ОТЗЫВ

научного руководителя о диссертации С. А. Новоселова

«Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом»,

представленной на соискание ученой степени кандидата физико-математических наук по специальности 01.01.09 — дискретная математика и математическая кибернетика

Диссертационная работа С. А. Новоселова относится к важным разделам теории алгебраических кривых, в частности, к гиперэллиптическим кривым над конечными полями. Актуальность темы исследования обусловлена необходимостью разработки быстрых алгоритмов вычисления значения порядка якобиана кривой и дальнейшего использования таких кривых в криптографических приложениях, а также в теории кодирования. В настоящий момент, получение явных формул для эффективного вычисления числа точек якобиана – достаточно актуальная задача. На сегодняшний день существуют некоторые вариации алгоритмов типа Схоофа, которые являются, своего рода, симбиозом полиномиального и экспоненциального подходов, например, модификации Годри, Абеляра, Коэля, Рупрая, в связи с чем вопрос оптимизации этих модификаций также является весьма актуальным. Представленные в работе классы гиперэллиптических кривых позволяют получить явные формулы для числа точек, а методы их описывающие быстрее существующих на сегодняшний день.

В диссертационной работе исследуются гиперэллиптические кривые с геометрически разложимыми якобианами с целью получения явных формул для их характеристических многочленов и, как следствие, быстрых алгоритмов подсчета точек.

Представленная к защите диссертационная работа состоит из введения, четырех глав, заключения, списка литературы из 158 наименований и приложений.

Первая глава диссертации носит обзорный характер и посвящена вопросам исследования разложения якобианов кривых. Представлены общие понятия и теоремы теории абелевых многообразий, описаны методы разложения якобианов гиперэллиптических кривых (разложение из накрытий, метод Кани-Роузена), а также представлены методы вычисления точек на абелевых многообразиях.

Вторая глава посвящена новым теоретическим результатам, а именно,

- обобщен метод Сато восстановления характеристического многочлена эндоморфизма Фробениуса на случай произвольного абелева многообразия, представлены соответствующие оценки сложности нахождения характеристических многочленов, в частных случаях относительно степени расширения конечного поля доказано, что характеристический многочлен может быть восстановлен за полиномиальное время от степени расширения поля;
- подробно исследован вопрос разложения якобианов геометрически приводимых абелевых многообразий и представлены сопутствующие эвристические вероятностные временные оценки, уменьшение оценки сложности задачи сводится к рассмотрению многообразий меньших размерностей, заданных над расширением конечного поля;
- исследован специальный класс гиперэллиптических кривых с геометрически разложимым якобианом, разложение на якобианы меньших размерностей получено с точностью до степени расширения поля, представлены методы восстановления характеристического многочлена для таких кривых с помощью спуска по относительным расширениям конечных полей, а также на базе оператора Картье с использованием многочленов Лежандра.
- представлено полное описание характеристических многочленов относительно заданной характеристики поля для родов $g \leq 7$ с использованием матриц Картье-Манина и многочленов Лежандра.

Третья глава содержит специализации алгоритмов и методов, представленных во второй главе, к случаю специального вида кривых родов 3 и 4, выведены оценки сложности

вычисления числа точек для таких кривых, которые существенно ниже, нежели существующие оценки для достаточно больших классов гиперэллиптических кривых.

Четвертая глава посвящена применению полученных результатов в криптографических приложениях, а именно, для генерации кривых с заданными свойствами и генерации кривых с большой подгруппой простого порядка в ее якобиане, а также для анализа криптосистем на группах с неизвестным порядком.

Все основные результаты диссертации являются новыми и получены С.А. Новоселовым самостоятельно. Представленные результаты составляют значимое и завершенное исследование, позволяющее при этом находить приложения в криптографии и теории кодирования. Утверждения снабжены корректными доказательствами и своевременно опубликованы в ведущих научных журналах, включая три публикации в ведущих журналах из списка, рекомендованного ВАК РФ. Работа апробирована в ряде докладов на российских и международных конференциях и семинарах.

Отдельно хотелось бы отметить высокий научный уровень работы. Выполняя работу, Семен Александрович продемонстрировал глубокие знания в области алгебраических кривых и их криптографических приложений, а также высокую степень самостоятельности и инициативности.

На основании вышеизложенного считаю, что диссертационная работа «Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом» удовлетворяет всем требованиям, предъявляемым к кандидатской диссертации «Положением о порядке присуждения ученых степеней» ВАК РФ, а ее автор Новоселов Семен Александрович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Научный руководитель _____ Е.С. Малыгина

кандидат физико-математических наук,
доцент, м.н.с. лаборатории “Математические методы защиты и обработки информации”
Малыгина Екатерина Сергеевна,
236041, г. Калининград, ул. А. Невского, 14,
корпус №2, каб. 211,
тел. +79622546654
e-mail: EMalygina@kantiana.ru,
ФГАОУ ВПО «Балтийский федеральный университет имени Иммануила Канта»,

19.12.2021 г.