Секция «Математика»

Сравнительный анализ вычисления кратных точек на эллиптических кривых

Хазиева Вера Денисовна
Студент (бакалавр)
Казанский (Приволжский) федеральный университет, Институт вычислительной математики и информационных технологий, Казань, Россия
E-mail: VDKhazieva@stud.kpfu.ru

В 1985 году Н.Коблицем и В. Миллером было предложено использовать эллиптические кривые для построения ассиметричных криптосистем. Применение данных кривых в криптографии позволяет более эффективно решать проблемы информационной безопасности [1].

Криптография с открытым ключом на базе эллиптических кривых связана с использованием односторонней функции: нахождение кратной точки (операция скалярного произведения **kP**, где **k** — некоторое целое число, а **P** — точка на кривой) вычисляется достаточно просто, а вот задача дискретного логарифмирования, т.е нахождение целого **k**, не имеет субэкспоненциальных алгоритмов для решения. В данной работе анализируются методы и алгоритмы, позволяющие ускорить вычисление операций сложения, удвоения и вычисление кратных точек на эллиптических кривых над конечными полями; приводится сравнение данных операций на эллиптических кривых разных форм.

Определение 1. Пусть F_q является конечным полем. Тогда эллиптической кривой над полем F_q называется множество точек $(x, y) \subseteq (F_q)^2$, удовлетворяющих уравнению Вейерштрасса:

$$y^2 + ay + b = x^3 + cx^2 + dx + e \tag{1}$$

Если характеристика поля $\neq 2$ и $\neq 3$, то уравнение (1) можно преобразовать в уравнение вида

$$y^2 = x^3 + ax + b \tag{2}$$

Одним из вариантов ускорения операций сложения точек и удвоения точки является переход от аффинных координат к проективным. Повышение производительности происходит за счет того, что мы избегаем вычисления обратного элемента. Также существует метод смешанного сложения, где координаты первой точки заданы в проективных координатах, а второй — в афинных. Число операций, затрачиваемых на данную модификацию, равно $9M+2S$, где M — операция умножения, а S — операция возведения в степень. Сложение же точек в проективных координатах расходует $12M + 2S$ операций, что значительно затратнее.

Далее возможен переход от канонического представления (2) к другим формам эллиптических кривых, например, к уравнению кривой в форме Эдвардса:

$$x^2 + y^2 = c^2(1 + dx^2y^2) \tag{3}$$

В работе Д.Берштейна и Т.Ланге [3] доказывается, что эта форма кривой способна увеличить скорость вычисления операций. Существуют и другие известные формы эллиптических кривых, которые заслуживают отдельного внимания и изучения.

Кроме того, имеются различные алгоритмы для скалярного произведения точек: оконные методы, алгоритм Монтгомери и другие [4]. Существуют способы распараллеливания вычислений [2].

Таким образом, в данной работе, путем комбинирования различных вариантов форм кривых, координатных представлений точек и алгоритмов сложения и удвоения, проводится анализ быстродействия вычисления кратных точек на эллиптических кривых. Будут представлены формулы вычисления кратных точек высокого порядка и проведен анализ быстродействия по сравнению с вычислениями, использующими кратные точки меньшего порядка.

Источники и литература

1) Соколов А. А. Формирование цифровой подписи на основе эллиптических кривых // Вестник магистратуры. 2015. Т. 1, № 6(45). С. 25–30.
2) Василенко О. Н. Новые методы вычисления кратной точки на эллиптической кривой над конечным полем // Труды по дискретной математике. 2008. Т. 11, № 2. С. 5–30.
3) Bernstein D., Lange T. Faster addition and doubling on elliptic curves // In International conference on the Theory and Application of cryptology and Information security, Kuching, Malaysia, 2007, P. 29–50.
4) Hankerson D., Menezes A., Vanstone S. Guide to elliptic curve cryptography. New York: Springer, 2004.