

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 логарифма 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, передаваемый 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-Гамала, шифр RSA и другие.

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. 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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

© Захаров П. С., Пискун М. Г., 2018

© Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)», 2018

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

$$y^2 = x^3 + ax + b, a, b, x, y \in K \quad (2)$$

### Определение 2.

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

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

Если кривая не является суперсингулярной, т.е. На основе этой проблемы 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 из  $[1, q-1]$ . Дальнейшие вычисления:

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

Пара  $(r, s)$  - подпись.

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

$$\begin{aligned} v_1 &= s^{-1}h \bmod q \\ v_2 &= s^{-1}r \bmod q \\ v_1P + v_2Q &= (x_b, y_b) \\ \hat{r} &= x_b \bmod q \end{aligned} \quad (4)$$

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  $R = P + Q$

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

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  $K^3 \setminus \{(0, 0, 0)\}$ :

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

Оно разбивает  $K^3 \setminus \{(0, 0, 0)\}$  на классы эквивалентности. 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 координатах. Классы с  $Z = 0$ , удовлетворяющие уравнению, будут считаться точками на бесконечности. Различный выбор  $c$  и  $d$  порождает разные виды проективных координат:

**Стандартные проективные координаты:**  $c = 1, d = 1$

## 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.