Методы и алгоритмы генерации эллиптических кривых для криптографии

Екатерина Малыгина

07.02.2023

1 Наивный метод

Алгоритм 1 Наивный метод

Вход: p – характеристика конечного поля, $N = |E(\mathbb{F}_p)|$.
Выход: Уравнение кривой $E/\mathbb{F}_p$ с числом точек N.

$P := (1, 1)$.
$t := p + 1 - N$.
$i := 0$.
$S := \mathbb{F}_p \backslash \{\frac{-27}{4}\}$.
Повторять
    Выбрать случайным образом $a \in S$.
    Положить $E/\mathbb{F}_p : y^2 = x^3 + ax - a$.
    Если $(p + 1 - t)P =$, **то**
        вернуть кривую E.
    Конец условия
    Если $(p + 1 + t)P =$, **то**
        вернуть квадратичное скручивание кривой E.
    Конец условия
    $S := S \backslash \{a\}$.
Пока $S = \varnothing$.