«Утверждаю»
Директор ИВМ РАН

академик РАН Е. Е. Тыртышников
28.04.2017

ОТЗЫВ

на диссертационную работу 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

Целью диссертационной работы М. А. Черепнева является:

- оптимизация под современные программно-аппаратные средства теоретико-числовых алгоритмов факторизации, дискретного логарифмирования и решения больших разреженных линейных систем над конечными полями;
- получение теоретических оценок вычислительной сложности алгоритмов для задач дискретного логарифмирования, факторизации и решения линейных систем над конечными полями;
- изучение зависимости вычислительной сложности алгоритмов от способа задания исходных данных.

Актуальность темы.
Развитие теоретико-числовых конструкций и алгоритмов существенно влияет на современные способы безопасного хранения и передачи данных, а современные вычислительные средства позволяют применять эти конструкции и алгоритмы к задачам все большей вычислительной сложности. В диссертационной работе М.А. Черепнева рассматриваются новые подходы к построению и анализу алгоритмов, а также их эффективному отображению на современные вычислительные системы для задач дискретного логарифмирования, факторизации и решения больших разреженных систем линейных уравнений над конечными полями. Актуальность темы исследования определяется тем фактом, что вычислительная (алгоритмическая) сложность рассматриваемых методов напрямую связана с вопросами стойкости известных систем шифрования. Среди исследований автора особенно отметим те, которые связаны с так называемым линейным этапом в проблеме факторизации и задаче дискретного логарифмирования. Получение новых алгоритмов линейного этапа, допускающих значительное ускорение с помощью распределенных вычислительний, – важная и актуальная задача. Значительную ценность имеют такие алгоритмы, время выполнения которых не зависит или слабо зависит от архитектуры вычислительной системы, а только от её общей производительности. Как правило, в таких алгоритмах обмен данными является минимальным.

Таким образом, исследование применимости современных математических методов к задачам дискретного логарифмирования, факторизации и решения линейных систем над конечными полями имеют – помимо теоретического – важное практическое значение.

Основные результаты работы.

Работа состоит из пяти частей: введения, положений, выносимых на защиту, основного содержания диссертации, заключения и приложения. Основное содержание диссертации представлено в семи разделах.

Во введении делается краткий обзор содержания диссертации. В положениях, выносимых на защиту, основные результаты, представленные в диссертации, увязываются с историей вопроса и публикациями автора по теме диссертации.

Первый раздел основного содержания диссертации содержит результаты автора, относящиеся к редукции задачи дискретного логарифмирования (DL) к задаче Диффи-Хеллмана (DH). Теорема 1.1 содержит редукцию показательных сравнений в кольцах вычетов по модулю степени простого числа к случаю, когда эта степень 1. В дальнейшем не используется.

Редукция DL-задачи к DH-задаче с помощью функции высоты дерева Пратта, обозначаемой у автора символом s дает результаты, близкие к мировому уровню. Так, полиномиальная сложность DH-задачи совместно с гипотезой Коняева о высоте дерева Пратта влечет у автора «почти» полиномиальную сложность DL-задачи. Это соответствует, например, теореме D. Boneh, R. J. Lipton, в которой «почти» полиномиальная сложность DH-задачи для эллиптической кривой вместе с некоторой гипотезой о вероятности гладкости чисел, выбираемых из интервала длиной $\sqrt{p}$ влечет «почти» полиномиальную сложность DL-задачи для группы размера p.

Аналогичный результат для групп эллиптических кривых над конечными полями составляет содержание теоремы 1.5.

Идея использования функции $s(m)$ при получении оценки сложности задачи дискретного логарифмирования через задачу Диффи-Хеллмана приналежит автору. Предложенный подход применен к анализу стойкости Российского стандарта числовой подписи ГОСТ Р 34.10-2012 на эллиптических кривых. Показано, что для некоторых эллиптических кривых, удовлетворяющих стандарту, алгоритмы решения задач дискретного логарифмирования полиномиальны эквивалентны.

Во **втором разделе основного содержания диссертации** в связи с необходимостью оценки функции s высоты дерева Пратта получены теоремы, оценивающие количество больших делителей на каждом уровне этого дерева. Попутно в этом разделе получена оценка на функцию Эйлера $\varphi(n)$ числа n, улучшающая известную оценку Ландау.

В **разделе 3** исследуется стойкость протокола открытого распределения ключей на основе некоммутативной операции, предложенного В. М. Сидельниковым. Представлен анализ стойкости этого протокола. Построены алгоритмы сводящие задачу вскрытия этого протокола к системам линейных уравнений. Доказано, что протокол нестоек для некоторых естественных групп.

В **разделе 4** содержит анализ неподвижных точек в задаче дискретного логарифмирования. Показывается, что задача универсальной подделки подписей по схеме Эль – Гамаля сводится к задаче нахождения неподвижных точек в задаче дискретного ло-

гарифмирования (идея сведения принадлежит автору диссертации). Полученные аналитические формулы и оценки на число неподвижных точек позволили построить подельную подпись для схемы по ГОСТ Р.34.10 – 94.

В **разделе 5** изучается задача дискретного логарифмиоования в группе точек эллиптической кривой. Установлены свойства ядра гомоморфизма Вейля для полей характеристики 2. Полученные результаты позволяют описать случай, когда ядро гомоморфизма Вейля является нетривиальным, а задача дискретного логарифмирования обладает сниженной сложностью.

В **разделе 6 основного содержания диссертации** изучаются методы решения больших разреженных систем линейных уравнений над полем GF(2). Автором предложена конструкция нового блочного метода Ланцоша – Паде, использующего метод построения последовательностей матричных приближений Паде для матричного ряда, порождаемого симметризованной системой уравнений. Главным достоинством нового метода является его значительный *алгоритмический* параллельный ресурс (и гарантированно малое число обменов), допускающий эффективную реализацию метода на вычислительных системах с медленными и ненадежными коммуникационными соединениями между узлами. Для нового метода доказаны вероятностные оценки на его успешное завершение; построена модель параллельных вычислений на вычислительных системах с распределенной памятью; представлены оценки сложности рассмотренной модели параллельных вычислений; приведены результаты численных экспериментов с программами, реализующими аналогичные и/или близкие подходы.

Дополнительно для некоторых алгоритмов типа Видемана – Копперсмита построена модель параллельных вычислений на системах с распределенной памятью; полученны оценки на время выполнения таких алгоритмов. Указана связь между алгоритмами Видемана – Копперсмита, Ланцоша – Паде и Монтгомери.

В **разделе 7 основного содержания диссертации** построен новый алгоритм решения больших разреженных систем линейных уравнений над большими конечными полями. Показано, что конструкция метода Ланцоша – Паде над полем GF(2) в случае большого поля допускает значительное упрощение. Предложенный алгоритм назван блочным методом Ланцоша – Паде. Введено понятие точек синхронизации, использование которых позволяет уменьшить требования к объему используемой памяти. Алгоритм, использующий точки синхронизации, назван универсальным методом Ланцоша – Паде для систем линейных уравнений над большими полями. Для новых методов рассмотрена простейшая модель организации параллельных вычислений. Получены оценки параллельной сложности.

В **приложении** приводятся дополнительные теоретические сведения, используемые в основном содержании диссертационной работы.

Степень обоснованности научных положений, выводов и рекомендаций. Большинство положений и выводов диссертации обоснованы. Достоверность результатов подтверждается необходимыми математическими доказательствами, компьютерными экспериментами и актами внедрения. Результаты являются новыми, что подтверждается авторскими публикациями в рецензируемых научных изданиях.

Подтверждение опубликования основных результатов диссертации. В журналах

из перечня ведущих рецензируемых научных журналов и изданий, рекомендованных ВАК, по теме диссертации опубликовано 16 работ (в соавторстве 4). Получен 1 патент и 2 два свидетельства о регистрации права на ПО. Результаты диссертации обсуждались на кафедрах МГУ и других организациях (в Академии криптографии РФ, в Математическом институте им. В.А. Стеклова РАН, в Институте проблем информатики РАН и др.). По результатам диссертации автором были сделаны доклады на российских и международных конференциях.

Научная новизна. В диссертационной работе предложена новая оценка сверху на сложность задачи дискретного логарифмирования через сложность задачи Диффи-Хеллмана. Изложенный метод применен к оценке сложности задачи дискретного логарифмирования на группе точек эллиптической кривой простого порядка p, в случае когда $p-1$ раскладывается на небольшие взаимно простые множители. Показано, что в этом случае обе задачи полиномиально эквивалентны. Получены новые оценки о числе и величине простых делителей чисел вида $p-1$, где p – простое. Получена новая оценка снизу для функции Эйлера для почти всех аргументов. Показано, что задача задача универсальной подделки ГОСТ Р 34.10-1994 сводится к нахождению неподвижных точек в задаче дискретного логарифмирования. Построены аналитические формулы для таких неподвижных точек, отличные от общеизвестных. Предложены новые алгоритмы решения разреженных систем линейных уравнений над полем $GF(2)$ и над большими простыми полями. Структура новых алгоритмов допускает их реализацию на вычислительных системах с медленными и ненадежными коммуникациями между отдельными узлами.

Замечания к диссертационной работе.

1. Некоторые свои результаты из первого раздела автор представляет несколько тенденциозно. Например, на с. 9 читаем: *теорема 1.3 вошла в обзор Маурера-Вольфа в качестве одного из итоговых результатов.* На деле конкретная формулировка теоремы в указанном обзоре не упоминается; вместо этого сказано лишь, что «Черепнев использовал тот же самый метод для построения алгоритма, решающего DL-задачу, из алгоритма решения DH-задачи. Из-за результатов Шупа редукция Черепнева не требуется для доказательства нижней оценки сложности DH-задачи».

   Кроме того, на стр. 3, 9 автор утверждает, что функция высоты дерева Пратта s рассмотрена им впервые. Но в статье Конягина и соавторов, на которую имеются ссылки в диссертации, указано, например, что Катаи получил нижнюю оценку $s(p) \geqslant c \log_2 p$ в 1968 г. Вероятно имелось ввиду, что функция $s(m)$ впервые применялась автором именно к задаче редукции.

2. На с. 16 автор называет гипотезу Коняева и соавторов о нормальном порядке арифметической функции $s(p)$, равном $e \log_2 p$, гипотезой о точной верхней оценке; это несправедливо.

3. Теоремы главы 2 можно коротко описать так: $p-1$ имеет около $\log_2 p$ простых множителей, равномерно распределенных на дважды логарифмической шкале. Информация об одном (или двух последовательных) уровнях дерева Пратта, однако, не дает какого-либо существенного понимания о свойствах дерева в целом

(в частности, его высоте). Соображения в начале с. 61, упоминающие тривиальную вернюю оценку для функции s, явно недостаточны. Во всяком случае, новых оценок для s раздел 2 в итоге не дает.

4. текст раздела 6 основного содержания диссертации по-видимому содержит не весь материал, на основании которого автор делает заключения и выводы. Это приводит к разного рода нестыковкам и несоответствиям. Например, на стр. 32 сообщается буквально следующее: «далее последовательно излагаются несколько версий нового алгоритма. Для наилучшей с нашей точки, оптимизированной версии доказана оценка сложности, представленная в теореме ??.» Знаки вопроса в номере теоремы можно было бы списать на типографскую опечатку, но в реальности в тексте нет ни оптимизированной версии алгоритма, ни теоремы о сложности такого алгоритма. Это упоминание об оптимизированной версии алгоритма не является единственным. На стр. 162 снова встречается ссылка «на подраздел, посвященный оптимизированной версии». Ссылки встречаются и на стр. 160 и 161, причем на стр. 161 оптимизированная версия увязывается с «процедурой синхронизации», описание которой отсутствует в этом разделе.

   Список несоотвествий можно продолжить. Так на стр. 156 диссертационной работы находим: «как будет показано ниже, существует алгоритм, реализующий умножение плотного блока размера $N \times n$ на маленькую матрицу из $\mathbb{F}^{n\times n}$ за время $\mathcal{O}(N/(n\log(N)))$, а также алгоритм, реализующий умножение ...». Тем не менее, в тексте диссертации описание такого алгоритма отсутствует.

   Трудности с пониманием раздела 6 диссертации многократно возрастают в связи со сказанным выше и регулярным употреблением оборота «наш алгоритм». Совершенно непонятно, какой именно алгоритм является «нашим». Единственным алгоритмом, имеющим полное описание, является блочный алгоритм Ланцоша – Паде, представленный в разделе «Алгоритм типа Ланцоша - Паде (первая версия)» стр. 139. Маловероятно, что автор имел ввиду именно этот алгоритм.

   Аналогичное замечание относится и к таблицам на стр. 33 и 35. Аналитические оценки из таблицы на стр. 33, предложены для алгоритмов, которых нет в таблице на стр. 35.

5. Утверждение автора стр. 143 диссертации, что «время работы алгоритмов Ланцоша – Паде сокращается практически до естественной границы – времени на построение пространства Крылова» *неверно.*

   Если рассматривать размер блока в блочном методе Ланцоша – Паде как единственный ресурс параллельности алгоритма, то в таком случае (вне зависимости от того используются или нет в алгоритме точки синхронизации) параллельная сложность алгоритма Ланцоша – Паде будет иметь немасштабируемое слагаемое $\mathcal{O}(N^2)$ (где N – размер симметризованной A^TA матрицы линейной системы). Наличие такого немасштабируемого слагаемого не является следствием обмена данными, а связано с выполнением операций с плотными матрицами и блоками. Если точки синхронизации не используются, то это слагаемое получается, например, из вычислений по формулам (6.20), (6.21) для случая поля GF(2), и вычислений по

формулам (7.23) (7.25) для случая большого поля. Если же точки синхронизации используются, то соответствующее слагаемое появляется на этапе перевычисления (**Шаг 4 (a)** универсального метода Ланцоша – Паде, стр. 240 диссертации) новых блоков направлений. Эффект близкой к идеальной масштабируемости метода Ланцоша – Паде наблюдается только для относительно небольших размеров блока.

6. Описание деталей хранения данных и параллельной реализации алгоритмов из раздела 6 является с точки зрения собственно реализации параллельных вычислений существенно неполным. Известно, что эффективность выполнения различных операций над векторами, матрицами и блоками, может требовать различных способов хранения одних и тех же данных. На практике это приводит к необходимости создавать преобразователи (конверторы) из одного формата данных в другой. Применение конвертеров существенно влияет на время выпонения алгоритма и может полностью нивелировать алгоритмические преимущества. В предлагаемом описании алгоритма Ланцоша – Паде для поля GF(2) такой потенциально опасной операцией является работа со столбцами в «процедуре доортогонализации» стр. 156 – 158 диссертации. Если предположить (как делает автор), что матрицы и блоки хранятся по строкам, то работа со столбцами, необходимая в «процедуре доортогонализации», окажется весьма неэффективной.

7. Сравнение автором времени выполнения алгоритмов Монтгомери, Ланцоша – Паде, матричного Видемана – Копперсмита и супербыстрого варианта Томэ алгоритма Видемана – Копперсмита едва ли может считаться объективным. Не потому что автор не старается быть объективным, а потому что это невозможно. Вообще говоря, более или менее адекватное сравнение можно предположить только для последовательной алгоритмической сложности. В этом случае метод Видемана – Копперсмита в версии Томэ *выигрывает за явным преимуществом.* Реальная ситуация много сложнее. Для аналитической оценки параллельной сложности, а тем более для оценки времени выполнения различных алгоритмов на реальных или воображаемых вычислительных системах анализ должен учитывать слишком большое число деталей. Вот простой пример. В работе Томэ получена оценка на сложность супербыстрого алгоритма Видемана – Коппперсмита. Однако эта оценка не учитывает возможности выполнения супербыстрого шага на параллельном вычислителе, что не соответствует практике!

   Представляется, что авторская оценка алгоритма Ланцоша – Паде *как алгоритма принципиально лучшего (стр. 32 диссертации), чем алгоритм Видемана – Копперсмита* необъективна. В разных ситуациях (для разных вычислительных систем) более предпочтительным может оказаться тот или иной алгоритм, в том числе и алгоритм Монтгомери. Идеальной нишей для алгоритма Ланцоша – Паде, по-видимому, являются вычислительные системы с медленными и ненадежными коммуникациями.

8. В разделе 6 недостаточно последовательно прописана архитектура паралелльного вычислителя. На стр. 140 принимается следующее предположение: рассматрива-

ются вычислительные системы с распределенной памятью, для которых не делается дополнительных предположений о топологии межузловых (межпроцессорных) соединений (предлагается считаеть, что в топология – кольцо). Однако это предположение выдерживается не долго. На стр. 171 находим: «будем считать, что на кластере возмжна как адресная рассылка между выполняющими конкретные задания вычислительными узлами, так и рассылка с фиксированного узла на узлы некоторой группы по бинарному дереву (бродкаст), то есть за логарифм *времени* от числа элементов этой группы.» В топологии кольцо это невозможно.

На стр. 175 к уже определенной вычислительной системе вдруг приписываются дополнительные вычислители числом p для каждой группы из l узлов. Последнее значительно усложняет понимание текста и, скорее всего, приводит к неверным выводам.

9. в разделе 7 в финальных формулах (7.65) и (7.66) для сложности и параллельной сложности метода Ланцоша – Паде пропущены слагаемые n^2K и n^2, соответственно.

10. В диссертации имеется ряд опечаток стр. 70, 92, 114, 134.

Заключение. В целом диссертационная работа Черпнева М.А. «О вычислительной сложности алгоритмов фактоизации и дискретного логарифмирования» является исследованием, в котором разработаны теоретические положения, совокупность которых можнго квалифицировать как крупный вклад в криптографию. Разработаны условиия полиномиальной эквивалентности задач Диффи – Хелманна и дискретного логарифмирования; исследована задача о неподвижных точках в задаче дискретного логарифмирования для построения поддельной подписи в схеме Эль – Гамаля; произведен анализ ядра преобразования спуска Вейля в задаче дискретного логарифмированияя на эллиптических кривых над полем характеристики 2; построены блочные алгоритмы решения больших разреженных систем линейных уравнений над полем GF(2) и полями с большим числом элементов, допускающими реализацию на вычислительных системах с медленными коммуникациями.

Содержание автореферата полностью соответствует основным положениям диссертации.

Диссертационная работа Черепнева Михаила Алексеевича полностью удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней» ВАК, предъявляемых к диссертации на соискание ученой степени доктора физико-математических наук, а ее автор заслуживает присуждения степени доктора физико-математических наук по специальности 01.01.09 – дискретная математика и кибернетика.

Отзыв обсужден и утвержден на семинаре «Матрицы и вычисления», 05.04.17.

Директор ИВМ РАН, академик Тыртышников Е.Е.

28.04.2017