УДК 004.056.55

П. С. Захаров, М. Г. Пискун

Московский физико-технический институт (государственный университет)

Представления точек на эллиптических кривых

В современных информационных системах большое значение имеет криптография с открытым ключом. Подобные системы реализованы, к примеру на эллиптических кривых. Они используют проблему дискретного логарфима в применении к точкам на эллиптических кривых над конечными полями. Подобные системы нашли применение, к примеру, в ГОСТ Р 34.10-2012. В практических применениях важна не только защищенность системы, но и ее производительность. Различные представления точек на кривых позволяют оптимизировать процесс вычислений и ускорить производительность. В данной статье рассматриваются различные представления точек с точки зрения количества требуемых операций и используемой памяти на примере ECDSA - алгоритма для создания цифровой подписи.

Ключевые слова: Криптография с открытым ключом, эллиптические кривые, ЭЦП

1. Введение

В настоящее время распространены ассиметричные криптографические алгоритмы с открытым ключом. В таких алгоритмах существует два ключа - открытый, передавемый по незащищенному каналу, и закрытый, держащийся в тайне и тяжело вычисляющийся из открытого. Такие системы используются для проверки цифровых подписей или обмена ключами от симметричных систем. К ним относятся широко известные алгоритмы Диффи-Хеллмана, Эль-Гамаля, шифр RSA и другие [3].

Реалии современного мира предъявляют высокие требования как к защищенности криптосистем, так и к их производительности. Первое требование, помимо прочего, обуславливает выбор больших параметров системы (к примеру, порядок используемого конечного поля), в особенности для ассиметричных криптосистем. В сочетании с большим количеством вычислений, требующихся для произведения одной итерации шифрования или создания одной подписи, это явно противоречит второму требованию. В связи с этим используются различные методики более быстрых вычислений.

В криптографии на эллиптических кривых основой вычислений являются операции над точками на кривой - сложение и умножение на число. Каждая из этих операций подразумевает определенное количество сложений, умножений и инверсий в конечном поле. Более сложные представления точек позволяют сократить число этих операций за счет хранения большего числа информации [1]. В данной работе сравниваются разные представления с точки зрения производительности и используемой памяти. В разделе 1 вводятся эллиптические кривые и описывается тестовый алгоритм - ECDSA (Elliptic Curve Digital Signature Algorithm), в разделе 2 рассматриваются различные представления точек, в разделе 3 описывается вычислительный эксперимент. В разделе 4 обсуждаются результаты.

2. Эллиптические кривые и ECDSA

Определение 1. *Эллиптической кривой на плоскости называется кривая в $\mathbb{R}^2$, описываемая выражением*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

Практическое приложение имеют эллиптические кривые над конечными полями - в этом случае коэффициенты и координаты точек принадлежат соответсвующему полю. В случае, если характеристика поля не равна 2 или 3, кривая может быть приведена к виду [1]:

$$y^2 = x^3 + ax + b, a, b, x, y \in K \tag{2}$$

Определение 2.

Если к множеству точек кривой добавить ∞, то на получившемся множестве E можно ввести операцию сложения (и, соответсвенно, умножения на целое) [2]. Нетрудно показать, что E с соотвествующим образом определенной операцией является группой. В данной группе имеет место проблема дискретного логарифма для точек на эллиптических кривых [2]:

Определение 3. *Пусть E - эллиптическая кривая над полем K, и G - точка на E. Задачей дискретного логарифмирования на E с основанием B называется задача нахождения для данной точки $P \in E$ $a \in K$ (если существует) такого, что $P = aG$*

Если кривая не является суперсингулярной, не существует субъэкспоненциального алгоритма для решения этой проблемы. На основе её и создан алгоритм цифровой подписи ECDSA.

Алгоритм ECDSA подразумевает, что Алиса и Боб договорились относительно используемых кривой и поля. При этом в группе точек на этой кривой должна быть циклическая подгруппа достаточно большого простого порядка q. Пусть P - порождающая точка в этой подгруппе, т.е. $qP = O$. Алиса выбирает случайное число $d \in [1, q-1]$ - это ее закрытый ключ. Точка $Q = dP$ - открытый ключ. (P также известна всем участникам. Проблема дискретного логарифма гарантирует сохранность закрытого ключа)

Пусть $m = h(M)$ - хэш сообщения (достаточно короткий), k - случайное число их $[1, q-1]$. Дальнейшие вычисления:

$$\begin{aligned} C = kP &= (x_c, y_c) \\ r &= x_c \, mod \, q \\ s &= k^{-1}(m + rd) \; mod \, q \end{aligned} \tag{3}$$

Пара (r, s) - подпись.

Для проверки подписи Бобу требуется проверить, что $0 \leq r, s \leq q-1$, а также провести вычисления:

$$\begin{aligned} v_1 &= s^{-1} h \, mod \, q \\ v_2 &= s^{-1} r \, mod \, q \\ v_1 P + v_2 Q &= (x_b, y_b) \\ \hat{r} &= x_b \, mod \, q \end{aligned} \tag{4}$$

Полученное в (4) $\hat{r}$ должно совпасть с r

3. Представления точек

Сложение, а тем более умножение точки на число является затратной операцией: в стандартных координатах в кривых над полями с характеристикой, отличной от 2 и 3, сложение точек выглядит следующим образом. Пусть $P = (x_P, y_P), Q = (x_Q, y_Q) \in E, P \neq \pm Q$. Тогда для $R = P + Q$

$$x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q, \quad y_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_R) - y_P \tag{5}$$

Видно, что для сложения точек требуется инверсия и умножение в поле. Первая является особенно дорогостоящей операцией, и от нее хотелось бы избавиться. Это позволяют сделать другие координатные системы [2], которые позволяют добиться лучшей производительности за счет дополнительной информации. Одним из таких представлений являются проективные координаты.

3.1. Проективные координаты

Пусть c, d - положительные целые. Рассмотрим следующее отношение эквивалентности на $K^3 \setminus \{(0,0,0)\}$:

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2) \Leftrightarrow \exists \lambda \in K : X_1 = \lambda^c X_2, Y_1 = \lambda^d Y_2, Z_1 = \lambda Z_2 \tag{6}$$

Оно разбивает $K^3 \setminus \{(0,0,0)\}$ на классы эквивалентности. Эти классы эквивалентности будем называть проективными точками. Отметим, что при этом либо у всех представителей класса $Z = 0$, либо есть представитель с $Z = 1$. Сопоставим точке $P = (X, Y)$ на кривой класс с представителем $(X, Y, 1)$. Если подставить в 2 $x = \frac{X}{Z^c}, y = \frac{y}{Z^d}$ и избавиться от знаменателя, то можно получить уравнение кривой в проективных кординатах. Проективные точки с $Z = 0$, удовлетворяющие уравнению, будут считаться точками на бесконечности. Различный выбор c и d порождает разные виды проективных координат:

Стандартные проективные координаты: $c = 1$, $d = 1$ В данном случае проективной точке $(X : Y : Z)\,, Z \neq 0$, сопоставляется афинная точка $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$. При подстановке (2) переходит в

$$Y^2 Z = X^3 + aX^2 Z + bZ^3 \tag{7}$$

Этому уравнению удовлетворяет точка $(0 : 1 : 0)$ - ей будет соответствовать афинная точка ∞. Заменим в (5) афинные координаты на проективные, при этом в выражении для Y'_R учтя, что $x_P - x_R = 2 * x_P + x_Q - \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2$:

$$\begin{aligned}
\text{Пусть } M &= Y_Q Z_P - Y_P Z_Q, \quad N = X_Q Z_P - X_P Z_Q. \quad \text{Тогда} \\
X'_R &= \left(\frac{M}{N}\right)^2 - \frac{X_P Z_Q + X_Q Z_P}{Z_P Z_Q} = \frac{M^2 Z_P Z_Q - N^2 \left(X_P Z_Q + X_Q Z_P\right)}{N^2 Z_P Z_Q} \\
Y'_R &= \left(\frac{M}{N}\right)\left(2 * \frac{X_P}{Z_P} + \frac{X_Q}{Z_Q} - \left(\frac{M}{N}\right)^2\right) - \frac{Y_P}{Z_P} = \\
&= \frac{M\left(N^2 \left(2 * X_P Z_Q + X_Q Z_P\right) - M^2 Z_P Z_Q\right)}{N^3 Z_P Z_Q} - \frac{Y_P}{Z_P}
\end{aligned}$$

Пользуясь соотношением эквивалентности, избавимся от знаменателя, задав $Z_R = N^3 Z_P Z_Q$:

$$\begin{aligned}
X_R &= N M^2 Z_P Z_Q - N^3 \left(X_P Z_Q + X_Q Z_P\right) \\
Y_R &= M\left(N^2 \left(2 * X_P Z_Q + X_Q Z_P\right) - M^2 Z_P Z_Q\right) - Y_P Z_Q N^3 \\
Z_R &= N^3 Z_P Z_Q
\end{aligned} \tag{8}$$

Аналогичным образом выводятся формулы для удвоения точки:

$$\begin{aligned}
X_R &= M^2 N - 4N^2 X_P Y_P \\
Y_R &= 6X_P Y_P M N - M^3 - 2N^2 Y_P^2 \\
Z_R &= N^3,
\end{aligned} \tag{9}$$

где $M = 3X_P + aZ_P^2, N = 2Y_P Z_P$. Как видно, в случае выбора этих кординат нет нужды производить инверсию в поле - операцию гораздо более трудоемкую, нежели сложение или умножение.

Проективные координаты Якоби: $c = 2, d = 3$ Проективной точке $(X : Y : Z), Z \neq 0$, сопоставляется афинная точка $\left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$. Уравнение кривой выглядит следующим образом:

$$Y^2 = X^3 + aXZ^4 + bZ^6 \tag{10}$$

Используя рассуждения, подобные использовавшимся в предыдущем пункте, получаем формулы для сложения

$$\begin{array}{rcl} M & = & Y_Q Z_P^3 - Y_P Z_Q^3, \quad N = X_Q Z_P^2 - X_P Z_Q^2 \\ X_R & = & M^2 - N^2 \left(X_P Z_Q^2 + X_Q Z_P^2\right) \\ Y_R & = & MN^2 \left(2X_P Z_Q^2 + X_Q Z_P^2\right) - M^3 - Y_P Z_Q^3 N^3 \\ Z_R & = & Z_P Z_Q N \end{array} \tag{11}$$

и удвоения:

$$\begin{array}{rcl} X_R & = & \left(3X_P^2 + aZ_P^4\right)^2 - 8X_P Y_P^2 \\ Y_R & = & \left(3X_P^2 + aZ_P^4\right)\left(4X_P Y_P^2 - X_R\right) - 8Y_P^4 \\ Z_R & = & 2Y_P Z_P \end{array} \tag{12}$$

4. Заключение

Текст заключения.

Литература

1. *Hankerson D., Menezes A., Vanstone S.* - Guide to Elliptic Curve Cryptography. — New York: Springer-Verlag, 2004 — 311 P.
2. *Коблиц Н.* Курс теории чисел и криптографии. — М.: Научное издательство ТВП, 2001. — 254 С.
3. *Владимиров С.М. [и др.]* - Криптографические методы защиты информации. — М.: МФТИ, 2016. — 266 С.