ВЫЧИСЛЕНИЕ КРАТНОЙ ТОЧКИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ С ПОМОЩЬЮ МНОГОЧЛЕНОВ ДЕЛЕНИЯ

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

Научно-исследовательский институт прикладных проблем математики и информатики, Минск, Беларусь,

Белорусский государственный университет, Минск, Беларусь,

e-mail: agievich@bsu.by, poruchnikstanislav@gmail.com, semenov.vlad.by@gmail.com

Криптография на эллиптических кривых (Elliptic Curve Cryptography, ECC, [1]) – это основная на сегодняшний день платформа для построения криптографических механизмов 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 $E\colon y^2 = x^3 + ax + b$ $(a,\ b \in F)$, 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 — большое 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 $d \in \{1, 2,\ldots, q - 1\}$. Кратность d — это, как правило, случайное секретное число. Относительно точки P возможны две ситуации:

1) P заранее известна, и с ней можно провести предвычисления;

2) P – произвольная (*свободная*) ненулевая точка группы $\langle G\rangle$.

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

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

Операция `I` является наиболее трудоемкой, по разным оценкам ее сложность в 80 – 100 раз выше сложности `M`. Чтобы сократить использование `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 `I`. На кривой Вейерштрасса с $a = -3$ (это

оптимальный выбор коэффициента) сложение якобиановых точек можно выполнить со сложностью $11\mathtt{M} + 5\mathtt{S}$, удвоение – со сложностью $3\mathtt{M} + 5\mathtt{S}$, сложение якобиановой точки с аффинной – со сложностью $7\mathtt{M} + 4\mathtt{S}$.

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 $w \geq 2$ (*длина окна*) рассчитываются малые кратные $\pm(2i + 1)P$, $i = 0, 1, \ldots, 2^{w-1} - 1$, точки P.

II. Затем по d и малым кратным $\pm(2i + 1)P$ 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 основаны на многочленах деления. Использовать эти многочлены для вычисления кратной точки предложил еще В. Миллер (см. [2]), один из основоположников ECC. Предложение Миллера так и осталось наброском, не доведенном до реализации из-за недостаточной проработки алгоритмических деталей (это и не было основной задачей Миллера). Проблема в том, что основанные на многочленах деления арифметические схемы для вычисления dP быстро усложняются с ростом d. Тем не менее, сложность схем для вычисления малых кратных $\pm(2i + 1)P$ остается приемлемой, более того, эти схемы по нашим оценкам оказываются эффективнее стандартных схем типа «удвоить – сложить».

Наши алгоритмы второго этапа отличаются от стандартных оконных тем, что в них исключены условные переходы. Алгоритмы без условных переходов принято называть *регулярными* (constant-time в англоязычной литературе). 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). Для регуляризации мы представляем число d или, если оно четное, число $q - d$ в виде суммы $d_0 + 2^w d_1 + \ldots + 2^{(k-1)w} d_{k-1}$, $d_j \in \{-2^w + 1, -2^w + 3, \ldots, 2^w - 1\}$. На шагах алгоритмов числа d_j определяют номера используемых малых кратных.

Малые кратные, которые выдают алгоритмы этапа I и которые принимают алгоритмы этапа II, могут быть либо аффинными, либо якобиановыми точками. При использовании аффинных точек замедляется этап I и ускоряется этап II, при использовании якобиановых – все наоборот. Якобиановы точки этапа I предлагается одновременно переводить в аффинные с помощью схемы, предложенной П. Монтгомери. Сложность схемы: $\mathtt{I} + (3 \cdot 2^{w-1} - 6)\mathtt{M}$.

В следующей таблице представлена трудоемкость разработанных алгоритмов применительно к кривым в короткой форме Вейерштрасса с $a = -3$. В таблице $k = \lceil l / w \rceil$.

Этап, входы / выходы	Трудоемкость
I, якобиановы точки на выходе	$(22 \cdot 2^{w-2} - 12)\mathtt{M} + (2^w + 4)\mathtt{S}$
I, аффинные точки на выходе	$\mathtt{I} + (34 \cdot 2^{w-2} - 21)\mathtt{M} + (3 \cdot 2^{w-1} + 3)\mathtt{S}$
II, якобиановы точки на входе	$\mathtt{I} + (3(k-1)w + 11k - 8)\mathtt{M} + (5(k-1)w + 5k - 4)\mathtt{S}$
II, аффинные точки на входе	$\mathtt{I} + (3(k-1)w + 7k - 4)\mathtt{M} + (5(k-1)w + 4k - 3)\mathtt{S}$

Библиографические ссылки

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

2. Miller, V.S. Use of Elliptic Curves in Cryptography / In: Advances in Cryptology – CRYPTO'85 Proceedings. LNCS 218, pp. 417–426, 1986.