

ВЫЧИСЛЕНИЕ КРАТНОЙ ТОЧКИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ С ПОМОЩЬЮ МНОГОЧЛЕНОВ ДЕЛЕНИЯ

С. В. Агиевич, С. В. Поручник, В. И. Семенов

*Научно-исследовательский институт прикладных проблем математики и информатики,
Белорусский государственный университет,
Минск, Беларусь,
e-mail: agievich@bsu.by, poruchnikstanislav@gmail.com, semenov.vlad.by@gmail.com*

В данной работе приводятся результаты оценок трудоемкости разработанного регулярного оконного алгоритма вычисления кратной точки эллиптической кривой, основанного на многочленах деления. Вычисление кратной точки эллиптической кривой — основная операция Elliptic Curve Cryptography (ECC). Алгоритмы, основанные на многочленах деления имеют вычислительные преимущества перед известными аналогами. Исследовались кривые над большим простым конечным полем, заданные в короткой форме Вейерштрасса с коэффициентом $a = -3$.

Ключевые слова: регулярные алгоритмы; оконные алгоритмы; эллиптические кривые; вычисление кратной точки; многочлены деления.

ECC (Elliptic Curve Cryptography, [2]) — это основное на сегодняшний день направление криптографии с открытым ключом. ECC используется для шифрования почтовых сообщений, формирования общих для TLS-серверов и их клиентов секретных ключей, подписи транзакций криптовалют и многих многих других, уже ставших почти рутинными, криптографических операций. Алгоритмы и протоколы ECC широко применяются в нашей стране, будучи введенными в государственных стандартах СТБ 34.101.45 и СТБ 34.101.66.

Далее мы рассматриваем эллиптическую кривую над большим простым конечным полем F . Кривая задается уравнением $E: y^2 = x^3 + ax + b$ ($a, b \in F$), которое называется короткой формой Вейерштрасса. Кривые именно такой формы в основном применяются в ECC. В частности, кривые Вейерштрасса стандартизированы в упомянутых СТБ.

Для аффинных точек кривой, т. е. удовлетворяющих E пар $(x, y) \in F^2$, определена операция сложения. Результатом операции может быть специальная бесконечно удаленная точка O . Эта же точка может выступать в качестве операнда. Сложение определяется так, что аффинные точки, дополненные O , образуют абелеву группу. При этом O — нуль группы, а $(x, -y)$ — точка, обратная точке (x, y) . В группе точек кривой E выбирается базовая точка G , которая порождает циклическую группу $\langle G \rangle$ порядка q . В криптографии используются такие (E, G) , что q — простое число близкое к $|F|$. Пусть l — битовая длина q .

Основная операция ECC — это вычисление кратной точки: нахождение dP по $P \in \langle G \rangle$, $P \neq O$, и $d \in \{1, 2, \dots, q-1\}$. Кратность d — это произвольное и, как правило, секретное и случайное число. Относительно базовой точки P возможны две ситуации:

- 1) P заранее известна, и с ней можно провести предвычисления;
- 2) P — произвольная ненулевая точка $\langle G \rangle$ (свободная базовая точка).

Первая ситуация возникает, например, при выработке ЭЦП ЭльГамала или Шнора, вторая — при формировании общего ключа в протоколах типа Диффи – Хеллмана.

Имеется большое количество алгоритмов и методов вычисления кратной точки. В настоящей работе мы развиваем, так называемые, оконные методы. В них расчет $(d, P) \mapsto dP$ выполняется в два этапа:

I. Сначала для небольшого w (длина окна) рассчитываются малые кратные $\pm(2k + 1)P$, $k = 0, 1, \dots, 2^{w-1} - 1$, базовой точки P .

II. Затем по d и найденным малым кратным $\pm(2k + 1)P$ рассчитывается dP .

Для фиксированной точки P малые кратные можно рассчитать заранее, т. е. первый этап исключается.

Мы предлагаем алгоритмы, реализующие оба этапа расчетов. Алгоритмы первого этапа, основанные на многочленах деления [1], имеют вычислительные преимущества перед известными аналогами. Алгоритмы второго этапа отличаются от стандартных оконных тем, что в них исключены условные переходы. Алгоритмы без условных переходов принято называть регулярными (constant-time в англоязычном контексте). Только регулярные алгоритмы признаются на сегодняшний день надежными, поскольку в современных процессорах условные переходы индуцируют флуктуации времени выполнения алгоритма с потенциальной утечкой информации о секретных данных (в нашем случае кратности d).

Вычисления с ненулевыми точками эллиптической кривой сводятся к вычислениям с их координатами, т.е. к вычислениям с элементами F . Такие вычисления описываются арифметическими (над F) схемами со следующими операциями: $\mathbb{I}$ – мультипликативное обращение, $\mathbb{M}$ – умножение двух произвольных элементов, $\mathbb{S}$ – возведение в квадрат. Аддитивные операции и умножения на небольшие константы мы игнорируем. Запись $i\mathbb{I} + m\mathbb{M} + s\mathbb{S}$ означает, что в вычислениях используется i операций $\mathbb{I}$, m операций $\mathbb{M}$ и s операций $\mathbb{S}$. Например, на кривых Вейерштрасса сложение аффинных точек можно выполнить со сложностью $1\mathbb{I} + 2\mathbb{M} + 1\mathbb{S}$, удвоение – со сложностью $1\mathbb{I} + 2\mathbb{M} + 2\mathbb{S}$.

Операция $\mathbb{I}$ является наиболее трудоемкой, по разным оценкам ее сложность в 80 – 100 раз выше сложности $\mathbb{M}$. Чтобы максимально избежать использования $\mathbb{I}$, от аффинных точек (x, y) переходят к проективным точкам (X, Y, Z) . Мы используем якобиановы проективные точки: $X/Z^2 = x$, $Y/Z^3 = y$. Координата Z выступает в роли нормирующего множителя, фактически «поглощая» неудобную операцию $\mathbb{I}$. На кривой Вейерштрасса с $a = -3$ (это оптимальный выбор коэффициента) сложение якобиановых точек можно выполнить со сложностью $11\mathbb{M} + 5\mathbb{S}$, удвоение – со сложностью $3\mathbb{M} + 5\mathbb{S}$, сложение якобиановой точки с аффинной – со сложностью .

Малые кратные, которые выдают алгоритмы этапа I и которые принимают алгоритмы этапа II, могут быть либо аффинными, либо якобиановыми точками. При использовании аффинных точек ускоряется этап I и замедляется этап II, при использовании якобиановых – все наоборот.

Трудоемкость разработанных алгоритмов при разных соглашениях о входах / выходах представлена в следующей таблице. Для простоты (и с незначительными потерями в точности) считаем, что w делит l .

Этап, входы / выходы	Трудоемкость
I, якобиановы точки на выходе	$(21 \cdot 2^{w-2} - 12)\mathbb{M} + (2^w + 4)\mathbb{S}$
I, аффинные точки на выходе	$\mathbb{I} + (31 \cdot 2^{w-2} - 15)\mathbb{M} + (3 \cdot 2^{w-1} + 3)\mathbb{S}$
II, якобиановы точки на входе	$\mathbb{I} + (3(l - w) + 11 \, l / w - 8)\mathbb{M} + (5(l - w) + 5 \, l / w - 4)\mathbb{S}$
II, аффинные точки на входе	$\mathbb{I} + (3(l - w) + 7 \, l / w - 4)\mathbb{M} + (5(l - w) + 4 \, l / w - 3)\mathbb{S}$

Библиографические ссылки

1. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

2. Hankerson, D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone. – Springer, 2006. – 312 p.