

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)

Диссертационная работа М.В. Николаева посвящена актуальной теме разработки алгоритмов решения различных вариантов задачи дискретного логарифмирования. Автором разработаны наиболее эффективные алгоритмы решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а также решения задачи дискретного логарифмирования в интервале для групп с эффективным инвертированием.

Следует отметить, что до работ М.В. Николаева оставался неизученным вопрос существования алгоритма решения двумерной задачи дискретного логарифмирования, использующего наличие у группы эффективного автоморфизма порядка 6. Для указанного случая диссертантом разработана модификация алгоритма Годри-Шоста и получена оценка средней трудоемкости, что позволяет говорить о завершении целого ряда исследований, посвященных решению двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами.

Определенным недостатком текста автореферата, на мой взгляд, является отсутствие описания свойств рассматриваемых групп точек эллиптических кривых с эффективным автоморфизмом. Указанный недостаток не снижает общего положительного впечатления о диссертационной работе.

Диссертация Николаева М.В. представляет собой законченную исследовательскую работу, направленную на решение актуальных задач, выполненную на высоком методическом уровне и имеющую важное научное значение. Основные результаты, полученные диссертантом, доложены на ряде всероссийских и международных научных конференций, а также опубликованы в журналах, определенных п.2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Диссертационная работа М.В. Николаева «О сложности решения некоторых обобщений задачи дискретного логарифмирования» отвечает критериям, установленным Положением о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова для кандидатских диссертаций, а ее автор заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

доктор физико-математических наук,
профессор, профконсультант
Консультационно-методического центра РГГУ
Максимов Валерий Михайлович

«23» мая 2018 г.

Годится Максимов В. М. удостоверяю

