ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 003.015.01, СОЗДАННОГО НА БАЗЕ федерального государственного бюджетного учреждения науки Института математики им. С.Л. Соболева Сибирского отделения Российской академии наук (Федеральное агентство научных организаций), ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 18 мая 2022 г. №1/2

О присуждении Новоселову Семену Александровичу, гражданину Российской Федерации, учёной степени кандидата физико-математических наук.

Диссертация «Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом» по специальности 01.01.09 – дискретная математика и математическая кибернетика – принята к защите 18 февраля 2022 г., протокол № 1/1, диссертационным советом Д 003.015.01, созданным на базе ФГБУН «Институт математики им. С.Л. Соболева СО РАН» (Федеральное агентство научных организаций), находящегося по адресу: 630090, Новосибирская область, город Новосибирск, проспект Академика Коптюга, дом 4 (совет утверждён приказом Минобрнауки РФ №1925-161 от 08.09.2009 г.).

Соискатель Новоселов Семен Александрович, 26 марта 1990 года рождения в 2013 г. окончил Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта», а в 2016 – аспирантуру в том же учреждении. В настоящее время работает младшим научным сотрудником и старшим преподавателем в ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта».

Диссертация выполнена в лаборатории математических методов защиты и обработки информации ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта».

Научный руководитель – кандидат физико-математических наук Малыгина Екатерина Сергеевна, доцент и младший научный сотрудник в ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта».

Официальные оппоненты:

1. Романьков Виталий Анатольевич, доктор физико-математических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского», профессор,

2. Панкратова Ирина Анатольевна, кандидат физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет», заведующая лабораторией компьютерной криптографии,

дали положительные отзывы на диссертацию.

Ведущая организация, Федеральное государственное бюджетное учреждение науки «Институт проблем передачи информации имени А. А. Харкевича» РАН, город Москва, в своём положительном отзыве, подписанном Сергеем Юрьевичем Рыбаковым, кандидатом физико-математических наук, старшим научным сотрудником лаборатории 13 Института проблем передачи информации имени А. А. Харкевича РАН, и утвержденная исполняющим обязанности директора Института проблем передачи информации имени А. А. Харкевича РАН, доктором физико-математических наук, профессором Соболевским Андреем Николаевичем указала, что диссертация Новоселова Семена Александровича соответствует всем требованиям ВАК, а её автор заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Соискатель имеет 7 опубликованных работ все по теме диссертации, из них в рецензируемых научных изданиях из списка ВАК – 4. Наиболее значимыми являются следующие работы:

1. Novoselov S. A. Counting points on hyperelliptic curves of type $y^2 = x^{2g+1}+$

$ax^{g+1} + bx$ // Finite Fields and Their Applications. — 2020. — Vol. 68, no. 101757. — P. 1—27.

2. Novoselov S. A. Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials // Прикладная дискретная математика. — 2017. — № 37. — С. 20—31.

3. Malygina E. S., Novoselov S. A. Division polynomials for hyperelliptic curves defined by Dickson polynomials // Математические вопросы криптографии. — 2020. — Т. 11, № 2. — С. 69—81.

4. Новоселов С. А. Границы сбалансированной степени вложения для криптографии на билинейных спариваниях // Прикладная дискретная математика. — 2016. — Т. 32, № 2. — С. 63—86.

В работах изучается задача подсчета точек на гиперэллиптических кривых и её приложения в криптографии и теории кодирования, предложены новые эффективные алгоритмы для решения данной задачи на специальном классе кривых вместе с оценками её сложности.

Выбор ведущей организации обосновывается тем, что в число её сотрудников входят признанные специалисты в области кривых над конечным полем, математической криптографии и теории кодирования. Выбор официальных оппонентов обусловлен их научным авторитетом и высокой компетентностью в указанных областях. Официальные оппоненты и сотрудники ведущей организации имеют публикации по теме диссертации.

Диссертационный совет отмечает, что:

В диссертации решаются задачи, имеющие существенное значение в области криптографии и теории кодирования. Объектом исследования диссертации является задача нахождения числа точек на гиперэллиптической кривой над конечным полем и связанной с ней группе — якобиане. Предмет исследования — вычислительная сложность данной задачи в случае специального класса кривых с геометрически приводимым якобианом, а также алгоритмы её решения.

Соискателем получены следующие основные результаты:

1) Предложены новые алгоритмы для решения задачи подсчёта точек на кривых с геометрически разложимым якобианом, в частности для кривых Лежандра – Сато.

2) Получены явные формулы для числа точек на кривых Лежандра – Сато рода 3 и, в общем случае, формулы для числа точек по модулю характеристики поля, выраженные через многочлены Лежандра.

3) Получены специализированные алгоритмы для родов 3, 4 на основе многочленов Лежандра и разложения якобиана. Доказано, что сложность данных алгоритмов равна $O(\log^4 q)$ и $O(\log^8 q)$, соответственно. Это позволило существенно снизить сложность задачи подсчёта точек на данном классе кривых, так как общий алгоритм имеет сложность $O(\log^{14} q)$ и $O(\log^{18} q)$, соответственно.

Работа носит как теоретический, так и экспериментальный характер. Результаты диссертации являются новыми, теоретически строго обоснованными и могут быть использованы в исследованиях, проводимых в Институте математики им. С.Л. Соболева СО РАН, Новосибирском государственном университете, Институте проблем передачи информации имени А. А. Харкевича РАН и БФУ им. И. Канта, а также в соответствующих университетских курсах для подготовки специалистов в области криптографии и теории кодирования. Разработанные методы могут использоваться для решения практических задач – генерации кривых для криптографии, анализа стойкости функций задержки, построения АГ-кодов.

Теоретическая значимость исследования заключается в том, что результаты вносят существенный вклад в теорию кривых над конечным полем, математическую криптографию и теорию кодирования.

Практическая значимость исследования обусловлена возможностью использовать разработанные алгоритмы для генерации кривых для криптографии, анализа стойкости верифицируемых функций задержки и генерации максимальных кривых для построения оптимальных АГ-кодов.

Оценка достоверности результатов исследования показала, что результаты диссертации точно сформулированы и снабжены строгими математическими доказательствами, все полученные соискателем результаты согласуются с ранее опубликованными работами по теме диссертации.

Личный вклад соискателя заключается в том, что все основные результаты диссертации получены им лично, соискатель лично докладывал результаты на семинарах, всероссийских и международных научных конференциях.

Диссертационный совет пришёл к выводу о том, что диссертация Новоселова Семена Александровича представляет собой научно-квалификационную работу, которая соответствует критериям, установленным Положением о порядке присуждения учёных степеней, утвержденным постановлениями Правительства Российской Федерации от 24 сентября 2013 г. №842 и 21 апреля 2016 г. №335, а её автор заслуживает присуждения учёной степени кандидата физико-математических наук.

На заседании 18 мая 2022 г. диссертационный совет принял решение присудить Новоселову Семену Александровичу учёную степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 10 докторов наук по специальности 01.01.09 – дискретная математика и математическая кибернетика, участвовавших в заседании, из 16 человек, входящих в состав совета, проголосовали: за – 16, против – нет, недействительных бюллетеней – нет.

Заместитель председателя
диссертационного совета Береснев Владимир Леонидович

Учёный секретарь
диссертационного совета Батуева Цындыма Чимит-Доржиевна

18 мая 2022 г.