Отзыв научного руководителя на диссертационную работу Николаева Максима Владимировича «О сложности решения некоторых обобщений задачи дискретного логарифмирования», представленную к защите на соискание учёной степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Николаева М.В. посвящена исследованию трудоёмкости решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале в конечной циклической группе простого порядка, обладающей так называемым эффективным автоморфизмом, т. е. автоморфизмом, для которого вычисление орбиты любого элемента группы может быть выполнено существенно быстрее групповой операции. В работе рассматриваются практически важные примеры таких групп — подгруппы большого простого порядка группы точек эллиптической кривой $y^2 = x^3 + Ax^2 + B$ над конечным простым полем из $p > 3$ элементов в следующих случаях:

1) A, B, p – произвольные (эффективный автоморфизм порядка 2 — операция вычисления обратного элемента);
2) $B = 0, p \equiv 1 \bmod 4$(эффективный автоморфизм порядка 4);
3) $A = 0, p \equiv 1 \bmod 3$ (эффективный автоморфизм порядка 6),

для которых известны соответствующие модификации алгоритма Полларда решения классической задачи дискретного логарифмирования.

Диссертация состоит из введения, четырёх глав, заключения, списка сокращений и обозначений, двух приложений и списка литературы.

Глава 1 диссертации представляет собой систематизированное изложение формулировок задач, наиболее интересных примеров их практического применения в области защиты информации, известных результатов по теме исследования, необходимого математического аппарата. Несомненным достоинством данной главы является наличие в ней отдельного параграфа (1.4),

в котором обсуждается влияние трудоёмкости вычисления орбиты точки эллиптической кривой под действием эффективного автоморфизма на общую трудоёмкость использующих такой автоморфизм модификаций итерационных алгоритмов решения задачи дискретного логарифмирования и ее обобщений, в том числе алгоритма Годри-Шоста, и делается справедливый вывод о том, что количество выполняемых групповых операций адекватно характеризует трудоёмкость не только исходных, но и модифицированных алгоритмов.

В главе 2 диссертации рассматривается двумерная задача дискретного логарифмирования в случае 3. Для данного случая автором впервые предложена модификация алгоритма Годри-Шоста решения указанной задачи, использующая наличие у группы эффективного автоморфизма, и получена верхняя асимптотическая оценка средней трудоёмкости модифицированного алгоритма, которая меньше оценок, ранее полученных Лиу для случаев 1 и 2. Несмотря на то, что рассмотренный автором случай является наиболее сложным, предложенное им доказательство оценки является более простым, чем доказательства оценок в работе Лиу, за счёт использования условного математического ожидания количества выполняемых алгоритмом групповых операций при условии принадлежности решения задачи различным подмножествам.

В главе 3 диссертации автором предложен оригинальный способ параметризации известных модификаций алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случаях 1-3 и задачи дискретного логарифмирования в интервале в случае 1, и показано, что за счёт выбора значений параметра константы при главных членах в верхних асимптотических оценках средней трудоёмкости решения указанных задач могут быть выбраны сколь угодно близкими к рассчитанным автором «предельным» значениям. Таким образом, автором получены асимптотически наиболее эффективные алгоритмы решения указанных задач. Также в данной главе рассмотрена возникающая на практике ситуация, когда возможно сведение классической задачи дискретного логарифмирования к двумерной задаче, и с использованием рассчитанных «предельных» значений в случаях 2 и 3 сформулированы условия, при которых предложенные автором модификации алгоритма Годри-Шоста решения двумерной задачи будут асимптотически эффективнее соответствующих модификаций алгоритма Полларда решения классической задачи.

Глава 4 диссертации содержит описание и результаты экспериментов, проведенных автором для параметризованных алгоритмов, изложенных в главе 3 диссертации, на конкретных примерах используемых на практике эллиптических кривых при различных входных данных задачи и значениях параметра. Эмпирические средние значения трудоёмкости алгоритмов достаточно хоро-

шо приближаются главными членами полученных в главе 3 соответствующих асимптотических оценок средней трудоёмкости.

В заключении к диссертации приведен краткий перечень полученных автором результатов и описаны возможные перспективы дальнейшей разработки темы. Приложения содержат исходные коды разработанных автором компьютерных программ, которые использовались в ходе исследования, с подробными комментариями.

Диссертация является законченным исследованием, содержащим самостоятельно полученные автором новые результаты, которые вносят существенный вклад в решение практически значимых обобщений задачи дискретного логарифмирования и могут быть использованы при обосновании выбора параметров современных математических методов защиты информации.

Содержание диссертации соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Диссертация оформлена согласно приложениям №№ 5, 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова. Таким образом, диссертационная работа «О сложности решения некоторых обобщений задачи дискретного логарифмирования» отвечает всем требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода, а её автор, Николаев Максим Владимирович, заслуживает присуждения ему учёной степени кандидата физико-математических наук.

Научный руководитель
кандидат физико-математических наук Д.В. Матюхин

Почтовый адрес: 121351, г. Москва, в/ч 43753
Телефон: +7 (916) 501-61-70
Адрес электронной почты: matyukhin_dv@gov.ru

Подпись Матюхина Д.В. удостоверяю.
Командир в/ч 43753 А.М. Ивашко