Федеральное государственное
бюджетное учреждение науки
Институт проблем
передачи информации
им. А. А. Харкевича
Российской академии наук

ИППИ РАН

Большой Каретный пер., д. 19, стр. 1, Москва, 127051
ОКПО: 02699464 ОГРН: 1037700064940
ИНН/КПП: 7707020131/770701001
тел.: (495) 650-42-25 | факс: (495) 650-05-79 | director@iitp.ru

25.04. 2022 г. №11615-2115/119

На № _____ от _____

УТВЕРЖДАЮ
И.о. директора ИППИ РАН
д-р физ.-мат. наук, профессор РАН

_____ А. Н.Соболевский
«26» ___ апреля 2022г.

Отзыв ведущей организации
на диссертацию С. А. Новоселова
«Подсчёт числа точек на гиперэллиптических кривых
с геометрически разложимым якобианом»,
представленную на соискание ученой степени кандидата физико-математических наук по специальности 01.01.09 – Дискретная математика и математическая кибернетика

Диссертация посвящена проблеме вычисления порядка группы точек якобиана гиперэллиптической кривой над конечным полем. Эта задача является важной одновременно и для теории алгебраических кривых и для приложений в криптографии и теории кодирования.

Хорошо известно, что якобианы для кривых малых родов могут быть рассмотрены в качестве источника циклических групп, которые являются приемлемыми для проблемы дискретного логарифмирования. Данная проблема оказывается наиболее трудоемкой для групп большого простого порядка. Определять число точек на якобиане кривой можно при помощи обобщения Пилэ на многомерный случай классического алгоритма Схоофа для эллиптических кривых. Однако, несмотря на его асимптотическое полиномиальное время работы, в многомерии он все-таки невыполним над конечными полями криптографического размера.

Целью диссертации является построение быстрых алгоритмов подсчета точек на якобианах кривых специального вида, у которых над конечным расширением якобиан изогенен произведению абелевых многообразий меньшей размерности, то есть геометрически приводим. В диссертации также вычислены характеристические многочлены Фробениуса по модулю p для кривых малых родов (от 2 до 7).

Особенно отметим, что результаты диссертации были представлены на таких общепризнанных тематических конференциях как Algorithmic Number Theory Symposium и Workshop on Elliptic Curve Cryptography.
Диссертация состоит из введения, 4 глав, заключения, списка литературы и четырех приложений. Общий объем диссертации 155 страниц. Во введении изложена история вопроса, постановка задачи и кратко сформулированы основные результаты работы. В первой главе приводятся основные определения и результаты, используемые в работе.

В главе 2 доказаны основные технические результаты диссертации. Во-первых, предложен общий метод восстановления характеристического многочлена эндоморфизма Фробениуса абелева многообразия над конечным полем, если известен аналогичный характеристический многочлен над некоторым конечным расширением основного поля. Также дается оценка вычислительной сложности полученного алгоритма в некоторых специальных случаях, которых вполне достаточно для целей диссертации. Во-вторых, предложен алгоритм вычисления числа точек на гиперэллиптических кривых с уравнением $y^2 = x^{2g+1} + ax^{g+1} + bx$ над некоторым конечным расширением у таких кривых много автоморфизмов, поэтому над этим расширением якобиан изогенен произведению якобианов кривых меньшего рода. Если род у этих кривых достаточно мал, то вычислить характеристические многочлены эндоморфизма Фробениуса их якобианов намного легче. После этого автор использует алгоритм из первой части главы.

В главе 3 получены результаты, уточняющие результаты главы 2 для кривых рода 3 и 4. Глава четыре посвящена приложениям в криптографии. В частности, построены интересные примеры кривых рода 3 и 4 над большим конечным полем. К сожалению, пока не стоит ожидать непосредственного практического применения диссертации в реальных системах защиты информации.

Замечания. Диссертация содержит ряд неточностей. Например, на стр. 20 якобиан кривой определен как абелева группа, а не как абелево многообразие. На стр. 30 скрутка (twist) абелева многообразия названа кручением, что можно перепутать с группой точек конечного порядка (torsion).

Вышесказанное нисколько не уменьшает научную ценность работы. Все результаты являются новыми, интересными и важными.

Заключение. Диссертация С. А. Новосёлова посвящена поиску быстрых алгоритмов вычисления порядка группы точек якобиана гиперэллиптической кривой над конечным полем. Этой проблеме посвящена обширная литература, поэтому каждое новое продвижение дается со все большим трудом. Автор получил интересные результаты, которые могут быть со временем использованы для построения криптографических систем с открытым ключом.

Результаты диссертации опубликованы в семи статьях, из них четыре в ведущих рецензируемых изданиях из списка ВАК. и прошли апробацию на нескольких авторитетных отечественных и международных семинарах и конференциях. Все результаты снабжены подробными и полными доказательствами. Результаты изложены четко, полно и строго. Автореферат правильно отражает содержание диссертации.

Результаты диссертации могут быть рекомендованы для использования в работе специалистов по дискретной математике и алгебраической геометрии над конечными полями, работающих, например, в МГУ им. Ломоносова и ИППИ РАН, а также специалистов по криптографии, работающих, например, в ММФ НГУ и Институте математики им. С. Л. Соболева СО РАН.

На основании вышеизложенного можно заключить, что диссертация С. А. Новоселова «Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом» удовлетворяет всем требованиям ВАК и паспорту специальности 01.01.09 — Дискретная математика и математическая кибернетика, а ее автор, Новоселов Семен Александрович, заслуживает присуждения ученой степени кандидата физико-математических наук.

Отзыв обсужден и одобрен на заседании семинара лаборатории 13 федерального государственного бюджетного учреждения науки Институт проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН) 25 апреля 2022 г.

С.н.с. лаборатории 13, секретарь семинара,
кандидат физико-математических наук _____ С.Ю. Рыбаков