\omega})$ получаем число $\mathbb{F}_p$ -рациональных точек кривой $E$. Для построения соответствующей кривой $E$ над $\mathbb{F}_p$ сначала вычисляются инварианты $j_1, \ldots, j_h$ группы классов поля $K$. Они и являются $j$-инвариантами сопряженных над $K$ эллиптических кривых $E_j/K(j)$. Согласно теории комплексного умножения, инварианты являются целыми алгебраическими числами, и числовое поле $K(j)$ представляет собой гильбертово поле классов. Поэтому коэффициенты полинома Гильберта $H(x) = \prod_{i=1}^{h}(x - j_i)$ – целые, и редуцированные инварианты $j_{(p)}$, однозначно определяющие кривую $E_{j(p)}$ над полем $\mathbb{F}_p$, будут корнями полинома $H_p(x)=H(x) \ mod \ p$. Путем возведения точки $P \ E_j(p) \in (\mathbb{F}_p)$ в степень $N_p = f_p(1)$ определяется нужная кривая.

*Замечание*. Порядок $\mathcal{O}$ в мнимом квадратичном числовом поле $K$ – подкольцо с единицей поля $K$, такое что $\mathcal{O}$ является конечно порожденным $\mathbb{Z}$-модулем, содержащим $\mathbb{Q}$-базис поля $K$. Кольцо алгебраических целых элементов $\mathcal{O}_K$ поля $K$ также носит название максимального порядка.

Рассмотрим теперь эллиптическую кривую $E$ / $\mathbb{C}$ и отображение

$\varphi_n$: $E \to E$, $P \to nP$, $n \in \mathbb{Z}$, а также инъективное отображение
$\varphi$: $\mathbb{Z} \to End(E)$, $n \to \varphi_n$. Если рассмотреть $\varphi$ как биекцию на свой образ, то можно считать, что $\mathbb{Z} \subset End(E)$. Говорят, что эллиптическая кривая $E$ обладает комплексным умножением, если $\mathbb{Z} \subset End(E)$ и $\mathbb{Z} \neq End(E)$, то есть существует эндоморфизм $\psi \neq \phi_n$ для всех $n \in \mathbb{Z}$.

Известно, что кольцо эндоморфизмов эллиптической кривой представляет собой одно из следующих колец:

1) $\mathbb{Z}$;

2) $\mathbb{Z} + f\,\mathcal{O}_K$, $f > 0$, $f \in \mathbb{Z}$, то есть является порядком в мнимом квадратичном числовом поле;

3) $End(E) \otimes \mathbb{Q} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta, \alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2 < 0, \beta^2 < 0, \beta\alpha = -\alpha\beta$.

Перейдём теперь к описанию алгоритма построения подходящей эллиптической кривой. Он имеет следующую структуру:

1. Вычисление полинома Гильберта. Выбирается мнимое квадратичное поле $K$ / $\mathbb{Q}$ ($K \neq \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$) с максимальным порядком $\mathcal{O}_K$ и дискриминантом $D_K$.

1.1. Нахождение всех представителей классов идеалов в $\mathcal{O}_K$ (учитывая тот факт, что группа классов идеалов изоморфна группе классов квадратичных форм):

$$a_i = a\mathbb{Z} + \frac{-b + \sqrt{D_K}}{2}\mathbb{Z}.$$

1.2. Вычисление $\tau_i = \dfrac{-b + \sqrt{D_K}}{2}$, $i = 1,\ldots,h_K$, $\tau_i \in H$, где
$H = \{z \in \mathbb{C}: Im\ z > 0\}$ – верхняя полуплоскость Зигеля.

1.3. Вычисление $j(\tau_i)$ с заданной точностью.

1.4. Нахождение полинома Гильберта с заданной точностью:

$$H_{D_K}(X) = \prod_{i=1}^{h_K}(x - j(\tau_i)).$$

Коэффициенты многочлена должны быть целыми, поэтому округляем их.

Заметим, что значения $j(\tau_i)$ – это комплексные числа, представленные с некоторым округлением. Как правило, точность вычислений должна быть не хуже нескольких десятков десятичных знаков. Найти, какое именно алгебраическое число представляет приближенное значение $j(\tau_i)$, сложно. Поэтому сначала по приближенным значениям составляется полином Гильберта $H_{D_K}(X)$, затем его коэффициенты округляются до целых чисел, и находятся алгебраические числа, являющиеся корнями полинома классов, то есть алгебраические $j$-инварианты.

2. Определение подходящего простого числа.

Подбирается простое число $p$, удовлетворяющее условию $p = \omega\overline{\omega}$. Другими словами, должно выполняться равенство $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, где идеалы $\mathfrak{p} = (\omega)$ и $\overline{\mathfrak{p}} = (\overline{\omega})$ являются главными. Подходящим порядком группы в этом случае будет либо $n_1 = (1 - \omega)(1 - \overline{\omega})$, либо $n_2 = (1 + \omega)(1 + \overline{\omega})$.

Заметим, что в гильбертовом поле классов найдётся идеал $P$ такой, что $P \mid \mathfrak{p}$ и $\mathfrak{p}$ тотально расщеплён. Это можно сделать, поскольку группа классов конечна, а из теоремы Чеботарёва [26] следует бесконечность множества таких простых $\mathfrak{p}$, которые были бы тотально расщепленными. Кроме того, простой идеал тотально расщеплен в гильбертовом поле классов в том и только том случае, когда является главным. По теореме Дойринга для каждой эллиптической кривой над $H_K$ с комплексным умножением и кольцом эндоморфизмов $\mathcal{O}_K$ выполняется $End(E\ mod\ P) \cong \mathcal{O}_K$, так что редуцированная кривая также будет обладать комплексным умножением.

3. Определение уравнения кривой.

3.1. Находим $j := H_{D_K}(x)\ mod\ p, j \in \mathbb{F}_p$.

3.2. Проверяем, имеет ли кривая
$E_1: y^2 = 4x^3 - kx - k$ $(y^2 = 4x^3 - kc^2x - kc^3)$
требуемое число $n_1$ ($n_2$) точек, где $c$ – квадратичный невычет по модулю $p$, $k = \dfrac{27j}{j - 1728}$.

**4. Обобщённый алгоритм генерации гиперэллиптических кривых.** Естественным образом возникает вопрос построения подходящего для *DL* - систем многообразия Якоби кривой рода 2, поскольку в этом случае проблема дискретного логарифма представляется весьма сложной. Здесь его уже нельзя отождествить с группой точек кривой. Для обобщения метода Дойринга используется теория Шимуры – Таниямы комплексного умножения абелевых многообразий. Многообразие Якоби кривой рода 2 является группой классов дивизоров степени нуль $Pic_C^0$, а, с другой стороны, это – главно поляризованное абелево многообразие $J_C$ размерности 2, см. [13]. Кроме того, оно обладает структурой аналитического многообразия, являясь комплексным тором $T = \mathbb{C}^2/\Lambda$. Другими словами, имеет место изоморфизм $J_C \cong Pic_C^0 \cong \mathbb{C}^2/\Lambda$. Кольцо эндоморфизмов многообразия Якоби кривой рода 2 является максимальным порядком в $CM$-поле степени 4 над полем рациональных чисел (мнимом квадратичном расширении тотально действительного числового поля).

Простое абелево многообразие $\mathcal{A}$ обладает комплексным умножением, если $End_K(\mathcal{A}) \otimes \mathbb{Q}$ содержит числовое поле $F$ степени не больше $2dim(\mathcal{A})$ над $\mathbb{Q}$. Если $[F : \mathbb{Q}] = 2dim(\mathcal{A})$, то оно является полем $CM$-типа, то есть мнимым квадратичным расширением тотально действительного поля $F_0$ (это означает, что всякое вложение $F_0$ в $\mathbb{C}$ лежит в $\mathbb{R}$, и ни одно из вложений $F$ в $\mathbb{C}$ не лежит в поле $\mathbb{R}$). При этом
$F = End_K(\mathcal{A}) \otimes \mathbb{Q}$. Если $char(K) = 0$, то $End_K(\mathcal{A})$ является порядком в числовом поле $F$.

Пусть абелево многообразие $F$ определено над полем $\mathbb{C}$, обозначим $\mathcal{A}^* := Pic^0(\mathcal{A})$. Для каждого

абелева многообразия существует поляризация, т.е. изогения $\varphi$: $\mathcal{A} \to \mathcal{A}^*$. Если $\varphi$ изоморфизм, то многообразие называется главно поляризованным.

**5. Описание основного алгоритма.** Рассмотрим обобщение алгоритма генерации кривых для случая, когда их род равен двум. Алгоритм в данном случае имеет следующую структуру:

**5.1.** ***Выбор CM-поля, нахождение подходящего простого числа p и возможных порядков группы точек многообразия Якоби гиперэллиптической кривой.*** Фиксируется *CM*-поле степени 4 над $\mathbb{Q}$ и подбирается простое число $p = \omega\bar{\omega}$. Известно, что, поскольку $\mathcal{A}$ обладает комплексным умножением на $End(\mathcal{A}) = \mathcal{O}_K$, существует определенное над $\mathbb{F}_p$ простое главно поляризованное абелево многообразие $\mathcal{A}$ с кольцом эндоморфизмов $\mathcal{O}_K$ и элементом Фробениуса $\omega \in \mathcal{O}_K$. Оно и является многообразием Якоби $J_C$ кривой $C$ рода 2 над $\mathbb{F}_p$. Поскольку $dim(\mathcal{A}) = 2$, то при подстановке $x = 1$ в характеристический многочлен $f_p(x)$ элемента Фробениуса получаем число $\mathbb{F}_p$ -рациональных точек многообразия

$$N_p = f_p(1) = \prod_{i=1}^{4}(1 \pm \omega_i) = 1 \pm a_1 + a_2 \pm a_1(p+1) + (p+1)^2,$$

где $\omega_i$ – сопряженные с $\omega$ элементы,

$$a_1 = \sum_{i=1}^{4}\omega_i, a_2 = \sum_{i \neq j}^{4}\omega_i\omega_j .$$

1.1. Подбирается натуральное свободное от квадратов $d \in \mathbb{N}$, такое, что число классов поля $K_0 = \mathbb{Q}(\sqrt{d})$ равно 1. В этом случае идеалы в $\mathcal{O}_K$ имеют целый базис по отношению к $\mathcal{O}_{K_0}$ и становится возможным задать матрицы периодов главно поляризованных абелевых многообразий с комплексным умножением на $\mathcal{O}_K$.

1.2. Выбирается такое свободное от квадратов число $\alpha = a + b\sqrt{d}$, чтобы выполнялось неравенство $a \pm b\sqrt{d} > 0$. Поле $K = K_0(i\sqrt{\alpha})$ является *CM*-полем степени 4.

Заметим, что, для того чтобы многообразие Якоби было простым, K/$\mathbb{Q}$ не должно быть расширением Галуа поля с группой Галуа, равной $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.3. Выбор простого числа $p = \omega\bar{\omega}$.

Цель состоит в подборе подходящего простого числа, такого, чтобы число точек в группе $Pic_0(C)$ удовлетворяло требуемому свойству. Для этого можно применить один из пакетов алгоритмической теории чисел. В настоящей работе рассматривается другой подход, который заключается в использовании более эффективного метода подходящих чисел Вейля.

**Определение.** Пусть $p \in \mathbb{Z}$ – простое число. Алгебраическое целое $\omega$ является числом Вейля для $p$, если абсолютное значение всех сопряженных с ним равно $p^{1/2}$. Число $\omega$ называется подходящим числом Вейля для $p$, если

1. $\omega$ и все сопряженные с ним не являются действительными;
2. $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$;
3. $\mathbb{Q}(\omega)$ не содержит мнимых квадратичных подполей;
4. $(p, \omega + \bar{\omega}) = 1$;
5. $\mathbb{Q}(\omega) \neq \mathbb{Q}(\omega)\, e^{2\pi i/3}$.

Число $N_p = f_\omega(1)$, где $f_\omega(x)$ – минимальный многочлен для $\omega$, задает количество $\mathbb{F}_p$-рациональных точек соответствующего абелева многообразия [1].

Процедура выбора простого числа по методу Вейля имеет следующий вид:

1.3.1. Пусть $\omega \in \mathcal{O}_K, N_{K/K_0}(\omega) \in \mathbb{Z}$, $\mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$, $\eta = i\sqrt{a + b\mu}$,
$\{1, \mu, \eta, \mu\eta\}$ – базис $\mathcal{O}_K$ над $\mathbb{Z}$.

По свойствам квадратичных полей, $D \equiv 0 \ mod\ 4$ либо $D \equiv 1 \ mod\ 4$, где $D$ – дискриминант поля $K_0$, так что возможны случаи

$$\eta = i\sqrt{a + b\sqrt{d}} \quad \text{или} \quad \eta = i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})}.$$

Будем рассматривать случай $D \equiv 0 \ mod\ 4$.

1.3.2. Представим $\omega$ в виде $\omega = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})i\sqrt{a + b\sqrt{d}}$.

1.3.3. Вычисляем

$$N_{K/K_0}(\omega) = (c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})i\sqrt{a + b\sqrt{d}}) \times$$

$$\times(c_1 + c_2\sqrt{d} - (c_3 + c_4\sqrt{d})i\sqrt{a + b\sqrt{d}}).$$

1.3.4. В силу действительности нормы получаем уравнения:

$$c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3c_4bd = p,$$

$$2c_1c_2 + 2c_3c_4a + c_3^2 b + c_4^2 bd = 0.$$

1.3.5. Случайным образом выбираем $c_3$, $c_4$ так, чтобы они были взаимно простыми.

1.3.6. Для выбранных $c_3$ и $c_4$ проверяем выполнение условия

$c_3^2 b + c_4^2 bd \equiv 0 \ mod\ 2$, вытекающего из второго уравнения в 3.1.4. В случае невыполнения условия переходим к шагу 3.1.5.

1.3.7. Случайным образом выбираем $c_1$, $c_2$ удовлетворяющие условию $2c_1c_2 = -2c_3c4a - c_3^2 b - c_4^2 bd$.

1.3.8. Проверяем, является ли простым число $c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3c_4bd = p$. В случае невыполнения условия переходим к шагу 3.1.7, а в случае невыполнения 3.1.8 при всех $c_1$, $c_2$ – к шагу 3.1.5.

1.3.9. Возможный порядок группы точек многообразия полагаем равным

$$n = (p+1)^2 \pm (p+1)(4c_1 - 2c_2) + 4(c_1^2 - c_1c_2 + c_2^2(\frac{1-d}{4})).$$

1.3.10. Проверяем условие того, что порядок группы обладает достаточно большим простым

делителем. В случае неудачи возвращаемся к шагу 1.3.1.

Случай $D \equiv 1 \ mod \ 4$ рассматривается аналогично.

**5.2.** ***Нахождение классов изоморфных абелевых многообразий.*** Кольцо эндоморфизмов многообразия Якоби является порядком в *CM*-поле $K$ степени $2 = 4$ над $\mathbb{Q}$. Аналитическое представление многообразия $\mathcal{A}$ зависит от комплексного представления кольца эндоморфизмов, поэтому в рассмотрение вводятся *CM*-типы. Пусть $\varphi_i$, $1 \leqslant i \leqslant 2g$ – различные вложения $K$ в $\mathbb{C}$, и никакие два из них не являются сопряженными. Тогда набор $(K, \Phi) = (K, \{\varphi_1,\ldots,\varphi_g\})$ представляет собой *CM*-тип. Для каждого абелева многообразия $\mathcal{A}$, обладающего свойством $End_K(\mathcal{A}) \otimes \mathbb{Q} \cong K$, существует *CM*-тип $(K, \Phi) = (K, \{\varphi_1,\ldots,\varphi_g\})$.

2.1. Выбирая пару различных несопряженных вложений $\varphi_1$, $\varphi_2$ поля $K$ в $\mathbb{C}$, получаем *CM*-тип $(K, \Phi) = (K, \{\varphi_1, \varphi_2\})$. Полагаем

$$\Phi(A) = (\varphi_1(\alpha), \varphi_2(\alpha))^t, A \text{ – идеал.}$$

Данное множество представляет собой решётку в $\mathbb{C}^2$, а тор $\mathbb{C}^2 / \Phi(A)$ является абелевым многообразием с комплексным умножением на $\mathcal{O}_K$.

2.2. С помощью одной из систем компьютерной алгебры осуществляется вычисление фундаментальной единицы $\varepsilon_0$ поля $K_0$.

2.3. Определяются классы идеалов кольца $\mathcal{O}_K$, содержащие идеал $A$, такие, что $A\bar{A} = \mathcal{O}_K$, $\varphi_1(\alpha)$, $\varphi_2(\alpha)$ действительны и положительны.

2.4. Выбирается полная система представителей классов идеалов $A_1,\ldots,A_{h'_K}$. Каждый из них имеет вид

$$A_j = \mathcal{O}_{K_0} + \tau_j \mathcal{O}_{K_0}, \text{ где } Im(\tau_j) > 0, N_{K_0/\mathbb{Q}}(\varepsilon_0) < 0,$$

причём $N_{K_0/\mathbb{Q}}(\tau_j)$ тотально положительна.

2.5. Находятся представители всех классов изоморфных главно поляризованных абелевых многообразий *CM*-типа $(K, \Phi)$, относящихся к идеалам $A_i$ и обладающих кольцом эндоморфизмов, равным $\mathcal{O}_K$.

2.6. Определяются матрицы периодов $\Omega_i \in H_2$, связанные с кривыми $C_i$ посредством решеток $\Lambda_{C_i}$, соответствующих идеалам $A_i$ из $\mathcal{O}_K$. Здесь $H_2 = \{z \in \mathbb{C}^{2\times 2}, \ z = z^t, \ Im\, z > 0\}$ – верхняя полуплоскость Зигеля.

**5.3.** ***Нахождение полиномов Гильберта.*** С помощью матриц периодов $\Omega_i$ вычисляются тета-константы. Посредством 10-ти четных тета-констант, соответствующих матрицам периодов, можно получить полную систему инвариантов кривых рода 2, выражающихся через коэффициенты уравнения кривой. Алгебраическая система уравнений будет задаваться инвариантами Игусы (*J. I. Igusa*), которые выражаются в рациональных функциях через тета-константы. Эти инварианты порождают неразветвленное поле классов над двойственным полем $K^*$, относящимся к полю $K$, и являются целыми алгебраическими числами. Корни редуцированного многочлена будут соответственно инвариантами редуцированной кривой. Решая систему уравнений для каждой из кривых $C_i$, найдём многочлены $H_{K,k}(X)$. Инвариантам кривых, определенных над простым полем $\mathbb{F}_p$, соответствуют корни многочленов $H'_{K,k}(X)$ по модулю $p$. Поэтому выбирается тройка чисел

$$(j_1^{(i)}, j_2^{(j)}, j_3^{(k)}) \in \mathbb{F}_p{}^3, i, j, k \in \{1,\ldots, s\},$$

где $s$ – число классов изоморфных кривых, и с помощью алгоритма Местре проверяется, будет ли она набором инвариантов кривой.

3.1. Вычисление тета-констант. В терминах матрицы периодов $\Omega$ для рода 2 они определяются следующим образом:

$$\theta\begin{bmatrix}\delta\\ \varepsilon\end{bmatrix}(z,\Omega) = \sum_{n\in\mathbb{Z}^2} \exp(\pi i(n+\delta/2)^t \Omega(n+\delta/2) + 2(n+\delta/2)^t(z+\varepsilon/2)),$$

$$\delta, \varepsilon \in (\mathbb{Z}/2\mathbb{Z})^g, z = 0.$$

Для кривых рода 2 требуются значения десяти чётных тета-констант:

$$\theta_1 := \theta\begin{bmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}0\\0\end{pmatrix}\end{bmatrix}, \ \theta_2 := \theta\begin{bmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}1\\0\end{pmatrix}\end{bmatrix},$$

$$\theta_3 := \theta\begin{bmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}0\\1\end{pmatrix}\end{bmatrix}, \ \theta_4 := \theta\begin{bmatrix}\begin{pmatrix}0\\0\end{pmatrix}\\ \begin{pmatrix}1\\1\end{pmatrix}\end{bmatrix},$$

$$\theta_5 := \theta\begin{bmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\ \begin{pmatrix}0\\0\end{pmatrix}\end{bmatrix}, \ \theta_6 := \theta\begin{bmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\ \begin{pmatrix}0\\1\end{pmatrix}\end{bmatrix},$$

$$\theta_7 := \theta\begin{bmatrix}\begin{pmatrix}0\\1\end{pmatrix}\\ \begin{pmatrix}0\\0\end{pmatrix}\end{bmatrix}, \ \theta_8 := \theta\begin{bmatrix}\begin{pmatrix}0\\1\end{pmatrix}\\ \begin{pmatrix}1\\0\end{pmatrix}\end{bmatrix},$$

$$\theta_9 := \theta\begin{bmatrix}\begin{pmatrix}1\\1\end{pmatrix}\\ \begin{pmatrix}0\\0\end{pmatrix}\end{bmatrix}, \ \theta_{10} := \theta\begin{bmatrix}\begin{pmatrix}1\\1\end{pmatrix}\\ \begin{pmatrix}1\\1\end{pmatrix}\end{bmatrix}.$$

3.2. Вычисление инвариантов Игусы $j_1$, $j_2$, $j_3$ осуществляется посредством тета-констант, для этого вводятся значения $h_4$, $h_{10}$, $h_{12}$, $h_{16}$, связанные с модулярными формами подходящего веса [18].

3.2.1. Вычисление $h_4$, $h_{10}$, $h_{12}$, $h_{16}$ с помощью тета-констант.

3.2.2. Вычисление инвариантов

$$I_2 = \frac{h_{12}}{h_{10}}, I_4 = h_4, I_6 = \frac{h_{16}}{h_{10}}, I_{10} = h_{10}.$$

3.2.3. Вычисление абсолютных инвариантов Игусы

$$j_1 = \frac{I_2^5}{I_{10}}, j_2 = \frac{I_4 I_2^3}{I_{10}}, j_3 = \frac{I_6 I_2^2}{I_{10}}.$$

Известно, что $j_1$, $j_2$, $j_3$ являются рациональными порождающими элементами поля абсолютных инвариантов. Отметим также, что главно поляризованные абелевы многообразия изоморфны тогда и только тогда, когда обладают одинаковыми инвариантами $j_1$, $j_2$, $j_3$.

3.3. Вычисление полиномов Гильберта, которые, в отличие от случая эллиптических кривых, имеют не целые, а рациональные коэффициенты:

$$H_{K,1}(X) = \prod_{i=1}^{s}(X - j_1^{(i)}),\ H_{K,2}(X) = \prod_{i=1}^{s}(X - j_2^{(i)}),$$

$$H_{K,3}(X) = \prod_{i=1}^{s}(X - j_3^{(i)}).$$

3.4. Переход к полиномам $H'_{K,k}(X)$ с целыми коэффициентами.

Для этого ко вторым по величине коэффициентам многочленов применяется алгоритм цепных дробей, чтобы получить возможные знаменатели $d_{K,k}$. Зачастую бывает достаточно домножить многочлен $H_{K,k}(X)$ на $d_{K,k}$. Этот метод почти всегда приводит к нахождению полинома с целыми коэффициентами. Однако есть и исключения, когда знаменатели остальных коэффициентов имеют либо другие делители, либо содержат те же делители, но более высоких степеней. В этом случае алгоритм цепных дробей применяется и к остальным коэффициентам.

3.5. Редукция полиномов $H'_{K,k}(X)$ по модулю числа $p$.

3.6. Выбирается тройка ($a_1$, $a_2$, $a_3$) корней редуцированных полиномов. Полагаем $j_1 := a_1$, $j_2 := a_2$, $j_3 := a_3$, $j_i \in \mathbb{F}_p$.

**5.4.** ***Определение уравнения кривой.*** Для определения уравнений кривых по их инвариантам используется метод Местре (*J.-F. Mestre*), основанный на теории инвариантов бинарных форм [10]. Если известны инварианты Игусы, то, решая систему полиномиальных уравнений, получаем коэффициенты уравнений кривых и уравнения соответствующих многообразий Якоби. Для этого сначала вычисляются новые инварианты Местре, с помощью которых записываются уравнения коники и кубики. Последние пересекаются в шести точках, являющихся корнями многочлена шестой степени.

4.1. *Алгоритм Местре*.

4.1.1. Вычисляются $A$, $B$, $C$, $D$ – инварианты степеней 2, 4, 6, 10, введенные Местре.

4.1.2. Полагаем $j_1' = \frac{A^5}{D}, j_2' = \frac{A^3 B}{D}, j_3' = \frac{A^2}{C}$.

4.1.3. Применяются формулы преобразования

$$j_1' = -\frac{j_1}{120^5}, j_2' = \frac{720 j_1}{6750} - \frac{j_2}{120^3 \times 6750},$$

$$j_3' = \frac{j_3}{120^2 \times 2025100} + \frac{1080 j_2}{2025} - \frac{16 j_1}{375}.$$

Здесь числа $j_1$, $j_2$, $j_3 \in \mathbb{F}_p$ – возможные $j$-инварианты кривой, полученные на шаге 3.6. Напомним, что все вычисления производятся в конечном поле $\mathbb{F}_p$.

4.1.4. Для абсолютного инварианта $\alpha = \frac{D}{\Delta}$ ($\Delta$ – дискриминант Игусы) находится выражение через $j_i'$:

$$\alpha = -\frac{1}{4556250}\left(\frac{1}{j_i' + 62208}\right) + \frac{16 j_2'}{75 j_1'} + \frac{16 j_3'}{45 j_1'} - 2\frac{j_2'^2}{3 j_1'^2} - 4\frac{j_2' j_3'}{3 j_1'^2}.$$

Для удобства далее вместо $j_i'$ будем использовать обозначения $j_i$.

4.1.5. Вычисляются инварианты Местре

$$Q_{11} = \frac{(2 j_3 + \frac{1}{3} j_2)}{j_1}, Q_{12} = \frac{2}{3}\frac{(j_2^2 + j_1 j_3)}{j_1^2},,$$

$$Q_{13} = Q_{22} = \alpha,$$

$$Q_{23} = \frac{1}{j_1^2}\left(\frac{j_2^3}{3 j_1} + \frac{4 j_2 j_3}{9} + \frac{2 j_3^2}{3}\right),$$

$$Q_{33} = \frac{1}{j_1^2}\left(\frac{j_1 j_2 \alpha}{2} + \frac{2 j_2^2 j_3}{9 j_1} + \frac{2 j_3^3}{9}\right),'$$

$$H_{111} = \frac{2}{9}\frac{j_1^2 j_3 - 6 j_1 j_2 j_3 + 9 j_1^2}{j_1^2},$$

$$H_{112} = \frac{1}{9}\frac{2 j_2^3 + 4 j_1 j_2 j_3 + 12 j_1 j_3^2 + 3 j_1^2}{j_1^3},'$$

$$H_{113} = H_{122} = \frac{1}{9}\frac{j_2^3 + 4/3 j_1 j_2 j_3 + 4 j_2^2 j_3 + 6 j_1 j_3^2 + 3 j_1 j_2}{j_1^3},$$

$$H_{123} = \frac{1}{18 j_1^3}\frac{2 j_2^4}{j_1} + 4 j_2^2 j_3 + \frac{4 j_1 j_3^2}{3} + 4 j_2 j_3^2 + 3 j_1 j_2 + 12 j_1 j_3,$$

$$H_{133} = \frac{1}{18 j_1^3}\left(\frac{j_2^4}{j_1} + \frac{4 j_2^2 j_3}{3} + \frac{16 j_2^3 j_3}{3 j_1} + \frac{26 j_2 j_3^2}{3} + 8 j_3^3 + 3 j_2^2 + 2 j_1 j_3\right),$$

$$H_{222} = \frac{1}{9 j_1^3}\left(3\frac{j_2^4}{j_1} + 6 j_2^2 j_3 + \frac{8}{3} j_1 j_3^2 + 2 j_2 j_3^2 - 3 j_1 j_3\right),$$

$$H_{223} = \frac{1}{18 j_1^3}\left(-\frac{2 j_2^3 j_3}{3 j_1} - \frac{4 j_2 j_3^3}{3} - 4 j_3^3 + 9 j_2^2 + 8 j_1 j_3\right),$$

$$H_{233} = \frac{1}{18 j_1^3}\left(\frac{j_2^5 j_1}{2} + 2\frac{j_2^3 j_3}{j_1} + \frac{8}{9} j_2 j_3^2 + \frac{2 j_2^2 j_3^2}{3 j_1} - j_2 j_3 + 9 j_1\right),$$

$$H_{333} = \frac{1}{36 j_1^3}\left(-2\frac{j_2^4}{j_1^2} - 4\frac{j_2^2 j_3^2}{j_1} - \frac{16}{9} j_3^3 - \frac{4 j_2 j_3^2}{j_1} + 9\frac{j_2^3}{j_1} + \right.$$

$$\left. + 12 j_2 j_3 + 20 j_3^2\right).$$

4.1.6. Получаем уравнения коники $Q$ и кубики $H$:

$$Q(j_1, j_2, j_3): \sum_{1\,i\,j\,1} Q_{ij} x_i x_j = 0,$$

$$H(j_1, j_2, j_3): \sum_{1\,i\,j\,k\,1} Q_{ijk} x_i x_j x_k = 0.$$

4.1.7. Осуществляется параметризация коники $(f_1(t), f_2(t), f_3(t))$, для чего последняя приводится к нормальной форме $Q_{11}'x_1^2 + Q_{22}'x_2^2 + Q_{33}'x_3^2$.

4.1.8. Получаем модель гиперэллиптической кривой

$$y^2 = \sum_{i\,j\,k} H_{ijk} f_i(t) f_j(t) f_k(t) =: f(t).$$

Заметим, что по лемме Местре [10] кривая $C$ с инвариантами Игусы $j_1, j_2, j_3$ задается уравнением $y^2 = f(x)$, где $f(x)$ – построенный выше многочлен степени 6.

Пусть $\mathcal{A}$ – главно поляризованное абелево многообразие, определенное над $\mathbb{C}$, и $\{j_1, j_2, j_3\}$ – его инварианты Игусы. Пусть $K_0 \subset \mathbb{C}$ – поле, содержащее эти инварианты, такое, что коника $Q(j_1, j_2, j_3)$ имеет $K_0$-рациональную точку. Тогда $\mathcal{A}$ – многообразие Якоби кривой $C$ рода 2, определённой над $K_0$. Ее уравнение задается в виде $y^2 = f(x)$, где $f(x)$ – полином шестой степени из леммы Местре, построенный выше.

4.1.9. Преобразуем полином шестой степени $f(t)$ к многочлену пятой степени $g(t)$, это возможно в том и только том случае, когда гиперэллиптическая кривая обладает $\mathbb{F}_p$-рациональной вейерштрассовой точкой (т.е. многочлен $f(t)$ имеет нуль в $\mathbb{F}_p$).

4.2. *Заключительный шаг*. Записывается аффинное уравнение

$y^2 = f(x)$, $\deg \bar{f} = 5$. Путем выбора класса дивизоров $Pic_C^0$ и проверки условия $[N]\,\overline{D} = 0$ выясняется, имеет ли группа точек многообразия Якоби построенной кривой $C$ (или её скручивания) одно из возможных значений порядка (здесь $N = \{N_\omega = \chi_\omega(1) \mid \omega \in W\}$). Если проверка оказалась неудачной для каждого из четырех чисел, то выбирается новая тройка инвариантов или, в случае ещё одной неудачи, новое простое $p$.

**6. Применение метода и перспективы дальнейших исследований.** Отметим, что *CM*-метод часто используется в других приложениях, где для порядка группы должно выполняться какое-либо свойство, назовём его (*). Это свойство может выражаться, например, в том, что порядок группы должен иметь простой делитель, превосходящий заданную границу.

Определим квадратичное скручивание кривой $C$ следующим образом:

$C_v: vy^2 = f(x)$, $v$ не является квадратом в $\mathbb{F}_p$.

Если $|J_C| = N_\omega$, то $|J_{C_v}| = N_{-\omega}$, и требуемым свойством (*) будет обладать $C$ либо $C_v$. Зафиксируем *CM*-поле $K$ и рассмотрим алгебраическое число $\omega_1 \in K$, такое, что $\omega\bar{\omega} = p$ и $[\mathbb{Q}(\omega_1) : \mathbb{Q}] = 4$. Сопряженные элементы задаются в виде $\omega_i$, $i = 2,\ldots,4$. Пусть $Tor(U)$ – группа кручения единиц. Пусть имеется кривая над $\mathbb{F}_p$ с комплексным умножением на $\mathcal{O}_K$. Тогда для порядка группы $J(\mathbb{F}_p)$ имеется в точности $\#Tor(U)$ возможностей. Если $K$ не содержит круговых полей, то для порядка группы существуют 2 возможности: $\prod_{i=1}^{4}(1-\omega_i)$ и $\prod_{i=1}^{4}(1+\omega_i)$.

Отметим, что для случая кривой рода 2 за счёт увеличения размерности усложняется процедура вычисления группы классов. Кроме того, для вычисления полиномов классов требуются значения тета-констант и уже не одного, а трёх инвариантов для каждого из классов кривых. Полиномов становится три вместо одного, и они уже будут иметь не целые, а рациональные коэффициенты. Поэтому добавляется шаг 3.4, представляющий отдельную задачу. Далее, если в случае эллиптических кривых после редукции многочленов по модулю простого числа можно сразу перейти к уравнению соответствующей кривой, то во втором случае ситуация усложняется. Существенную трудность представляет нахождение простого числа $p$, а также поиск редуцированных инвариантов, где, в наихудшем случае, выполняется проверка всевозможных $s^3$ троек. Тем не менее, метод Дойринга оказывается гораздо эффективнее случайного выбора кривой. Более подробно алгоритмы вычисления полиномов классов и инвариантов Игусы *CM*-поля $K$ рассматриваются в [4], [7], [8].

При практической реализации предложенного алгоритма возникает необходимость вычисления с большой точностью классических и обобщённых тета-функций. Вопросы реализации таких вычислений с тета-функциями, их особенности и способы преодоления присущих данному классу задач неустойчивостей рассмотрены в [19–21]. Отдельные шаги алгоритма могут быть оптимизированы при помощи усовершенствованных вариантов дискретного преобразования Фурье, см. [24 – 25].

## ЛИТЕРАТУРА


1. Adleman L.M., Huang M.-D. *Primality testing and Abelian varieties over finite fields. Lecture Notes in Math*. Vol. 1512. Springer-Verlag. – 1992..
2. Atkin A.O.L., Morain F. Elliptic curves and primality proving. *Math. Comp*. – 1993. –N 61. – P.29–68.
3. Bolza O. Darstellung der rationalen ganzen Invarianten der Binaerform sechsten Grades durch die Nullwerte der zugehoerigen-function. *Math.Ann*. – 1887. – Bd.30. – P. 478-495.
4. Broeker R., Lauter K. Modular *Polynomials for Genus 2*. URL: http://eprint.iacr.org/2008/161.

5. Cantor H.D.. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp*. – 1987. – v.48 – N 77. – P.95–101.
6. Cohen H., Frey G. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman Hall. CRC. – 2006.
7. Freeman D., Lauter K. *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*. URL: http://www.arxiv.org/abs/math/0701305.
8. Goren E., Lauter K. Class invariants of quartic CM fields. *Annales de l'Institut Fourier*. – 2007. – v.57. – N 2. – P.457–480.
9. Lang S. Complex Multiplication. Springler-Verlag. – 1983.
10. Mestre J.-F. Construction des courbes de genre 2 à partir de leurs modules. *Prog. Math.* – 1991. – N 94. – P.313–334.
11. Mumford D. *Abelian varieties*. Oxford University Press, NY. – 1974.
12. Shimura G. Abelian *Varieties with complex multiplication and modular funktions*, revised edition. Princeton University Press. – 1998.
13. Spallek A.-M. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen. – 1994.
14. Stichtenoth H. *Algebraic function fields and codes*. Springler-Verlag. – 1993.
15. Stichtenoth H., Xing C.P.. On the structure of the divisor class group of a class of curves over finite fields. *Arch.Math (Basel).* – 1995. – v.65. – N 2. – P.141–150.
16. van Wamelen P. Examples of genus two cm curves defined over the rationals. *Math. Comp*. – 1999. – N 68. – P.307–320.
17. Weng A. *Elliptische Kurven und komplexe Multiplikation.* Vorlesung am FB Mathematik (Manuscript). Universität GH Essen. – 2001.
18. Weng A. *Konstruction kryptographisch geeigneter Kurven mit komplexer Multiplikation*. Dissertation, FB 6 Universität GH Essen. – 2001.
19. Zhuravlev M.V., Kiselev E.A., Minin L.A., Sitnik S.M. Jacobi theta-functions and systems of integral shifts of Gaussian functions. *J. Math. Sci*. – 2011. – v.173. – N 2. – P.23 –241.
20. Журавлёв М.В., Киселёв Е.А., Минин Л.А., Ситник С.М. Тета-функции Якоби и системы целочисленных сдвигов функций Гаусса. *Современная математика и её приложения. т.67. Уравнения в частных производных*. – 2010. – С.107–116.
21. Журавлёв М.В., Минин Л.А., Ситник С.М. О вычислительных особенностях интерполяции с помощью целочисленных сдвигов гауссовых функций. *Научные ведомости Белгородского государственного университета*. – 2009 – N 13(68). – Вып.17/2. – С.89–99.
22. Коблиц Н. *Введение в эллиптические кривые и модулярные формы*. М.: Мир. – 1988.
23. Розен М., Айерлэнд К. Классическое введение в современную теорию чисел. М.: Мир. – 1987.
24. Ситник С.М. Компьютерный анализ спектральных свойств модифицированных дискретных преобразований Фурье. *Доклады Адыгской (Черкесской) Международной академии наук*. – 2007. – т. 9, N1. – С. 98 – 103.
25. Ситник С.М. Модифицированные дискретные преобразования Фурье. *Вестник Воронежского Института МВД России*. – 2006. – N 1 (26). – С. 108 – 113.
26. Януш Г.Дж. *Алгебраические числовые поля*. Новосибирск: Научная книга. – 2001.