УДК 004.056.55

**Представления точек на эллиптических кривых**

Захаров Павел Сергеевич, Пискун Максим Григорьевич

Московский физико-технический институт (государственный университет)

В статье рассмотрены актуальные на текущий день криптографические алгоритмы, использующие эллиптические кривые над конечными полями.[1] Рассмотрены основные виды представления данных (точек на кривых, чисел и т.д.), используемые операции в группах точек на кривых, их влияние на скорость вычислений.[2] Поставлен вычислительный эксперимент – написаны модели, использующие различные типы представления. Таким образом, проведено сравнение производительности криптографических алгоритмов на эллиптических кривых.

**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.