ОТЗЫВ

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

Актуальность избранной темы. Исследование сложности алгоритмов факторизации целых чисел и дискретного логарифмирования в конечных группах интенсивно исследуются в связи с тем, что на предположении их сложности строятся и другие «трудные» задачи теории конечных групп – задачи RSA, Рабина, Диффи–Хеллмана и др. В свою очередь, оценки сложности этих задач необходимы для анализа безопасности основанных на них криптографических систем, например RSA или Эли Гамаля, а также криптографических протоколов распределения ключей по открытым каналам и цифровой подписи. Задачи дискретного логарифмирования и Диффи-Хеллмана имеют место, как в числовых группах, так и в группах точек (дивизоров) эллиптических (гиперэллиптических) кривых. Соответственно имеются «числовые» и «эллиптические» варианты протоколов. При этом имеются два подхода к выбору поля, над которым задается эллиптическая кривая – простое поле или расширение простого поля. Во втором случае операции умножения на константу выполняются быстрее, но возникает необходимость сравнения сложности обратных операций – нахождения константы, умножением на которую базовой точки получена данная точка (это достигается решением задачи дискретного логарифмирования для эллиптической кривой) – в этих алгебраических структурах. В диссертации выявлены условия, при которых использование расширения поля понижает сложность задачи дискретного логарифмирования. В связи с тем, что задача Диффи-Хеллмана в известном смысле «не труднее» задачи дискретного логарифмирования важно оценить возможность решения второй с использованием первой. Автором выявлены условия, при которых сложность дискретного логарифмирования полиномиально эквивалентна сложности задачи Диффи-Хеллмана. При этом существенную роль имеет структура дерева множителей числа $p-1$ (дерева Пратта), изучению которой в диссертации уделено должное внимание. Алгоритмы факторизации целых чисел интенсивно совершенствуются и существенную роль (применительно к алгоритмам факторизации с факторной базой) при этом имеют методы решения систем линейных уравнений над двоичным полем и над конечными полями. Эти алгоритмы создаются в предположении осуществления распределенных вычислений, при этом существенной задачей является ограничение информационных обменов с тем, чтобы можно было использовать медленные каналы сети Интернет, чему отвечают созданные автором алгоритмы решения разреженных систем линейных уравнений. Эти задачи линейной алгебры возникают и при дискретном логарифмировании. Описанные проблемы

факторизации и дискретного логарифмирования и полученные автором результаты позволяют оценить и уточнить отечественные стандарты для систем информационной безопасности.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. Полученная оценка сверху трудоемкости задачи дискретного логарифмирования при помощи задачи Диффи-Хеллмана основана на результатах автора по исследованию структуры дерева Пратта с использованием введенной автором и признанной международным криптографическим сообществом функции максимальной длины цепи, соединяющей корень и лист этого дерева. Доказательство полученной оценки имеет конструктивный характер: впервые построен алгоритм решения задачи дискретного логарифмирования при помощи оракула, решающего задачу Диффи-Хеллмэна для элементов той же группы. Использование этого алгоритма позволило доказать полиномиальную эквивалентность задач дискретного логарифмирования и Диффи-Хеллмэна для некоторых эллиптических кривых, удовлетворяющих современному государственному стандарту на цифровую подпись Р.34.10 – 2012. Этот результат стал хорошо известен международному криптографическому сообществу (обзор Maurer, Wolf "Diffie-Hellman protocol"), поскольку относится к активно разрабатываемой в современной криптографии задаче открытого распределения ключа. Доказанная в ряде случаев полиномиальная или "почти" полиномиальная эквивалентность задач дискретного логарифмирования и Диффи-Хеллмэна свидетельствует в пользу надежности протокола Диффи-Хеллмэна (если не рассматривать атаку с блокировкой канала).

Обоснованные в диссертации аналитические формулы для нахождения неподвижных точек в задаче дискретного логарифмирования, а также полученные улучшенные оценки на их число позволили построить «длинную» поддельную подпись для схемы Эль-Гамаля, в частности подобной ей схемы подписи по ГОСТ Р.34.10 – 94: задача универсальной подделки таких подписей сведена к задаче нахождения неподвижных точек в задаче дискретного логарифмирования.

Условия, при которых использование расширения поля понижает сложность задачи дискретного логарифмирования, выявлены автором на основе доказательства при определенных условиях невырожденности ядра преобразования спуска Вейля при решении задачи дискретного логарифмирования на эллиптических кривых над полем характеристики 2.

Автором обоснован новый блочный алгоритм решения больших разреженных систем линейных уравнений над полем из двух элементов, которые возникают в алгоритме целой факторизации с факторной базой. При этом автором решена проблема построения матричных приближений Паде к матричному ряду при помощи полиномиального от длины этого ряда алгоритма. Принципиальная сложность этой задачи, по сравнению с известным случаем поля, заключается в существовании в кольце матриц делителей нуля. Далее автором предложена новая

формула построения ортогонального базиса пространства Крылова из приближений Паде формального ряда с коэффициентами – скалярными произведениями блоков произвольного базиса. Отметим, что формулы, предлагавшиеся для этой цели в скалярном случае другими авторами (Гуткнехт), в случае матричных коэффициентов неприменимы. Благодаря тому, что преобразование, задаваемое этими формулами, сохраняет сложение и умножение многочленов автору удалось предложить процедуру синхронизации, которая избавила от необходимости построения многочленов со степенью, равной размеру исходной системы. Это позволило убрать логарифмические множители в оценке времени работы алгоритма и избавиться от необходимости иметь дополнительную растущую оперативную память к той, которая содержит исходную задачу. При этом основные преимущества используемых в настоящее время для решения больших разреженных линейных систем алгоритмов Монтгомери и Видемана-Копперсмита сохранены. При этом алгоритм Видемана-Копперсмита, при помощи которого получен современный рекорд целочисленной факторизации, значительно превзойдён асимптотически и по времени работы и объёму используемой памяти и по вероятности срабатывания. Одно из основных преимуществ по сравнению с алгоритмом Монтгомери состоит в возможности группировать однотипные операции, что позволяет применять для их оптимизации специальные алгоритмы с распределёнными вычислениями.

На основе этих результатов сконструирована серия алгоритмов, которые имеют преимущества перед известными алгоритмами и допускают использование медленных каналов передачи данных между вычислителями и не связаны с использованием в них данных сверх данных, представляющих исходную задачу.

В диссертации указанная техника перенесена на случай систем над большим простым полем, что позволяет применить данный метод в алгоритме дискретного логарифмирования. Автором построен алгоритм решения больших разреженных систем над произвольным конечным полем, в котором объединены возможная минимальность количества операций с возможностью проводить все вычисления на слабо связанных (Интернет) вычислительных ресурсах, что позволяет добиваться минимального времени работы.

Полученные теоретические результаты *обоснованы* и их *достоверность* подтверждена необходимыми доказательствами и результатами компьютерных экспериментов. Результаты являются *новыми*, что подтверждается авторскими публикациями в рецензируемых научных журналах и монографии и признанием на мировом уровне.

Замечания. Исследования старого российского стандарта ГОСТ Р.34.10, возможно, уже не актуальны, хотя и подтверждают практическую значимость работы.

Новые доказательства, использующие представление Мамфорда дивизоров в виде пары многочленов, известных результатов об арифметических свойствах дивизоров не содержат существенной новизны.

В диссертации следовало бы рассмотреть условия, при которых возможно использование эллиптических кривых над полем характеристики два, рекомендуемых западными стандартами.

Из текста диссертации не ясна итоговая оценка времени работы алгоритма факторизации целых чисел. Автор ограничился лишь оценками для отдельных этапов, указанием на отсутствие в его алгоритме матричных многочленов растущей степени, приводящих в алгоритме Видемана-Копперсмита к логарифмическому множителю, и общей оценкой для случая большого простого поля, в которой оптимальное значение для количества используемых вычислительных узлов не выбрано.

Заключение. В диссертации разработаны теоретические положения об условиях полиномиальной эквивалентности задач Диффи-Хеллмана и дискретного логарифмирования, об использовании неподвижных точек задачи дискретного логарифмирования для построения поддельной подписи, о невырожденности ядра преобразования спуска Вейля при решении задачи дискретного логарифмирования на эллиптических кривых над полем характеристики два, о новом блочном алгоритме решения больших разреженных систем линейных уравнений над полем из двух элементов в алгоритме целочисленной факторизации с факторной базой и о новом блочном алгоритме решения таких систем над полем большой характеристики в задачах дискретного логарифмирования. Таким образом, диссертация М.А. Черепнева является исследованием, в котором разработаны теоретические положения, совокупность которых можно квалифицировать как новое крупное достижение в развитии криптографии. Диссертация соответствует критериям, установленным Положением о присуждении ученых степеней.

Автор диссертации Черепнев Михаил Алексеевич достоин присуждения ученой степени доктора физико-математических наук по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Официальный оппонент

Фролов Александр Борисович, доктор технических наук, профессор, профессор кафедры математического моделирования Национального исследовательского университета «Московский энергетический институт».

Москва, Красноказарменная ул. д.14; e-mail: abfrolov@mail.ru

Подпись удостоверяю

ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА
УПРАВЛЕНИЯ ПО РАБОТЕ С ПЕРСОНАЛОМ
Л.И.ПОЛЕВАЯ

17.04.2017