

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.073.05 НА
БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ИНФОРМАТИКА И УПРАВЛЕНИЕ» РОССИЙСКОЙ АКАДЕМИИ
НАУК» ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЁНОЙ СТЕПЕНИ
ДОКТОРА НАУК

Аттестационное дело №

Решение диссертационного совета от 18 мая 2017 года, протокол № 8.

О присуждении ЧЕРЕПНЕВУ Михаилу Алексеевичу, гражданину РФ, учёной степени доктора физико-математических наук.

Диссертация «О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования» по специальности 01.01.09 - дискретная математика и математическая кибернетика принята к защите 16 февраля 2017 г., протокол № 3, диссертационным советом Д 002.073.05 на базе Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Москва, ул. Вавилова, 40, созданным приказом Минобрнауки РФ 783/НК от 26.06.2016 года. Была произведена замена официального оппонента 16 марта 2017 года, протокол № 5.

Соискатель ЧЕРЕПНЕВ Михаил Алексеевич, 1965 года рождения.

Диссертацию на соискание ученой степени кандидата физико-математических наук "Об алгебраической независимости значений некоторых гипергеометрических E-функций по специальности 01.01.06 - математическая логика, алгебра и теория чисел защитил в 1992 году в диссертационном совете Д 053.05.05 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет имени М.В. Ломоносова».

Работает на кафедре информационной безопасности факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова».

Диссертация выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова».

Научный консультант - академик РАН Соколов Игорь Анатольевич, директор Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН).

Официальные оппоненты:

- Устинов Алексей Владимирович д.ф.-м.н., в.н.с. управления научно-исследовательских работ (заведующий учебно-научной лабораторией «Теория чисел и криптография») Федерального государственного бюджетного образовательного учреждения высшего образования «Тихоокеанский государственный университет», профессор кафедры высшей математики,

- Фролов Александр Борисович д.т.н., профессор кафедры математического моделирования Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ»,

- Фомичев Владимир Михайлович д.ф.-м.н., профессор кафедры информационной безопасности Федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации»,

дали положительные отзывы.

Ведущая организация - Федеральное государственное бюджетное учреждение науки Институт вычислительной математики Российской академии наук имени Г.И.Марчука в своём положительном заключении, подписанном директором института, академиком Российской академии наук Тыртышниковым Евгением Евгеньевичем, указала, что достоверность результатов диссертации М.А.ЧЕРЕПНЕВА подтверждается необходимыми математическими доказательствами, компьютерными экспериментами и актами внедрения, результаты являются новыми, что подтверждается авторскими публикациями в рецензируемых научных изданиях. В заключении ведущей организации отмечается, что диссертация является исследованием, в котором разработаны теоретические положения, совокупность которых можно квалифицировать как крупный вклад в криптографию, и полностью удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» ВАК, предъявляемым к диссертации на соискание ученой степени доктора физико-математических наук, а её автор заслуживает присуждения степени доктора физико-математических наук по специальности 01.01.09 - дискретная математика и математическая кибернетика.

Соискатель имеет более 50 опубликованных работ, в том числе - более 30 по теме диссертации из которых 19 - в рецензируемых научных изданиях из Перечня, рекомендованного ВАК Минобрнауки РФ для публикации основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук (в том числе 1 патент и 2 свидетельства о государственной регистрации прав на ПО). Автором получены два акта внедрения, а также написаны две книги. Результаты, изложенные в диссертации, получены автором самостоятельно. В коллективных публикациях автору принадлежат те их части, на которые автор указывает в тексте диссертации.

Наиболее значимые публикации по теме диссертации:

1. Сидельников В.М., Черепнёв М.А., Яценко В.В. Системы открытого распределения ключей на основе некоммутативных полугрупп.// ДАН СССР-1993.- т.332-№5-с.566-567.
2. Черепнёв М.А. О связи сложностей задач дискретного логарифмирования и Диффи-Хеллмана.// Дискретная математика.-1996.-т.8-вып.3-с.22-30.
3. Черепнёв М.А. Некоторые свойства больших простых делителей чисел вида $p-1$.// Математические заметки-2006.-80:6- р.920-925.
4. Черепнев М.А. Блочный алгоритм типа Ланцоша решения разреженных систем линейных уравнений.// Дискретная Математика-2008.-т.20-вып.1-с.145-150.
5. Черепнев М.А. Вариант блочного алгоритма типа Ланцоша решения систем линейных уравнений.// Материалы Третьей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ 25-27.10.2007 (МаБИТ-2007)-М.:МЦНМО,2008.-с.129-136.
6. Черепнев М.А. Некоторые эффективные оценки для числа решений задачи Бризолиса.// Современные проблемы математики и механики. Математика.-2009.- т.IV-вып.3-с.125-129.
7. Черепнев М.А. О некоторых вычислениях в пространствах Крылова над $GF(2)$.// Вестник Тамбовского университета Сер. Естественные и технические

науки.-2009.-т.14-вып.4-с.833-835.

8. Cherepnirov M.A. Some estimations of performance of parallel algorithms for solving large linear systems over $GF(2)$.// Journal of Tambov State University, The works of participants of International conference "ParCA" presented according to the results of reviewing by International Program Committee.-2010.-v.15-Iss.4-p.1342-1353.

9. Cherepnirov M.A. Version of block Lanczos-type algorithm for solving sparse linear systems.// Bull.Math.Soc.Sci.Math.Roumanie.-2010.-v.53(101)-no.3-p.225-230. (<http://rms.unibuc.ro/bulletin>)

10. Черепнев М.А. A connection of series approximations and the basis of the Krylov space in block algorithms of Coppersmith and Montgomery.// Journal of Mathematical Sciences -Volume 193, -Issue 4 (2013), -p.622-630.

11. Черепнёв М.А. Замечание о ядре группового гомоморфизма метода спуска Вейля.// Journal of Mathematical Sciences, Vol. 221, No. 3, March, 2017 p. 452-460.

12. Черепнев М.А. Модулярный алгоритм приведения матриц к Смитовой нормальной форме.// Дискретная математика Т.28, вып.2, 2016 с.160-164.

13. Черепнев М.А., Замарашкин Н.Л. Универсальный блочный метод Ланцоша-Паде для систем линейных уравнений над большими простыми полями.// Journal of Mathematical Sciences, Vol. 221, No. 3, March, 2017 p. 461-478.

14. Черепнёв М.А. Криптографические протоколы.-М.: Изд-во центра прикладных исследований при механико-математическом факультете.-2006.-70с.

Получено заключение об использовании результатов диссертации М.А.ЧЕРЕПНЕВА в учебном процессе на механико-математическом факультете и факультете ВМК Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В.Ломоносова», подписанное и.о. декана механико-математического факультета, профессором Чубариковым В.Н. и деканом факультета ВМК, академиком Моисеевым Е.И.

Выбор официальных оппонентов обосновывается тем, что оппоненты являются известными российскими учеными в области криптографии и теории чисел, что подтверждается соответствующими публикациями в авторитетных рецензируемых научных изданиях. Выбор в качестве ведущей организации Федерального государственного бюджетного учреждения науки Институт вычислительной математики Российской академии наук имени Г.И.Марчука обоснован тем, что данная организация является одной из лидирующих в России по созданию прикладных программ, а её сотрудники внесли существенный вклад в развитие теории алгоритмов и практическое программирование для решения насущных проблем народного хозяйства. (что подтверждено соответствующими публикациями, комплексами программ и др.)

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- построен полиномиальный алгоритм решения задачи дискретного логарифмирования с оракулом, решающим задачу Диффи-Хеллмэна. Данный алгоритм позволил получить следующую оценку сверху сложности решения задачи дискретного логарифмирования через сложность решения задачи Диффи-Хеллмэна, относительно элементов той же группы, связанных некоторыми специальными групповыми операциями.

- в ряде частных случаев (когда $p - 1$ раскладывается на «маленькие» простые множители, или когда высота дерева Пратта для растущего простого порядка p рассматриваемой группы ограничена) доказано, что сложность решения

задачи дискретного логарифмирования и сложность решения задачи вскрытия протокола Диффи-Хеллмана полиномиально эквивалентны. Такой случай возможен для групп точек на эллиптических кривых, удовлетворяющих ГОСТ Р 34.10-2012 (действующий государственный стандарт РФ на цифровую подпись).

- получены новые оценки на величину и число простых делителей чисел $p-1$, где p - простое.

- показано, что задача универсальной подделки ГОСТ Р 34.10-1994 (государственный стандарт РФ на цифровую подпись, действующий до 2005г.) сводится к нахождению неподвижных точек в задаче дискретного логарифмирования. Для решения последней задачи получены новые аналитические формулы и оценки на число решений.

- доказана невырожденность ядра преобразования спуска Вейля при решении задачи дискретного логарифмирования на эллиптических кривых над полем характеристики 2 для одного частного случая.

- разработан новый блочный алгоритм решения больших разреженных систем линейных уравнений над произвольным конечным полем, который в случае использования большого числа вычислителей эффективнее алгоритма Видемана-Копперсмита, в частности не требует растущего объема оперативной памяти по сравнению с размерами задачи. Новый алгоритм по числу операций не сложнее алгоритма Монтгомери, однако в отличие от него он имеет параллельную схему и может быть реализован на вычислителях, связанных медленной сеткой (Интернет). Применение этого алгоритма упрощает самый сложный, линейный, этап в решении задач факторизации и дискретного логарифмирования. В частности даёт возможность вообще отказаться от использования кластера в пользу большого числа небольших вычислителей, связанных медленной коммутационной сетью.

Тем самым получены теоретические обоснования необходимости выбора новых параметров безопасности используемых в настоящее время систем защиты информации на основе задач дискретного логарифмирования, целой факторизации и Диффи-Хеллмана.

Теоретическая значимость исследования обоснована тем, что доказанные теоремы о новых свойствах простых чисел, эллиптических кривых и приближений Паде позволяют в ряде случаев понизить сложность задач, лежащих в основе стойкости современных систем защиты информации.

Значение полученных соискателем результатов для практики подтверждается двумя актами внедрения, патентом и двумя свидетельствами о государственной регистрации прав на ПО.

Оценка достоверности результатов исследования выявила, что доказанные соискателем теоремы основаны на строгих рассуждениях и согласуются с известными результатами в данной области. Вычислительные эксперименты поставлены на кластере Межведомственного суперкомпьютерного центра РФ многопроцессорной вычислительной системы МВС-1000.

Личный вклад соискателя состоит в том, что им самостоятельно сформулированы новые понятия, предложены методы и доказаны утверждения, составляющие теоретическую основу диссертационной работы, а также подготовлены основные публикации по выполненной работе. Также автор участвовал в большом количестве научно-исследовательских работ, что подтверждается опубликованными отчётами, актами внедрения, патентом и другими документами.

На заседании 18 мая 2017 года диссертационный совет принял решение присудить ЧЕРЕПНЕВУ М.А. ученую степень доктора физико-математических наук. При

проведении тайного голосования диссертационный совет в количестве 28 человек, из них 7 докторов наук по специальности 01.01.09 - дискретная математика и математическая кибернетика, участвовавших в заседании, из 35 человек, входящих в состав совета (дополнительно введены на разовую защиту 0 человек), проголосовали «за» - 28 человек, «против» - 0 , недействительных бюллетеней - 0 .

Председатель диссертационного совета,
академик РАН, д.ф.-м.н., профессор



 Журавлев Ю.И.

Ученый секретарь диссертационного совета,
д.ф.-м.н., профессор

Рязанов В.В.

18 мая 2017 года