ОТЗЫВ

официального оппонента на диссертацию Черепнева Михаила Алексеевича «О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования», представленную на соискание ученой степени доктора физико-математических наук по специальности 01.01.09 – «Дискретная математика и математическая кибернетика».

Диссертация М.А. Черепнева посвящена решению ряда актуальных вопросов дискретной математики, относящихся к области алгоритмических и теоретико-числовых проблем синтеза и анализа асимметричных криптографических систем. Актуальность исследованных проблем определяется их содержательной связью с анализом современных стандартов электронной подписи и в целом с оценкой уровня защиты информации, обеспечиваемого современными системами удостоверения авторства.

Диссертационная работа состоит из семи глав. В первой главе доказана полиномиальная эквивалентность задачи дискретного логарифмирования и определенного класса задач Диффи-Хеллмана. Получена формула, позволяющая с использованием характеристик дерева Пратта соотнести вычислительные сложности этих задач. Предложены некоторые подходы к решению задачи дискретного логарифмирования в группе простого порядка p на стандартных эллиптических кривых в случае разложения числа p-1 на большое количество небольших взаимно простых множителей. Построены соответствующие алгоритмы дискретного логарифмирования. На основе анализа разложения числа p-1 и вычислительной сложности построенных алгоритмов автором предложены способы усиления свойств российского стандарта электронной подписи ГОСТ Р 34.10-2012.

Вторая глава посвящена получению оценок величины и количества простых делителей частного класса (связанного с деревьями Пратта) чисел вида p-1, характеризующих дерево Пратта, где p – простое число. Указанные величины характеризуют вычислительную сложность атак на стандарт электронной подписи ГОСТ Р 34.10-2012 и на его предыдущую версию ГОСТ Р 34.10-1994.

В третьей главе исследована эффективность схемы открытого распределения ключей В.М. Сидельникова, построенной на основе некоторых классов некоммутативных операций, используемых в ряде алгоритмов, применяемых в системах защиты информации. Стойкость данной схемы определяется вычислительной сложностью решения задачи факторизации относительно рассматриваемых операций. Автором построены

полиномиальные алгоритмы решения задачи факторизации для рассмотренных операций, а также предложена другая оригинальная некоммутативная операция, повышающая вычислительную сложность решения задачи факторизации для данной схемы открытого распределения ключей.

Четвертая глава посвящена решению одного класса экспоненциальных сравнений по простому модулю p. Решения сравнения (так называемые неподвижные точки в задаче дискретного логарифмирования) позволяют подделать подпись, в частности, при использовании прежней версии стандарта электронной подписи ГОСТ Р 34.10-1994. Получены новые формулы и оценки числа решений этих сравнений и алгоритмы определения самих решений с помощью вероятностного полиномиального алгоритма. В некоторых случаях получены точные формулы для решений сравнения.

В пятой главе исследована задача дискретного логарифмирования в группе точек эллиптической кривой. С использованием представления Мамфорда дивизоров гиперэллиптических кривых автор установил важные свойства ядра гомоморфизма Вейля, соответствующего рассмотрению полей характеристики 2. Доказанная теорема позволяет выявить случай, при котором ядро гомоморфизма (спуска Вейля) является нетривиальным, а также обладает некоторыми другими важными свойствами, позволяющими понизить вычислительную сложность решения задачи дискретного логарифмирования на гиперэллиптических кривых над полем характеристики 2.

Шестая и седьмая главы посвящены разработке новых блочных алгоритмов решения больших разреженных систем линейных уравнений, имеющих большое значение для решения задачи дискретного логарифмирования в мультипликативной группе конечного поля. В шестой главе предложены алгоритмы, сочетающие преимущества алгоритма Монтгомери и алгоритма Видемана-Копперсмита. Положительные свойства построенного диссертантом алгоритма не требуют обязательного использования большого вычислительного кластера для решения разреженных систем линейных уравнений и позволяют решать задачу с использованием более широкого класса вычислительных средств. Действенность разработанного класса алгоритмов показана в работе при помощи практической реализации на современной многопроцессорной технике, что подтверждено актом внедрения.

В главе 7 техника решения больших разреженных систем линейных уравнений распространена на случаи больших конечных простых полей.

Полученные результаты позволяют оценить разработанный класс алгоритмов решения больших разреженных систем линейных уравнений как наилучший по основным показателям из известных к настоящему времени алгоритмов. Результаты создают реальные предпосылки для корректировки требований к ряду систем защиты информации.

В целом результаты диссертации следует расценить как заметный прогресс в алгоритмическом решении задач факторизации целых чисел и дискретного логарифмирования, подтвержденный с помощью реализации соответствующего программного обеспечения на современной многопроцессорной технике.

Работа написана на хорошем математическом уровне, все утверждения в диссертации доказаны или на них имеются ссылки. Научные положения, выводы и рекомендации диссертационной работы обоснованы. Основные результаты диссертации, вынесенные автором на защиту, являются новыми. Их достоверность подтверждается как приведенными в публикациях математическими доказательствами, так и выполненной автором апробацией результатов с помощью докладов на соответствующих данной тематике математических конференциях и семинарах, а также внедрения в виде действующего программного обеспечения.

Представленные в диссертации исследования соответствуют Паспорту специальности 01.01.09 – дискретная математика и математическая кибернетика. Автореферат соответствует диссертации и достаточно полно отражает ее содержание.

Вместе с тем, по выполненной работе имеются замечания, связанные с отсутствием количественных оценок, которые было бы целесообразно отнести к некоторым утверждениям и выводам работы.

1. Утверждение главы 1 о «слабости действующего стандарта эллиптических кривых» не сопровождено количественными оценками (вычислительная сложность, вероятность и др.), что порождает неопределенность в оценке уровня защиты, обеспечиваемого данным стандартом.

2. Вывод главы 3 о преимуществе использования предложенной автором новой некоммутативной операции не подкреплен оценкой, показывающей усиление стойкости схемы открытого распределения ключей.

3. Утверждение 4-й главы о возможном анализе методов подделки подписи для стандартов ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 по аналогии с анализом ГОСТ Р 34.10-1994 не подкреплен оценкой результатов или сложности такого анализа.

4. Не оценена величина снижения сложности задачи дискретного логарифмирования в группе точек эллиптической кривой в связи с использованием свойств гомоморфизма Вейля.

5. Не оценена величина возможного снижения сложности задач дискретной факторизации и дискретного логарифмирования с помощью методов решения систем линейных уравнений, сочетающих преимущества алгоритмов Монтгомери и Видемана-Копперсмита.

В заключение следует отметить, что данные замечания не снижают существенно положительного впечатления от диссертационной работы.

Вывод: автором получены новые значимые результаты в области вычислительной сложности алгоритмов факторизации и дискретного логарифмирования. Диссертационная работа Черепнева Михаила Алексеевича «О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования» соответствует требованиям, предъявляемым к докторским диссертациям Положением о присуждении ученых степеней, утвержденным постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а ее автор, Черепнев Михаил Алексеевич, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 01.01.09 – «Дискретная математика и математическая кибернетика».

Официальный оппонент:
профессор кафедры «Информационная безопасность»
федерального государственного образовательного
бюджетного учреждения высшего образования
«Финансовый университет при
Правительстве Российской Федерации»,
доктор физико-математических наук, профессор

Владимир Михайлович Фомичев

18 апреля 2017 года

125468, г. Москва, Ленинградский проспект, 49.

Подпись В.М. Фомичева

ЗАВЕРЯЮ
Ученый секретарь Ученого совета
Финансового университета
Д.А. Смирнов
18 апреля 2017 г.