УДК 004.056.55

**Представления точек на эллиптических кривых**

*П.С.Захаров, М.Г.Пискун*

Московский физико-технический институт (государственный университет)

В настоящее время получают распространение криптографические алгоритмы на эллиптических кривых над конечными полями:

,

где K – некоторое конечное поле. В основе этих алгоритмов лежит проблема дискретного логарифма для точек на эллиптической кривой над конечным полем[1]: если известны ненулевые точки на эллиптической кривой *P* и *Q,* такие, что *Q=d\*P*, , а *d -* нет, то найти *d* вычислительно сложно.

Основой данных алгоритмов являются арифметические операции над точками кривой. Они включают в себя умножения, сложения и инверсии в конечном поле. Классическое представление *(x, y)* наиболее просто в исполнении, однако не оптимально. В статье рассматриваются другие представления - проективные координаты, Якобианские координаты, координаты Чудновского и соответствующие оптимизации вычислений.

Вышеуказанные представления, тем не менее, требуют больше памяти для реализации. Кроме того, существуют некоторые оптимизации, которые эффективны при определенных паттернах вычислений (скажем, много умножений подряд).[2] Для иллюстрации поставлен вычислительный эксперимент – реализован алгоритм цифровой подписи ECDSA с использованием различных представлений точек. Проведено сравнение полученных вариантов алгоритма с точки зрения памяти, быстродействия и т.д.

**Литература**

1. *Владимиров С.М. [и др.]* Криптографические методы защиты информации. М.: МФТИ, 2016. 266 с.
2. *Hankerson D., Menezes A., Vanstone S.* - Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004. 311 p.