УДК 511.48:519.61

И. Д. Ильяшенко

ОБЗОР ЭФФЕКТИВНЫХ АЛГОРИТМОВ ПОДСЧЕТА ЧИСЛА ТОЧЕК ЯКОБИАНА ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД КОНЕЧНЫМ ПОЛЕМ

Рассмотрены различные алгоритмы нахождения порядка якобиана, их область применения и эффективность.

Various algorithms for finding of the order of Jacobian, their range of use and efficiency are considered.

Ключевые слова: гиперэллиптическая кривая, якобиан, подсчет точек, дискретный логарифм.

Key words: hyperelliptic curve, Jacobian, point counting, discrete logarithm.

Пусть p — простое число, F_q — конечное поле, где $q = p^i$. C — гиперэллиптическая кривая рода g, определенная над полем F_q вида $y^2 = f(x)$, где $f(x)$ — многочлен степени $2g+1$ в $\mathrm{F}_q(x)$.

Пусть J_C — якобиан кривой C, а $J_C(\mathrm{F}_q)$ — группа рациональных точек якобиана, а $\chi(t)$ — характеристический многочлен эндоморфизма Фробениуса кривой C, тогда $\#J_C(\mathrm{F}_q) = \chi(1)$, поэтому задачу отыскания порядка якобиана можно свести к нахождению $\chi(t)$.

В случае кривой рода 2

$$\chi_q(t) = t^4 - s_1 t^3 + s_2 t^2 - s_1 q t + q^2, \qquad (1)$$

где $s_i \in \mathbf{Z}$, $|s_1| \leqslant 4\sqrt{q}$, $|s_2| \leqslant 6q$. Тогда

$$\#J_C(\mathrm{F}_q) = q^2 + 1 - s_1(q+1) + s_2. \qquad (2)$$

Не существует эффективного обобщенного способа вычисления числа рациональных точек якобиана произвольной эллиптической или гиперэллиптической кривой. Но созданы алгоритмы для конкретного семейства кривых, которые являются весьма быстрыми.

Колм О'Хегертэй сравнил [1] методы подсчета точек якобиана гиперэллиптических кривых над простыми полями и полями характеристики 2. Он сравнил время работы этих алгоритмов и определил их практическое применение для различных характеристик полей. Для полей характеристики 2 О'Хегертэй рассмотрел два алгоритма.

Алгоритм Коблица. Подсчет точек якобиана происходит за счет вычисления коэффициентов дзета-функции самой кривой и решения квадратных уравнений, построенных с их помощью. Алгоритм применим только для кривых рода 2, так как для кривых большего рода вычисление коэффициентов дзета-функции слишком сложно.

Алгоритм Сакая — Сакурая позволяет вычислять порядок якобиана для кривых произвольного рода над полями малых характеристик. Этот алгоритм является рекурсивным и сводится к нахождению порядка якобиана над полями меньшего размера.

Последний алгоритм работает гораздо медленнее, но зато применим для кривых произвольного рода.

Для кривых над простыми полями О'Хегертэй привел алгоритмы Хассе — Витта, Фурукавы — Кавазо — Такахаши и Коблица.

Алгоритм Хассе — Витта. Данный алгоритм возводит многочлен $f(x)$ из уравнения кривой в степень $(p-1)/2$, где p — характеристика поля (причем $64 < p < 100\ 000$, то есть применение данного поля в криптографии небезопасно). Коэффициенты полученного многочлена являются начальными значениями для рекурсивной функции, которая в итоге находит числа s_1 и s_2 для формулы (2).

Алгоритм Фурукавы, Кавазо и Такахаши также рекурсивен, но требует вместо возведения в степень нахождения $a \in \mathrm{F}_p$, не являющегося квадратичным вычетом, и числа $c \equiv 1 (\mathrm{mod}\, p)$ из $p = c^2 + 2d^2$, где d — целое.

Алгоритм Коблица применим для кривых вида $y^2 + y = x^n$, $n = 2g + 1$, $p \equiv 1 (\mathrm{mod}\, n)$, где g — род кривой. Для подсчета точек здесь используют суммы Якоби вида $J_r(\chi, \chi) = \sum_{t \in \mathrm{F}_{p^r}} \chi(t)\chi(1-t)$, причем вся сложность алгоритма сводится именно к нахождению этих сумм. Алгоритм Коблица по скорости сравним с алгоритмом Фукуравы, Кавазо, Такахаши.

А если поле произвольно и наша криптосистема работает с определенным типом кривых?

Кавазо, Такахаши и Фурукава рассмотрели в [3] семейство гиперэллиптических кривых $y^2 = x^5 + ax$ над большим конечным полем F_q. Основная идея алгоритма такова. Для данных кривых характеристический многочлен Фробениуса имеет вид (1). Значения s_1, s_2 ограничены: $\left\lceil 2\sqrt{q} \mid s_1 \mid -2q \right\rceil \leqslant s_2 \leqslant \left\lfloor q+1+(N_q(g)-(q+1))/g+2q \right\rfloor$. Пусть $q = p$ — простое, причем $p > 64$. Тогда, чтобы найти s_1, s_2, необходимо рассмотреть максимум три возможных значения s_2, найти для них число точек и проверить умножением на произвольную точку якобиана.

Позднее Ханеда, Кавазо, Такахаши расширили рассматриваемое семейство до гиперэллиптических кривых $y^2 = x^{2k+1} + ax$, предложив эффективный алгоритм вычисления порядка якобиана при помощи сумм якобстала $\phi_{k,r}(a) = \sum_{x \in \mathrm{F}_{p^r}} \chi_2(x^{k+1} + ax)$, где $a \in \mathrm{F}_p$, $r = 1, \ldots, g$, χ_2 — элемент порядка 2 поля F_{p^r}. Число рациональных точек кривой над полем F_{p^r} при этом равно $|C(\mathrm{F}_{p^r})| = p^r + 1 + \phi_{k,r}(a)$. Тогда находим характеристический многочлен Фробениуса из условия $\chi_t(t) = \prod_{i=1}^{2g}(t - a_i)$, тогда $|C(\mathrm{F}_{p^r})| = p^r + 1 + \sum_{i=1}^{2g} a_i^r$. С помощью данного алгоритма авторы выделяют наиболее приемлемые для безопасности конечные поля и соответствующие порядки якобианов.

Кавазо, Такахаши и Фурукава показали, что в некоторых случаях необязательно вычислять непосредственно точное значение порядка якобиана. Можно найти предполагаемые значения и проверить их. Имея на руках ограничение порядка якобиана, зависящее от размера поля, мы можем сократить количество таких чисел для проверки.

С. Халоуи показала в [4] верхние и нижние возможные границы для числа рациональных точек абелевых многообразий и якобианов. Если задано конечное поле F_q размерности g, то для абелевого многообразия A: $(q+1-2\sqrt{q})^g \leqslant \#A(\mathrm{F}_q) \leqslant (q+1+2\sqrt{q})^g$. Для якобианов всевозможных кривых над полем F_q это так же применимо, причем $J_q(g) \leqslant \leqslant (q+1+(N_q(g)-(q+1))/g)^g$, где $N_q(g)$ — максимальное число точек, которое может содержать кривая в F_q. Также для якобианов приведена асимптотическая оценка при росте размерности g: $q \leqslant J_q(\infty) \leqslant q + \sqrt{q}$.

На смену криптографии с использованием спаривания Вейля на эллиптических кривых приходит спаривание на якобианах гиперэллиптических кривых. Для того чтобы осуществить это спаривание, Кристиан Равншой в [5—7] предложил вероятностный алгоритм нахождения образующих группы кручения якобиана гиперэллиптической кривой рода 2 над конечным полем F_q. Для этого автор использует спаривание Тейта и «диагонализацию» множества случайно выбранных точек $\{P_1, \ldots, P_4, Q_1, \ldots, Q_4\}$ якобиана с использованием эндоморфизма Фробениуса. Тем самым автор касается нахождения подходящих для криптографии гиперэллиптических кривых, то есть кривых, якобианы которых содержат большие циклические подгруппы.

При работе с якобианами перед исследователями всегда стоят две трудности. Одна заключается в том, что элементы якобиана не всегда можно представить в компактной форме в отличие от элементов алгебраических торов. Ко второй трудности относится проблема вычисления дискретного логарифма.

Рассмотрим понятие «обобщенного» якобиана, упоминаемое Изабель Дешен [8; 9]. Это некоторая алгебраическая группа гиперэллиптической кривой. Она является обобщением таких структур, как якобиан и тор. «Обобщенный» якобиан аналогичен обычному, но вместо линейного отношения эквивалентности между дивизорами вводят специальное $D \sim_m D'$, если $\exists f \in K(C)^*$,

такой, что $(f) = D - D'$ и $f \equiv 1(\mathrm{mod}\, m)$, где C — некоторая кривая над конечным алгебраически замкнутым полем K, а m — положительный дивизор.

Элементы данной группы можно представить в виде пары (k, P), где $k \in G_m$, $P \in C$. Для такого представления описан групповой закон.

«Обобщенные» якобианы обладают полезными свойствами как обычных якобианов (маленький размер ключа), так и торов (компактное представление элементов). Однако решение проблемы дискретного логарифма здесь остается не менее сложной задачей, чем на самой кривой или в конечном поле. Гэлбрэйт и Смит показали, что данная проблема является и не более сложной [10]. Эффективный алгоритм решения проблемы дискретного алгоритма в якобиане гиперэллиптической кривой рассмотрен К. Нагао [11]. Он основан на работах Харли и Терьялу и использует множества гладких и почти гладких дивизоров относительно множества $B \subset \mathrm{P}$, где $\mathrm{P} = \left(P \,|\, -P \in \mathrm{P}\right)$. Генерируем множества гладких дивизоров, затем находим числа s_v по модулю $|J_q|$ такие, что $\sum_v s_v v \equiv \equiv 0(\mathrm{mod}\,|J_q|$, где v — почти гладкий дивизор. Подставляя значения в $-\sum_v s_v \alpha_v / \sum_v s_v \beta_v (\mathrm{mod}\,|J_q|)$, находим дискретный логарифм.

Список литературы

1. *Colm O hEigeartaigh.* A comparison of point counting methods for hyperelliptic curves over prime fields and fields of characteristic 2 // Cryptology ePrint Archive. 2004.

2. *Haneda M., Kawazoe M., Takahashi T.* Suitable curves for genus-4 HCC over prime fields: point counting formulae for hyperelliptic curves of type $y^2 = x^{2k+1} + ax$ // Ibid.

3. *Furukawa E., Kawazoe M., Takahashi T.* Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ // Ibid. 2002.

4. *Haloui S.* The minimum and maximum number of rational points on jacobian surfaces over finite fields. URL: http://arxiv. org/abs/1002.3683.2010.

5. *Ravnshoj C. R.* Generators of Jacobians of genus two curves // Cryptology ePrint Archive. 2008.

6. *Ravnshoj C. R.* Non-cyclic subgroups of Jacobians of genus two curves // Ibid.

7. *Ravnshoj C. R.* Non-cyclic subgroups of Jacobians of genus two curves with complex multiplication // Ibid.

8. *Dechene I.* Arithmetic of generalized Jacobians // Ibid. 2006.

9. *Dechene I.* On the security of generalized Jacobian cryptosystems // Ibid.

10. *Galbraith S. D., Smith B. A.* Discrete logarithms in generalized Jacobians // Ibid.

11. *Nagao K.* Improvement of theriault algorithm of index calculus for Jacobian of hyperelliptic curves of small genus // Ibid. 2004.

Об авторе

Илья Дмитриевич Ильяшенко — студ., РГУ им. И. Канта, e-mail: tommplay@ googlemail. com.

Author

Ilya Ilyashenko — student, IKSUR, e-mail: tommplay@googlemail. com.