УДК 681.3.06

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ КРИПТОСТОЙКИХ КРИВЫХ ЭДВАРДСА НАД ПРОСТЫМИ ПОЛЯМИ

Анатолий Бессалов, Алиса Дихтенко*

*ИССЗИ НТУУ «КПИ», *ДонНУ*

Аннотация: Рассмотрена форма Эдвардса эллиптической кривой. Приведены явные формулы изоморфного преобразования канонической эллиптической кривой в кривую Эдвардса и обратно. Найдено 40 приемлемых для криптографии кривых в форме Эдвардса над простыми полями, получены координаты генераторов криптосистем.
Ключевые слова: эллиптические кривые, каноническая форма, форма Эдвардса, изоморфизм, порядок кривой и точки, генератор криптосистемы.

Среди различных форм представления эллиптических кривых особое место занимает кривая в форме Эдвардса. Они обладают рядом замечательных свойств. Закон сложения точек кривой Эдвардса отличает свойства универсальности и полноты, точка на бесконечности заменяется нейтральным элементом (0,1) в аффинных координатах. Решающим преимуществом их является средний выигрыш в быстродействии в 1.5 раза в сравнении с каноническими кривыми при расчете скалярного произведения в проективных координатах. В этой связи кривые Эдвардса представляют выгодную альтернативу каноническим эллиптическим кривым в перспективных стандартах асимметричной криптографии.

Поиск кривых Эдвардса, приемлемых для криптографии, представляет собой нетривиальную задачу. Ключевым моментом в ней является расчет порядка кривой, заданной над конечным полем. В ранних работах авторов для поиска кривых Эдвардса почти простого порядка был предложен подход, в котором для найденных кривых над полями $\mathbf{F}_5$ и $\mathbf{F}_7$ с минимальным порядком 4 найдены кривые приемлемого почти простого порядка $4n$ в расширениях этих полей.

В докладе представлены результаты решения задачи поиска криптостойких кривых Эдвардса с почти простым порядком $4n$ не над расширениями малых полей, а над большими простыми полями. Обсуждается проблема определения порядка кривой Эдвардса и кратко описываются возможные пути ее решения. На основе метода SEA, изоморфизма кривых Эдвардса и канонических кривых были найдены порядки 40 кривых Эдвардса над простыми полями $\mathbf{F}_p$ с модулями p длиной 192, 224, 256 и 384 бит, а также координаты генераторов криптосистем. Найденные кривые удовлетворяют стандартным требованиям к порядку генератора криптосистемы и с большим успехом могут применяться на практике.