УДК 512.742 DOI 10.17223/2226308X/12/2

О ПОРЯДКЕ ДЕЙСТВИЯ ЭНДОМОРФИЗМА ФРОБЕНИУСА НА ГРУППУ l-КРУЧЕНИЯ АБЕЛЕВЫХ ПОВЕРХНОСТЕЙ[1]

Н. С. Колесников, С. А. Новоселов

Исследуется вероятностное распределение порядков действия эндоморфизма Фробениуса на группу l-кручения абелевых поверхностей. Получены числовые характеристики соответствующей случайной величины — дисперсия и среднеквадратическое отклонение. Описанные величины могут быть использованы для ускорения нахождения характеристических многочленов Фробениуса по модулю l в обобщении алгоритма Шуфа на абелевы поверхности.

Ключевые слова: *абелевы поверхности, гиперэллиптические кривые, подсчёт числа точек, многочлен Фробениуса.*

Введение

Построение криптосистем на абелевых многообразиях и, в частности, на гиперэллиптических кривых является в настоящее время альтернативой эллиптической криптографии. Они позволяют обеспечить сравнимый уровень криптостойкости при меньшей длине ключа. Сдерживающим фактором в развитии таких криптосистем является трудоёмкость вычислений в якобианах гиперэллиптических кривых. Кроме того, на практике возникает задача подсчёта точек в якобианах, которая на данный момент решена лишь для некоторых частных случаев. Для эллиптических кривых есть эффективный алгоритм Шуфа — Элкиса — Аткина [1]. Для гиперэллиптических кривых рода 2 есть алгоритм Годри — Шоста [2], который является обобщением алгоритма Шуфа. Обобщение оптимизаций Элкиса и Аткина на случай кривых рода 2 и выше является открытой проблемой.

В общем случае для любого абелева многообразия есть теоретический алгоритм подсчёта точек на абелевых многообразиях (обобщение алгоритма Шуфа) [3]. В его основе лежит поиск характеристического многочлена эндоморфизма Фробениуса χ_l, действующего на группу l-кручения. При этом χ_l находится простым перебором коэффициентов.

Одна из оптимизаций Аткина, в случае эллиптических кривых, заключается в нахождении порядка действия Фробениуса на группу l-кручения и его использование для ускорения перебора χ_l. При этом сам порядок вычисляется из разложения модулярных многочленов.

Для гиперэллиптических кривых рода 2 модулярные многочлены имеют большой размер, что делает их малопригодными для практических вычислений. Поэтому мы изучаем вероятностный подход для нахождения порядка действия Фробениуса.

В [4] представлена идея улучшения алгоритма за счёт оценки вероятностного распределения порядка действия эндоморфизма Фробениуса. В настоящей работе получены дополнительные характеристики распределения порядков матриц, соответствующих действию эндоморфизма Фробениуса на группу l-кручения. Вычислены дисперсия распределения и среднеквадратическое отклонение.

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-31-00244.

1. Распределение порядков действия эндоморфизма Фробениуса

Пусть A — абелева поверхность над конечным полем $\mathbb{F}_q$ нечётной характеристики p. Будем рассматривать действие эндоморфизма Фробениуса на группу l-кручения $A[l]$, где l — простое число, такое, что $q \equiv 1 \mod l$. В этом случае действие эндоморфизма Фробениуса на группу l-кручения как линейного оператора может быть представлено симплектической матрицей $F_l \in PSp_{2g}(\mathbb{F}_l)$, где $g = 2$ — размерность абелева многообразия.

Введём случайную величину ξ, которая принимает значения порядков $r = \mathrm{Ord}(F_l)$ симплектических матриц как элементов группы $PSp_4(\mathbb{F}_l)$. Отношение подобия разбивает симплектическую группу на классы эквивалентности $[A_i]$, в каждом из которых встречаются матрицы одного порядка $r_i = \mathrm{Ord}(A_i)$. Эти порядки вычислены для каждого класса в [4]. Там же приводится формула для вычисления математического ожидания $\mathrm{M}(\xi)$. Определим числовые характеристики этой случайной величины:

$$\mathsf{P}(\xi = r_k) = \frac{\#\{A \in PSp_4(\mathbb{F}_l) : \mathrm{Ord}(A) = r_k\}}{\#PSp_4(\mathbb{F}_l)} = \frac{\#[A_{i_1}] + \ldots + \#[A_{i_s}]}{\#PSp_4(\mathbb{F}_l)},$$

где $A_{i_1}, \ldots, A_{i_s}$ — представители всех классов, таких, что $\mathrm{Ord}(A_{i_1}) = \ldots = \mathrm{Ord}(A_{i_s}) = r_k$. Из [4] имеем

$$\mathrm{M}(\xi) = \sum_{i=1}^{k} r_k \frac{\#[A_{i_1}] + \ldots + \#[A_{i_s}]}{\#PSp_4(\mathbb{F}_l)} = \sum_{i=1}^{n} \mathrm{Ord}(A_i) \frac{\#[A_{i_1}]}{\#PSp_4(\mathbb{F}_l)} \approx$$
$$\approx \frac{\pi^2}{48} \frac{2l^5 + 16l^4 - 48l^3 + 65l - 37}{l(l^2-1)} \frac{1}{\log(l)}.$$

Последнее выражение получено при помощи аппроксимации функции НОД из работы [5].

Теорема 1. Пусть A — абелева поверхность над конечным полем $\mathbb{F}_q$ характеристики p и $l \neq p$ — простое число, такое, что $q \equiv 1 \mod l$. Тогда при $q \gg l$ дисперсия распределения порядков действия эндоморфизма Фробениуса на $A[l]$ и его среднеквадратическое отклонение могут быть вычислены по следующим формулам:

$$D(\xi) \approx \left(\frac{\pi^2}{48}\right)^2 \frac{\psi(l)}{l^2(l^2-1)^2} \frac{1}{\log^2(l)}, \quad \sigma(\xi) = \sqrt{D(\xi)} \approx \frac{\pi^2}{48} \frac{\sqrt{\psi(l)}}{l(l^2-1)} \frac{1}{\log(l)},$$

где

$$\psi(l) = 2l^{10} + 56l^9 - 316l^8 + 1344l^7 - 1948l^6 - 1770l^5 + 6660l^4 - 3516l^3 - 3831l^2 + 4684l - 1369.$$

ЛИТЕРАТУРА

1. *Schoof R.* Counting points on elliptic curves over finite fields // J. Theor. Nombres Bordeaux. 1995. V. 7. No. 1. P. 219–254.
2. *Gaudry P. and Schost É.* Genus 2 point counting over prime fields // J. Symb. Comput. 2012. V. 47. No. 4. P. 368–400.
3. *Pila J.* Frobenius maps of abelian varieties and finding roots of unity in finite fields // Mathematics of Computation. 1990. V. 55. No. 192. P. 745–763.
4. *Novoselov S. A. and Kolesnikov N. S.* On expected order of Frobenius action on l-torsion of abelian surfaces // Submitted at NuTMiC. 2019.
5. *Diaconis P. and Erdös P.* On the distribution of the greatest common divisor // Lecture Notes — Monograph Series. Institute of Mathematical Statistics. 2004. V. 45. P. 56–61.