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, 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-Гамаля, 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

Эллиптической кривой 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]:

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

Если к множеству точек кривой добавить ∞, то на получившемся множестве E можно ввести операцию сложения (и, соответсвенно, умножения на целое) [1]. Нетрудно показать, что E с соотвествующим образом определенной операцией является группой. В данной группе имеет место проблема дискретного логарифма для точек на эллиптических кривых: При данных точках G и $P = aG, a \in \mathbb{Z}$, *сложно определить* a. 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 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:

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

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

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

4. Заключение

Текст заключения.

Работа выполнена при поддержке Минобрнауки, проект № 10А.100.

Литература

1. *Шевченко Д. В., Шевченко В. П.* Выбор и оптимизация структуры построения автономных сейсмических средств обнаружения рубежного типа // Материалы VIII всероссийской научно-технической конференции «Современные охранные технологии и средства обеспечения комплексной безопасности объектов». — 2010. — С. 128–133.
2. *Diallo M. S., Kulesh M., Holschneider M., Sherbaum F., Adler F.* Characterization of polarization attributes of seismic waves using continuous wavelet transforms // Geophysics. — 2006. — V. 71, N. 3. — P. 67–77.
3. *Лайонс Р.* Цифровая обработка сигналов. — М.: Бином, 2006. — С. 361–369.