ОТЗЫВ

официального оппонента на диссертацию Новоселова Семена Александровича
«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»

Диссертационная работа С.А. Новоселова посвящена гиперэллиптическим кривым, широко применяющимся в современной криптографии. В частности, важной задачей является подсчёт числа точек на этих кривых, причём в разных аспектах: иногда (для генерации нужных кривых) полезно уметь быстро решать эту задачу, в других случаях (например, когда стойкость криптосистемы основана на том, что порядок группы неизвестен) желательно, чтобы сложность задачи подсчёта была высока. В исследовании использована сложная и глубокая теория алгебраических кривых и функциональных полей, которой автор работы владеет в совершенстве. Для общей оценки вклада рассматриваемой работы в проблему показательна таблица 2 в конце главы 1, где представлены оценки сложности задачи подсчёта числа точек на абелевых многообразиях и гиперэллиптических кривых различных классов: 6 из 15 строк этой таблицы — новые результаты, полученные в диссертации.

Перечислим основные результаты работы.

1) Получена общая оценка сложности подсчёта числа точек на абелевом многообразии над конечным полем с помощью нахождения характеристического многочлена эндоморфизма Фробениуса (Предложение 2).

2) Предложен алгоритм (Алгоритм 1) и приведена эвристическая вероятностная оценка времени его работы (Теорема 2.1.7) восстановления характеристического многочлена эндоморфизма Фробениуса абелева многообразия над базовым полем $\mathrm{GF}(q)$ из характеристического многочлена над расширением поля $\mathrm{GF}(q^k)$.

3) Та же задача рассмотрена для случаев $g = 3$, $k = 2^r3^s$ и $g = 4$, $k = 2^r$, получены в явном виде решения систем уравнений для расширений степени 2 и 3, в результате оценка п. 2 уточнена для произвольного абелева многообразия (Теоремы 2.1.8, 2.1.9) и для случая гиперэллиптической кривой (Следствия 2.1.8.1, 2.1.9.1).

4) Для геометрически разложимых абелевых многообразий размерности 3 и 4 оценки сложности задачи подсчёта числа точек в случаях $g = 3$, $k = 2^r3^s$ и $g = 4$, $k = 2^r$ улучшены (Теоремы 2.2.1 и 2.2.2).

5) Предложен алгоритм (Алгоритм 2) подсчёта числа точек гиперэллиптической кривой $C\colon y^2 = x^{2g+1} + ax^{g+1} + bx$ и в её якобиане, приведена оценка времени его работы (Теорема 2.3.4).

6) Исследованы свойства матриц Картье — Манина кривых C (Теоремы 2.3.7 — 2.3.13), в результате получены полные списки характеристических многочленов этих кривых по модулю характеристики поля для $g = 1, \ldots, 7$ (Приложения А, Б).

7) Детализированы алгоритмы подсчёта числа точек и уточнены оценки их сложности для некоторых специальных случаев: для кривых рода 3 вида $C\colon y^2 = x^7 + ax^4 + bx$ (Алгоритм 3; Предложение 5; Теоремы 3.2.1 и 3.2.1; в Следствии 3.2.2.1 получена оценка $O(\log^4 q)$) и для кривых рода 4 вида $C\colon y^2 = x^9 + ax^5 + bx$ (Алгоритм 4; Теорема 3.3.1 даёт оценку сложности $O(\log^8 q)$).

8) Приведены алгоритмы генерации гиперэллиптических кривых с заданным числом точек в якобиане (Алгоритм 5) и с большим простым делителем количества точек (Алгоритм 6), даны оценки сложности этих алгоритмов.

9) Установлено, что кривые рода 3 и 4 вида $C: y^2 = x^{2g+1} + ax^{g+1} + bx$ не следует использовать в криптосистемах, стойкость которых базируется на неизвестности порядка группы.

Все представленные результаты являются новыми.

Достоверность и обоснованность результатов диссертации С.А. Новоселова подтверждены строгими математическими доказательствами. Полученные результаты могут быть использованы для генерации гиперэллиптических кривых с требуемыми свойствами (с заданным или имеющим большой простой делитель числом точек) и для оценки безопасности криптосистем, построенных на группах с неизвестным порядком.

Диссертация состоит из введения, четырёх глав, заключения, списка литературы и четырёх приложений. Список литературы включает 158 наименований. Объём диссертации — 155 с. Глава 1 содержит подробный обзор известных результатов, использующихся в исследованиях и доказательствах.

Все результаты диссертации с достаточной полнотой опубликованы в 7 работах (3 из которых — в журналах, рекомендованных ВАК, и 3 — в изданиях, индексируемых БД WoS и Scopus), апробированы на научных конференциях и семинарах международного и всероссийского уровней.

Автореферат полностью соответствует содержанию диссертации.

Замечания:

1. С. 41, 9-я строка сверху: «Если выбрать l = ...». Должно быть «Если выбрать l > ...».

2. С. 64, в формулировке теоремы 2.3.2 опечатка: «степени степени m».

3. С. 124, второй абзац: «Для кривых рода 4 вида $y^2 = x^7 + ax^4 + bx$ ...». Должно быть «Для кривых рода 4 вида $y^2 = x^9 + ax^5 + bx$ ...».

4. По оформлению: имеется небольшое количество грамматических ошибок (например, «в отличи**и**») и несколько больше — пунктуационных (наличие лишних запятых и отсутствие нужных).

Указанные замечания не снижают общую высокую оценку работы.

Диссертация С.А. Новоселова соответствует специальности 01.01.09 — «Дискретная математика и математическая кибернетика», имеет внутреннее единство и является завершённой научно-квалификационной работой, в которой содержатся эффективные алгоритмы подсчёта числа точек гиперэллиптических кривых и явные формулы характеристических многочленов этих кривых.

Диссертация соответствует требованиям п. 9 «Положения о порядке присуждения учёных степеней» постановления Правительства Российской Федерации от 24.09.2013 г. № 842 (в редакции постановлений Правительства Российской Федерации от 30.07.2014 г. № 723; от 21.04.2016 г. № 335; от 02.08.2016 г. № 748; от 01.10.2018 г. № 1168; с изм. от 26.05.2020), а её автор Новоселов Семен Александрович достоин присуждения учёной степени кандидата физико-математических наук по специальности 01.01.09 – «Дискретная математика и математическая кибернетика».

Официальный оппонент:
к.ф.-м.н., доцент _____ / И.А. Панкратова

Панкратова Ирина Анатольевна
зав. лабораторией компьютерной криптографии
федерального государственного автономного
образовательного учреждения высшего образования
«Национальный исследовательский Томский государственный университет»,
кандидат физико-математических наук, доцент

634050, г. Томск, пр. Ленина, 36.
Тел. +7 (3822)-529-852
E-mail: rector@tsu.ru

22 марта 2022 года