УДК 004.056

ИСПОЛЬЗОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД РАЦИОНАЛЬНЫМИ ЧИСЛАМИ В КРИПТОГРАФИЧЕСКИХ СХЕМАХ

Давыдов В.В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – д.т.н., доцент Беззатеев С.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Данная работа посвящена исследованию использования эллиптических кривых, которые определены над полем рациональных чисел, в криптографических схемах.

Сегодня в криптографических схемам используются эллиптические кривые. Большинство таких схем построены на двух основных задачах: задача вычисления дискретного логарифма в группе точек эллиптической кривой и задача поиска пути в графе изогений. В современных криптографических схемах такие кривые используются над конечными полями. Проведено множество исследований, в которых показано, какие кривые и поля следует выбирать для достижения максимальной эффективности и стойкости построенных криптосистем. Однако интересной задачей является исследование применимости эллиптических кривых, определённых над рациональными числами, в криптографических схемах и оценка стойкости таких схем.

Пусть E – эллиптическая кривая, определённая над полем рациональных чисел. По теореме Морделла группа рациональных точек $E(Q)$ – это конечно сгенерированная абелева группа. По теореме Мазура E(Q) также имеет подгруппы кручения; доказано, что это за подгруппы. Более того, по теореме Нагелла-Лутца становится понятна зависимость между координатами генераторной точки кручения и дискриминантом эллиптической кривой. Следовательно, использование кривых над полем рациональных чисел в криптографии возможно. Использование кривых с рангом, большим нуля, представляет интересную задачу. На сегодняшний день неизвестно, есть ли ограничение сверху на значение ранга. Основной проблемой является сложность поиска кривых с большим значением ранга. Для кривых над рациональными числами с малым рангом использование в криптографических схемах затруднительно из-за предсказуемости получения значений координат точек, вследствие чего представляется возможным определить, каким образом генерировались точки. Однако если удастся найти кривые с большим рангом, то использование таких кривых в криптосистемах станет актуальным. Для поиска таких кривых используется гипотеза Бёрча-Свиннертон-Дайера, а также сумма Местре-Нагао и некоторые другие инструменты. Тем не менее, кривые невысоких рангов могут быть использованы при криптоанализе, например, для быстрой факторизации чисел.

В работе проведено исследование применимости эллиптических кривых над полем рациональных чисел в криптографических схемах. В дальнейшем планируется более детальное изучение гипотезы Бёрча-Свиннертон-Дайера, а также поиск методов для получения кривых высокого ранга.

Давыдов В.В. (автор)

Подпись

Беззатеев С.В. (научный руководитель)

Подпись