ОТЗЫВ

на автореферат диссертации Николаева Максима Владимировича «О сложности решения некоторых обобщений задачи дискретного логарифмирования», представленной на соискание учёной степени кандидата физико-математических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки)

Задача дискретного логарифмирования является одной из наиболее актуальных задач теоретической информационной безопасности. Это подтверждается большим количеством современных механизмов защиты информации (например, схем цифровой электронной подписи), использующих для обоснования своей стойкости трудоемкость решения различных обобщений задачи дискретного логарифмирования. Использование алгоритма Годри-Шоста является перспективным подходом к решению обобщений классической задачи: двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале. Именно этот подход Николаев М.В. развивает в диссертации. Автором выполнена разработка алгоритмов решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой в следующих случаях:

- эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов,
- эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов,
- эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов.

Для каждого из указанных случаев разработанные алгоритмы имеют наименьшую известную оценку средней трудоемкости.

Кроме того, диссертантом разработана модификация алгоритма Годри-Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, получена оценка средней трудоемкости разработанного алгоритма.

В качестве замечаний можно указать следующие моменты.

1. Для практики снижение стойкости не более чем в 2 раза, да и то для специальных кривых, не представляет проблемы. Экспоненциальная часть сложности от битовой длины величины интервала/размерности подгруппы осталась неизменной.

2. Автореферат не позволяет понять, почему собственно удалось понизить оценку сложности. Намек на варьирование размеров и формы домашних и диких множеств дан, но суть все же ускользает.

Считаю, что отмеченные недостатки не снижают общей ценности работы и качества автореферата.

Достоверность и обоснованность полученных результатов диссертационной работы подтверждаются математическими доказательствами и публикациями в изданиях, удовлетворяющих требованиям Положения о присуждении ученых степеней в МГУ имени М.В. Ломоносова.

Считаю, что автореферат диссертации М.В. Николаева в полной мере характеризует соответствие диссертации критериям, установленным «Положением о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», утвержденным Ректором МГУ 27 октября 2016 года. Таким образом, автор диссертации Николаев Максим Владимирович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

кандидат физико-математических наук,
заместитель генерального директора
ОАО «ИнфоТеКС»
Уривский Алексей Виктор

«25» мая 2018 г.

Подпись Уривского А.В. заверяю.

Начальник А.М. Бурменко
Отдела кадров