Автор:

Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская обалсть

ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИИ

Аннотация*: в статье рассматриваются общие принципы применения эллиптических кривых в криптографии. В основе работы лежат понятия об эллиптических кривых, криптографии, уравнении.*

Ключевые слова*: эллиптические кривые, уравнения, криптография.*

Введение

Эллиптической кривой – это множество точек, которые удовлетворяют уравнению $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Это уравнение можно привести к канонической форме (форме Вейерштрасса), если характеристика поля, рассматриваемого уравнения, не равна 2 или 3:

$$y^2 = x^3 + ax + b.$$

При характеристике поля равной *3*, канонический вид уравнения будет

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

И если характеристика поля равна *2*, то уравнение можно привести к двум видам:

$$y^2 + cy = x^3 + ax + b \text{ или } y^2 + xy = x^3 + ax^2 + b.$$

Эллиптические кривые в криптографии

Важным моментом является то, что все рассмотренные до этого кривые являются эллиптическими кривыми над вещественными числами. Пользуясь кривыми над вещественными числами, невозможно получить биекцию между исходным текстом и зашифрованными данными, из-за этого возникает проблема

округления. Чтобы данная проблема не возникала, в криптографии используются только эллиптические кривые над конечными полями. В таком случае, эллиптической кривой будет являться набор точек, координаты которых принадлежат конечному полю.

В криптографии на сегодняшний день используются два вида эллиптических кривых: над конечным полем Z_P, которое является кольцом вычетов по модулю простого числа. А также над полем $GF(2^m)$, являющимся бинарным конечным полем.

Эллиптических кривые обладают важным свойством над полем $GF(2^m)$. Элементы поля $GF(2^m)$ можно легко представить в виде n-битных кодовых слов, это позволяет ускорить аппаратную реализацию эллиптических алгоритмов.

Опираясь на законы конечного поля, над которым эллиптическая кривая построена, производятся все математические операции на эллиптических кривых над конечным полем. Например, при вычислении суммы двух точек эллиптической кривой E над кольцом вычетов Z_P операции производятся по модулю числа p.

Впрочем, если сложить два одинаковых элемента из бинарного конечного поля, то в результате получается 0, поскольку сложение происходит по модулю 2. Получается, что характеристика этого поля равна 2. Но эллиптическая кривая вида $y^2 = x^3 + ax + b$, описанная над полем характеристики 2 или 3, становится сингулярной, что является нежелательным для использования в криптографии.

Поэтому над бинарным конечным полем применяются кривые вида:

$$y^2 + xy = x^3 + ax^2 + b, \text{ где } b \neq 0.$$

Порядок эллиптической кривой является так же важным понятием эллиптической криптографии, показывающий количество точек кривой над конечным полем.

Теорема Хассе гласит, что при количестве точек N кривой, которая определена над полем Z_q с q элементами, справедливо равенство:

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

Учитывая, что бинарное конечное поле $GF(2^n)$ состоит из 2^n элементов, можно утверждать, что порядок кривой $E_2^n(a,b)$ равен 2^n+1-t, где $|t| \leq \sqrt{(2^n)}$.

Если t делится на характеристику поля без остатка, эллиптическая кривая над бинарным конечным полем в таком случае называется *суперсингулярной*.

Криптография на эллиптических кривых

Группа образуют если все точки эллиптической кривой над конечным полем. И для такой группы определены операция сложения и умножения точки G на число k, представляя умножение как сумма G+G+..+G из k слагаемых.

Допустим, имеется сообщение M, которое представлено в виде целого числа. Зашифровать сообщение можно пользуясь выражением: C=M*G.

Возникает задача определения сложности восстановления сообщения M, при известных параметрах кривой E(a,b), зашифрованного текста C и точки G.

Данная задача является дискретным логарифмом на эллиптической кривой, и быстрого решения она не имеет. Для решения дискретного логарифма на конечном поле существуют сравнительно быстрые алгоритмы, которые имеют сложность $O(\exp(c(\log p \log\log p)^d))$, где p является размером поля, а c и d некоторыми константами. Данные алгоритмы называются «субэкспоненциальные» и позволяют достаточно легко раскрывать дискретный логарифм в конечном поле, при условии, что размер поля очень большой, порядка 2^{1024}. Наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность $O(\sqrt{q})$, где q – количество точек эллиптической кривой. Таким образом, для обеспечения уровня стойкости в 2^{80} операций нужно, чтобы значение $q=2^{160}$. При вычислении дискретного логарифма в конечном поле необходимо поле порядка $q=2^{1024}$, чтобы получить аналогичный уровень сложности.

Список литературы

1. Дмитриев Е.А. Применение эллиптических кривых в криптографии / Е.А. Дмитриев, И.В. Танаев, В.В. Швейкин [и др.] // Научное сообщество студентов XXI столетия. Технические науки: Сб. ст. по мат. XLV междунар. студ. науч.-практ. конф. – №8 (44) [Электронный ресурс]. – Режим доступа: https://sibac.info/studconf/tech/xlv/60564 (дата обращения: 26.01.2018).