ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА МГУ.05.01
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Решение диссертационного совета от 6 июня 2018 года № 14

О присуждении Николаеву Максиму Владимировичу, гражданину Российской Федерации, учёной степени кандидата физико-математических наук.

Диссертация «О сложности решения некоторых обобщений задачи дискретного логарифмирования» по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) принята к защите диссертационным советом 18 апреля 2018 года, протокол № 10.

Соискатель **Николаев Максим Владимирович**, 1990 года рождения, в 2012 году окончил ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедру информационной безопасности по специальности «Прикладная математика и информатика». В 2015 году окончил очную аспирантуру в ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности по специальности «Методы и системы защиты информации, информационная безопасность».

Диссертация выполнена в ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» (МГУ имени М.В. Ломоносова), факультет вычислительной математики и кибернетики, кафедра информационной безопасности.

Научный руководитель – кандидат физико-математических наук, **Матюхин Дмитрий Викторович**, сотрудник в/ч 43753.

Официальные оппоненты:

Гашков Сергей Борисович, доктор физико-математических наук, профессор, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», Механико-математический факультет, кафедра дискретной математики, профессор;

Михайлов Владимир Гаврилович, доктор физико-математических наук, старший научный сотрудник, ФГБУН «Математический институт им. В.А. Стеклова Российской академии наук», отдел дискретной математики, ведущий научный сотрудник;

Катышев Сергей Юрьевич, кандидат физико-математических наук, ФГБОУ ВО «МИРЭА - Российский технологический университет», базовая кафедра 252, доцент.

Все официальные оппоненты дали **положительные отзывы** на диссертацию.

Соискатель имеет 3 опубликованные работы, в том числе по теме диссертации 3 работы, из них **3 статьи опубликованы в рецензируемых научных изданиях, индексируемых в Scopus и RSCI**, рекомендованных для защиты в диссертационном

совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

1. М.В. Николаев, Д.В. Матюхин. О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6. Дискретная математика, том 25 (2013), стр. 54–65. (Д. В. Матюхину принадлежит постановка задачи и стилистическое оформление части работы; решение поставленной задачи полностью принадлежит М.В. Николаеву).
2. М.В. Николаев. On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism. Математические вопросы криптографии, том 6 выпуск 2 (2015), стр. 45–57.
3. М.В. Николаев. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием. Прикладная дискретная математика, №2 (2015), стр. 97–102.

На диссертацию и автореферат поступило 5 отзывов, все положительные.

Выбор официальных оппонентов обусловлен тем обстоятельством, что они являются специалистами в области методов и систем защиты информации, информационной безопасности и имеют работы, близкие к теме диссертации соискателя.

Диссертационный совет отмечает, что представленная диссертация на соискание учёной степени кандидата физико-математических наук **является научно-квалификационной работой**, в которой автор, опираясь на разработанные ранее подходы, модифицирует несколькими способами алгоритм Годри–Шоста и, таким образом, **получает наиболее эффективные алгоритмы** решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами и решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием.

Автором получены следующие новые теоретические результаты, которые выдвигались на защиту.

Впервые **разработана модификация алгоритма** Годри-Шоста решения двумерной задачи дискретного логарифмирования при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ в случае эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов, где φ — эффективный автоморфизм порядка 6. **Получена оценка** средней трудоемкости нового алгоритма.

Получены оптимальные оценки (с точки зрения используемых параметров алгоритма Годри-Шоста) средней трудоемкости решения двумерной задачи дискретного

логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p>$ 3 элементов для случаев

- A, B, p – произвольные (эффективный автоморфизм порядка 2 операция вычисления обратного элемента);
- B = 0, p ≡ 1 mod 4 (эффективный автоморфизм порядка 4);
- A = 0, p ≡ 1 mod 3 (эффективный автоморфизм порядка 6).

Разработана модификация алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, а также **получена оценка** средней трудоемкости нового алгоритма.

В силу того, что для двумерной задачи дискретного логарифмирования ранее были получены модификации алгоритма Годри–Шоста лишь для эллиптических кривых, обладающих эффективными автоморфизмами порядков 2 и 4, результаты диссертационной работы восполняют существенный пробел в разработке эффективных вариантов алгоритма Годри-Шоста применительно к рассматриваемым задачам.

Принципиально новый шаг сделан также диссертантом в части оптимизации алгоритма Годри–Шоста, использующего эффективный автоморфизм. Алгоритм Годри-Шоста и его различные модификации оперируют так называемыми «диким» и «домашним» множествами, из которых поочередно выбираются элементы до тех пор, пока не будут найдены совпадающие. Диссертантом предложена удачная параметризация «дикого» множества, связывающая его размер со значением оценки средней трудоемкости алгоритма. Используя эту связь и варьируя размер «дикого» множества, диссертант построил менее трудоемкие алгоритмы (являющиеся модификациями алгоритма Годри–Шоста) и обосновал оценки их средней трудоемкости для задачи дискретного логарифмирования в интервале, а также для двумерной задачи дискретного логарифмирования при N1 = N2.

Полученные автором оценки трудоемкости показывают, что построенные для перечисленных задач алгоритмы являются наиболее эффективными среди известных в настоящее время. Кроме этого, в диссертации приведены описание и результаты численных экспериментов для построенных вариантов алгоритма Годри–Шоста. Экспериментальные данные хорошо согласуются с главными членами полученных теоретических оценок трудоемкости.

Востребованность полученных соискателем результатов на практике подтверждается тем, что они могут использоваться

- для обоснования стойкости конкретных реализаций математических методов

защиты информации;

- в атаках на алгоритмы выработки общего ключа типа Диффи-Хеллмана, а именно в атаках, использующих информацию из побочных каналов утечки, атаках по маленькой подгруппе;
- при анализе трудоемкости решения классической задачи дискретного логарифмирования в группе точек эллиптической кривой, обладающей эффективным автоморфизмом;
- при подсчете числа элементов многообразия Якоби.

Диссертация представляет собой **самостоятельное** законченное **исследование,** обладающее **внутренним единством**. Положения, которые выносились на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку. В ходе проведенных им исследований разработаны наиболее эффективные в настоящее время алгоритмы решения двумерной задачи дискретного логарифмирования для случая подгрупп группы точек эллиптической кривой, обладающей эффективным автоморфизмом порядка 2, 4 или 6, а также решения задачи дискретного логарифмирования в интервале для случая подгрупп группы точек эллиптической кривой (обладает эффективным инвертированием). Все результаты обоснованы строгими математическими доказательствами, результаты диссертации прошли апробацию на международных конференциях и авторитетных научных семинарах. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

С учетом изложенного выше, на заседании 6 июня 2018 года диссертационный совет принял решение присудить Николаеву Максиму Владимировичу учёную степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 24 человек, из них 7 докторов наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность», участвовавших в заседании, из 29 человек, входящих в состав совета, проголосовали: за 24, против 0, недействительных бюллетеней 0.

Заместитель председателя
диссертационного совета,
доктор физико-математических наук,
профессор Васенин Валерий Александрович

Учёный секретарь
диссертационного совета,
кандидат физико-математических наук Кривчиков Максим Александрович

6 июня 2018 года