ОТЗЫВ

официального оппонента д. ф.-м. н. А. В. Устинова о диссертации Черепнева Михаила Алексеевича «О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования», представленной на соискание ученой степени доктора физико-математических наук по специальности 01.01.09 — дискретная математика и математическая кибернетика.

Основное направление проведённых исследований — алгоритмические аспекты криптографии. Вместе с тем диссертация также содержит результаты, имеющие самостоятельную ценность в теории чисел и линейной алгебре.

Диссертация состоит из пяти частей. Результаты диссертации излагаются в части III, разбитой на семь глав. Нумерация теорем взята из части II.

Первая глава посвящена задаче дискретного логарифмирования. В теореме 1 доказаны формулы, которые с помощью частных Ферма позволяют поднимать решение сравнения $a \equiv g^x \pmod{p}$, где p — простое, до решения сравнения $a \equiv g^x \pmod{p^\alpha}$. При этом g (основание дискретного логарифма) может не быть первообразным корнем по модулю p. Это важно для криптографических приложений, поскольку в ряде протоколов в качестве основания g выбирается случайный элемент приведённой системы вычетов по модулю p. В теореме 2 для решения задачи дискретного логарифмирования впервые построен полиномиальный алгоритм, использующий оракул, решающий задачу Диффи — Хеллмэна. Тем самым подтверждена стойкость протокола Диффи — Хэллмэна, имеющего ключевое значение в асимметричной криптографии.

Вторая глава содержит новые результаты о распределении простых делителей чисел вида $p-1$, где p — простое. В теоремах 4 и 5 доказываются асимптотические формулы, описывающие типичное поведение величины и количества таких делителей. В качестве приложения этих формул в теореме 6 получен новый результат о типичном поведении функции Эйлера. Для почти всех натуральных n известная оценка Ландау $\varphi(n) > \frac{cn}{\ln\ln n}$ улучшена до $\varphi(n) > \frac{cn}{\ln\ln\ln n}$.

Третья глава посвящена исследованию стойкости протокола распределения ключей, построенного с помощью некоммутативной групповой операции (протокола Сидельникова). Стойкость этого протокола зависит от свойств рассматриваемой группы. В теореме 7 доказана нестойкость этого протокола для некоторых естественных групп. Затем предложены примеры групп, для которых протокол Сидельникова, вероятно, будет обладать более высокой стойкостью.

Четвёртая глава диссертации основана на простом, но очень красивом наблюдении автора, которое заключается в том, что схемы шифрования и электронной подписи Эль–Гамаля допускают универсальную подделку, если существует алгоритм, находящий для данных C и R решение сравнения $x \equiv CR^x \pmod{p}, x \in \{1, 2, \ldots, p-2\}$. (В классическом анализе решением аналогичного уравнения $z = W(z)e^{W(z)}$ является W–функция Ламберта, обладающая многими замечательными свойствами.) Пару (R, x) можно построить по любому первообразному корню g, удовлетворяющему условию Бризолиса $(g, p-1) = 1$. Теоремы 8

и 9 содержат новые сведения о парах (R, x), удовлетворяющих сравнению $x \equiv R^x \pmod{p}$. В теореме 10 получены новые нижние оценки числа первообразных корней, удовлетворяющих условию Бризолиса. Для числа таких корней была известна асимптотическая формула, доказанная Кобели и Захареску методом тригонометрических сумм (1999), однако результат теоремы 10, полученный элементарными методами, в ряде случаев оказывается более точным либо асимптотически, либо для «малых» простых (запись которых не превосходит нескольких сотен десятичных знаков).

Пятая глава посвящена задаче дискретного логарифмирования на эллиптических кривых. Главное внимание здесь уделяется возможности решения этой задачи с помощью спуска Вейля. Теорема 12 доказывает, что для эллиптических кривых над полем характеристики 2 спуск Вейля действительно может быть эффективен. Этот аргумент показывает, что для увеличения стойкости протоколов предпочтительнее использовать эллиптические кривые над полем большой характеристики. Кроме того, в пятой главе, как часть исходной задачи дискретного логарифмирования, построен новый алгоритм приведения матрицы к смитовой нормальной форме с одновременным вычислением матрицы приведения. Этот алгоритм оказывается эффективней других известных алгоритмов, решающих ту же задачу.

Шестая глава диссертации посвящена такой важной для приложений задаче, как решение больших разреженных систем линейных уравнений над полем из двух элементов. М. А. Черепнёв предложил здесь новый алгоритм, который по сравнению с используемыми в настоящее время алгоритмами Монтгомери и Видемана — Копперсмита имеет важное преимущество: он допускает высокую степень распараллеливания и не требует привлечения суперкомпьютера ни на одном из своих шагов (для его работы достаточно, чтобы память вычислителей могла хранить исходную матрицу задачи). При построении алгоритма автором был предложен очень оригинальный подход. Для вычислений используются аппроксимации Паде — инструмент, который обычно используется в других областях (теории интерполяции и теории диофантовых приближений). В седьмой главе разработанный подход перенесён на решение систем линейных уравнений над большим простым полем. Это существенно ускорило алгоритмы факторизации и дискретного логарифмирования, имеющие в криптографии исключительно важное значение. В качестве замечания следует отметить, что было бы интересно более точно оценить параллельный ресурс предложенного алгоритма. Для этого достаточно протестировать его на более мощной вычислительной технике и на большем числе разреженных систем линейных уравнений различного размера.

В целом в диссертации получены принципиально новые результаты в ряде задач, которые важны как для криптографии, так и для теории чисел. В доказательствах использован широкий спектр методов: методы линейной алгебры, алгебраической геометрии, элементарной и алгоритмической теории чисел, математического анализа и теории диофантовых приближений. Автореферат полностью отражает содержание диссертации.

Достоверность полученных результатов подтверждена необходимыми доказательствами. Построенные алгоритмы реализованы в компьютерных программах и проанализированы экспериментально. Результаты являются новыми, что под-

тверждается авторскими публикациями в рецензируемых научных журналах и монографиях, а также патентом, актами внедрения и свидетельствами о государственной регистрации прав на ПО.

В диссертации М. А. Черепнёва разработаны теоретические положения, совокупность которых можно квалифицировать как новое крупное достижение в развитии теории чисел и криптографии. Диссертация соответствует критериям, установленным Положением о присуждении ученых степеней.

Автор диссертации, Черепнев Михаил Алексеевич, несомненно заслуживает присуждения ученой степени доктора физико-математических наук по специальности 01.01.09 — дискретная математика и математическая кибернетика.

Ведущий научный сотрудник управления научно-исследовательских работ ТОГУ, заведующий лабораторией «Теория чисел и криптография», профессор кафедры высшей математики, д. ф.-м. н. Устинов А. В.

10 апреля 2017 года.

Подпись А. В. Устинова удостоверяю

Проректор по учебной работе ТОГУ
Н.Ю. Сорокин, 10.04.17