Отзыв

на диссертационную работу Черепнева М.А.

«О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования», представляемую на соискание ученой степени доктора физико-математических наук по специальности 01.01.09 – Дискретная математика и математическая кибернетика.

Диссертационная работа М.А.Черепнева посвящена алгоритмическим вопросам решения теоретико-числовых задач целой факторизации и дискретного логарифмирования, возникающих при анализе стойкости большинства современных криптографических протоколов.

Научная и практическая ценность диссертационной работы заключается в построении самого быстрого на сегодняшний момент алгоритма решения больших разреженных систем линейных уравнений над конечным полем. Важным результатом также является доказательство невырожденности преобразования спуска Вейля на эллиптических кривых над большим полем характеристики 2. Кроме того проведён сравнительный анализ трудоёмкости решения некоторых теоретико-числовых уравнений, к решению которых сводится вскрытие современных схем защиты информации.

Достоинством первого защищаемого положения является то, что построенный алгоритм успешно масштабируется на несколько десятков тысяч вычислительных узлов, что позволяет эффективно использовать современную кластерную вычислительную технику для сокращения работы самого трудного этапа решения задач факторизации целых чисел и дискретного логарифмирования наиболее быстрыми на сегодняшний момент алгоритмами с факторной базой. Автору удалось реализовать принципиально новые приемы построения ортогональных дополнений в пространстве Крылова из приближений Паде к матричному ряду, а также построить рекуррентные формулы для построения таких приближений.

Практическая значимость второго защищаемого положения состоит в доказательстве эффективности атаки спуска Вейля на криптопротоколы, использующие сложность задачи дискретного логарифмирования на группе точек эллиптической кривой над полями характеристики 2. Этот результат показывает, что, несмотря на значительную скорость реализации арифметики в полях характеристики 2 на компьютере, их использование в криптопротоколах с

эллиптическими кривыми менее надёжно, чем использование больших простых полей.

Важно, что оба эти положения программно реализованы и внедрены, что доказывают официальные акты, а также государственные свидетельства о регистрации прав на программное обеспечение.

Автор неоднократно участвовал в научных и практических работах совместно со специалистами Академии криптографии, Института вычислительной математики РАН, ФИЦ ИУ РАН, МГУ им. М.В.Ломоносова и других организаций. М.А.Черепнев хорошо известен криптографам и профессионалам в области специальных вычислительных задач как высококвалифицированный сотрудник, работающий на переднем крае исследований стойкости современных схем защиты информации, а его диссертация отвечает всем требованиям ВАК, предъявляемым к докторским диссертациям.

Академик РАН И.А.Соколов

31.01.2017 г.