На правах рукописи

Черепнев Михаил Алексеевич

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ АЛГОРИТМОВ ФАКТОРИЗАЦИИ И ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

01.01.09 - дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва - 2017

Работа 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.
Официальные оппоненты:	д.ф.-м.н., профессор Малашонок Геннадий Иванович Институт математики, физики и информатики Тамбовского государственного университета им. Г.Р.Державина, кафедра компьютерного и математического моделирования.
	д.т.н., профессор Фролов Александр Борисович Федеральное государственное бюджетное образовательное учреждение высшего образования «Национальный исследовательский университет «МЭИ», кафедра математического моделирования.
	д.ф.-м.н., профессор Фомичев Владимир Михайлович Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации», кафедра информационной безопасности.
Ведущая организация:	Федеральное государственное бюджетное учреждение науки Институт вычислительной математики Российской академии наук имени Г.И.Марчука.

Защита состоится 18 мая 2017 г. в 13-00 на заседании диссертационного совета Д002.073.05 при Федеральном государственном учреждении «Федеральный исследовательский центр Информатика и управление» Российской академии наук» по адресу: 119333, г.Москва, ул. Вавилова, д.40.

С диссертацией можно ознакомиться в библиотеке ФИЦ ИУ РАН, а также на сайте http://www.frccsc.ru/diss-council/00207305/diss/list

Автореферат разослан 2017 г.

Ученый секретарь
диссертационного совета Д 002.073.05
д.ф.-м.н., профессор Рязанов В.В.

Общая характеристика работы

Диссертация посвящена теоретико-числовым алгоритмам. Основу составляют исследования часто используемых на практике алгоритмов целочисленной факторизации и дискретного логарифмирования, а также некоторые смежные алгоритмические вопросы. Получены оценки вычислительной сложности, а также предложены новые модификации этих алгоритмов с меньшими требованиями по памяти, объёму коммутации и времени работы при реализации на современной многопроцессорной технике.

Актуальность темы. Использование теоретико-числовых конструкций позволило в последнее время получить множество новых систем информационного обмена. Оптимизация сопутствующих вычислений стала важной задачей. Значительное место среди прикладных вычислений занимают алгоритмы целочисленной факторизации дискретного логарифмирования и связанные с ними подалгоритмы, такие как решение больших систем линейных уравнений над конечными полями. Таким образом, исследования применимости современных математических методов к алгоритммическому решению задач дискретного логарифмирования и факторизации имеют важное прикладное значение.

Таким образом, тема диссерации, посвященной применению современных методов теории чисел к оценке вычислительной сложности теоретико-числовых алгоритмов факторизации и дискретного логарифмирования актуальна как в теоретическом, так и в прикладном смысле.

Предмет исследования - теоретико-числовые алгоритмы факторизации, дискретного логарифмирования и решения больших разреженных систем над конечным полем, а также смежные алгоритмические вопросы.

Цель работы - Оптимизация и адаптация рассматриваемых теоретико-числовых алгоритмов под современные программно-аппаратные средства. Получение теоретических и практических оценок вычислительной сложности этих алгоритмов. Выявление зависимости вычислительной сложности рассматриваемых алгоритмов от способа задания и параметров входных данных.

Для достижения поставленной цели в диссертации изложены новые теоретические результаты, в частности новые теоретико-числовые алгоритмы, позволяющие существенно упростить задачи факторизации и дискретного логарифмирования в конкретных случаях, имеющих важное практическое значение.

Научная новизна работы состоит в строго доказанных новых теоремах и корректных теоретико-числовых алгоритмах с доказанными оценками на время работы, объём требуемой памяти, объём передачи данных и эффективность использования параллельных вычислений.

- Построен новый алгоритм решения задачи дискретного логарифмирования с оракулом Диффи-Хеллмэна. Как результат применения этого алгоритма получено новое выражение сложности задачи дискретного логарифмирования через сложность задачи Диффи-Хеллмэна. Как следствие построенного алгоритма доказана полиномиальная эквивалентность задачи дискретного логарифмирования и задачи Диффи-Хеллмэна для некоторых кривых, удовлетворяющих действующему стандарту цифровой подписи ГОСТ Р 34.10-2012. Построен алгоритм, сводящий вскрытие схемы Диффи-Хеллмэна к решению системы полиномиальных уравнений с оценками на её степень.

- Показано, что универсальная подделка схем цифровой подписи, построенных на основе схемы Эль-Гамаля, сводится к нахождению неподвижных точек в задаче дискретного логарифмирования. Построены новые формулы для таких точек, а также получены оценки

снизу на число первообразных корней, удовлетворяющих условию Бризолиса, которые приводят к оценке числа таких точек снизу.

- При некотором легко проверяемом условии доказана невырожденность гомоморфизма, построенного в методе спуска Вейля дискретного логарифмирования на эллиптических кривых над полем характеристики 2. Получены новые свойства ядра этого гомоморфизма, характеризующие, в частности, его объём.

- Предложено несколько модификаций нового алгоритма решения больших разреженных систем линейных уравнений над конечным полем. Получены оценки на время его работы, объём необходимой оперативной памяти, объём коммутации а также эффективное число используемых независимых вычислительных узлов лучшие, чем у современных аналогов.

Практическая значимость работы заключается в следующем:

1. Доказана полиномиальная эквивалентность задач дискретного логарифмирования и Диффи-Хеллмэна в случае ограниченной длины ветвей дерева Пратта (в частности для некоторых кривых ГОСТ Р 34.10-2012). Кроме того, представленное доказательство даёт алгоритм решения задачи дискретного логарифмирования из алгоритма решения задачи Диффи-Хеллмэна в группах, образованных некоторыми подмножествами исходной группы с некоторыми специальными операциями, связанными с оракулом Диффи-Хеллмэна.

2. Получены новые оценки на величину и количество простых делителей чисел вида $p-1$.

3. Задача универсальной подделки цифровой подписи ГОСТ Р 34.10-1994 сведена к нахождению неподвижных точек функции дискретного логарифма. Тем самым доказано, что указаный ГОСТ без проверки длины подписи является нестойким. Получены аналитические формулы для указанных неподвижных точек, а также получена оценка на их число снизу.

4. При выполнении некоторых легко проверяемых условий доказана невырожденность гомоморфизма спуска Вейля. Это показывает, что использование эллиптических кривых над полем большой простой характеристики надёжнее, чем использование кривых над полем характеристики 2.

5. Построен новый алгоритм решения больших разреженных систем линейных уравнений. Доказано, что этот алгоритм эффективнее алгоритма Видемана-Копперсмита (имеет асимптотически лучшие характеристики). Кроме того, новый алгоритм позволяет использовать вычислительные ресурсы общего применения, связанные относительно медленными каналами связи. Построенные модификации алгоритма могут быть применены для решения задачи факторизации целых чисел и задачи дискретного логарифмирования в конечном поле.

Достоверность и обоснованность результатов обеспечиваются строгими математическими доказательствами теоретических результатов и подтверждаются компьютерными программами, результатами и замерами времени их работы и объёма используемой памяти. Все результаты, приведённые в основной части диссертации (1-7 глава), являются новыми, снабжены разъяснениями используемых понятий и определений.

Результатами диссертации, выносимыми на защиту, являются:

1. В общем случае получена оценка сверху на сложность задачи дискретного логарифмирования через сложность задачи Диффи-Хеллмэна. Данная оценка в ряде случаев приводит к полиномиальной эквивалентности этих задач. Полученная оценка обобщает результаты работы Боера 1988 года и работы Маурера 1994 года на общий случай. Эта теорема вошла в обзор Маурера и Вулфа 2001 года "Diffie-Hellman Protocol" в качестве одного из итоговых результатов. Впервые рассмотрена функция максимальной длины дерева Пратта $s(m)$ числа m. Это дерево введено в рассмотрение в 1975 году Праттом, который предложил его для

использования в алгоритме проверки простоты. В 1997 году Шуф показал, что алгоритм общего применения (generic algorithm), решающий задачу Диффи-Хеллмэна, не может быть "простым" (имеет экспоненциальную сложность для групп простого порядка). Однако, доказанная теорема об оценке применима не только к алгоритмам общего применения, но и к алгоритмам, работающим с элементами фиксированной группы, связанными несколькими специальными групповыми операциями.

Функция $s(m)$ была в 2008 году исследована Фордом, Конягиным и Люка, которые получили для неё нетривиальные оценки. Полученная ими оценка сверху отличается от тривиальной несколько лучшей константой в показателе. Поэтому её применение совместно с рассматриваемой оценкой не даёт новой информации о связи сложностей задач дискретного логарифмирования и Диффи-Хеллмэна. В этой же работе была высказана гипотеза об асимптотическом поведении функции $s(m)$ как $O(\ln \ln m)$ для почти всех m. Применение этой оценки уже приводит к нетривиальным результатам. А именно, в случае полиномиальности решения задачи Диффи-Хеллмэна получается алгоритм решения задачи дискретного логарифмирования, работающий "почти" полиномиально (лучше субэкспоненты).

Изложенный метод, применён к оценке сложности задачи дискретного логарифмирования на группе точек эллиптической кривой простого порядка p, где $p-1$ раскладывается на маленькие взаимнопростые множители. Такой случай возможен для кривых, удовлетворяющих ГОСТ Р 34.10-2012. Показано, что в этом случае задачи дискретного логарифмирования и Диффи-Хеллмэна полиномиально эквивалентны. Кроме того, построен конструктивный полиномиальный алгоритм вычисления дискретного логарифма при помощи оракула Диффи-Хеллмэна.

2. Доказаны теоремы о величине и числе простых делителей чисел вида $p-1$, где p - простое число. Эти теоремы предоставляют информацию о структуре одного шага дерева Пратта, которую можно использовать и при построении алгоритма дискретного логарифмирования с оракулом Диффи-Хеллмэна. Получена новая оценка снизу функции Эйлера для почти всех аргументов.

3. Проведён анализ некоторых известных некоммутативных групп на стойкость построенной на их основе схемы открытого распределения ключа, предложенной В.М.Сидельниковым [1]. Доказано, что задача разложения на множители в них является полиномиальной, а схема В.М.Сидельникова с их использованием — нестойкая. Предложен пример некоммутативной мультипликативной операции с несколько большей сложностью задачи разложения на множители.

4. Показано, что задача универсальной подделки ГОСТ Р 34.10-1994 [26] сводится к нахождению неподвижных точек в задаче дискретного логарифмирования. Построены аналитические формулы для вычисления пар (x, R), удовлетворяющих сравнению

$$x \equiv R^x (\mod p), x, R \in \mathbb{Z}, (R, p) = 1,$$

отличные от общеизвестных: $(g, g^{g^{-1} (\mod p-1)})$, где g - первообразный корень, удовлетворяющий условию $(g, p-1) = 1$ (условие Бризолиса). В этих формулах R уже необязательно первообразный корень. Доказана теорема о существовании решения с R, имеющим достаточно большой простой порядок. Получены оценки на число первообразных корней, удовлетворяющих условию Бризолиса.

5. Проведён анализ метода спуска Вейля при решении задачи дискретного логарифмирования на эллиптических кривых над полем характеристики 2. Основным

инструментом в этом исследовании выбрано представление Мамфорда приведённых дивизоров парой многочленов. Данное представление можно корректно связать с классами дивизоров (по модулю дивизоров рациональных функций).

Доказано, что при выполнении некоторого достаточно легко проверяемого условия порядок ядра преобразования спуска Вейля не делится на 2. Это означает, что в случае, когда порядок группы точек на эллиптической кривой делится на 2, сужение преобразования спуска Вейля на эту группу нетривиально.

6. Проанализирована сложность линейного этапа алгоритма факторизации целых чисел. Предложен новый алгоритм решения разреженных систем линейных уравнений над $GF(2)$, которые возникают при решении этой задачи алгоритмами с факторной базой. Доказано, что параллельная реализация построенного алгоритма работает быстрее алгоритма Видемана-Копперсмита 1993г., который был применён при постановке последнего рекорда факторизации чисел RSA в декабре 2009 г. Предложенная техника не только сохраняет возможность частичного распараллеливания высокого уровня при решении таких систем (то есть часть алгоритма может быть реализована на не связанных друг с другом кластерах), но позволяет вообще исключить использование кластеров большой мощности. Другими словами, эта техника позволяет распараллелить весь алгоритм на связанные медленным каналом ($Internet$) вычислители, единственное требование к которым - это возможность содержать в оперативной памяти рассматриваемую задачу (матрицу линейной системы). Помимо уменьшения времени на решение линейной системы, предложенный алгоритм не требует кратного увеличения оперативной памяти сверх объёма, необходимого для хранения указанной матрицы, как это было при постановке рекорда целой факторизации в декабре 2009 года при помощи алгоритма Видемана-Копперсмита. Таким образом, предложенный алгоритм превосходит алгоритм Видемана-Копперсмита по всем основным параметрам. Преимуществом по сравнению с алгоритмом Монтгомери 1994г. является более высокая точка насыщения, что позволяет решать значительно большие системы на многопроцессорной вычислительной технике. Таким образом, предложенный алгоритм оказывается на сегодняшний день наилучшим для использования на многопроцессорной технике с несколькими сотнями независимых вычислительных узлов.

7. Построен новый алгоритм решения разреженных систем линейных уравнений над $GF(p)$, которые возникают при решении задачи дискретного логарифмирования алгоритмами с факторной базой. Этот алгоритм обладает теми же преимуществами, что и, описанный выше, алгоритм для поля $GF(2)$.

Структура диссертации. Диссертация состоит из введения, 7 глав, списка литературы и приложения. В приложении изложены сведения, необходимые для понимания основного текста диссертации, а также текст и результаты работы компьютерной программы, реализующей предлагаемый алгоритм решения больших разреженных линейных систем. Общий объём диссертации 294 страницы.

Содержание работы

В первой главе диссертации рассматривается задача дискретного логарифмирования и связанные с её решением вопросы распределения целых простых чисел. Задача дискретного логарифмирования рассматривается в конечных полях, кольцах вычетов, на эллиптических кривых, а также в общей постановке.

В некоторых случаях дискретное логарифмирование оказывается простой задачей и имеет даже аналитическое выражение.

Частным Ферма называется функция

$$Q_m \pmod m : \quad (\mathbb{Z}/m^2\mathbb{Z})^* \to \mathbb{Z}/m\mathbb{Z},$$

определяемая по модулю m, где

$$Q_m(a) = \frac{a^{L(m)}-1}{m},$$

где $L(m)$ - функция Кармайкла, максимальный порядок элементов мультипликативной группы вычетов по модулю m (универсальная экспонента).

Далее (см. [26, 30]) получена формула для подъёма решений, когда основание дискретного логарифма по простому модулю не является первообразным корнем.

Пусть $p \mid Q_p(g)$. Обозначим $l = \gamma_p(Q_p(g)) \in \mathbb{N}$, то есть $p^l \parallel Q_p(g)$ (или $p^l \mid Q_p(g), p^{l+1} \nmid Q_p(g)$).

Теорема 1 ([26, 30, 20]) *Пусть p – простое число, $(g,p) = 1, l = \gamma_p(Q_p(g)) \in \mathbb{N}, \alpha \in \mathbb{N} \setminus \{1\}$. Тогда, если сравнение*

$$a \equiv g^x \pmod{p^\alpha} \tag{1}$$

разрешимо, то его решение x удовлетворяет следующим условиям

1. *При $\alpha \in \{1, \ldots, l\}$ выполнено $ord_{p^\alpha} g = ord_p g$ и x есть единственное $\pmod{ord_p g}$ решение сравнения*
$$a \equiv g^x \pmod p \tag{2}$$
2. *При $\alpha \geq l+1, k = \max\{l+1, \alpha-(l+1)\}$ выполнено равенство $ord_{p^\alpha} g = p^{\alpha-(l+1)} ord_p g$ и x есть единственное $\pmod{p^{\alpha-(l+1)} ord_p g}$ решение системы*
$$\begin{cases} a \equiv g^x \pmod p \\ x\frac{Q_{p^{k-l}}(g)}{p^l} \equiv \frac{Q_{p^{k-l}}(a)}{p^l} \pmod{p^{\alpha-(l+1)}}. \end{cases} \tag{3}$$

Данная теорема даёт формулы с меньшим модулем и меньшей степенью, чем в случае перехода к основанию, являющемуся первообразным корнем.

Наиболее распространённой схемой распределения ключа, основанной на задаче дискретного логарифмирования, является схема Диффи-Хеллмэна с использованием односторонней функции возведения в степень в конечной группе. Она, наряду со схемой RSA, была положена в основу широко применяемой схемы "Kerberos".

Для вскрытия схемы Диффи-Хеллмэна необходимо решить следующую задачу: по известным p, g, g^a, g^b найти g^{ab}. Эта задача носит название задачи Диффи-Хеллмэна. В диссертации вопрос о полиномиальной эквивалентности задачи Диффи-Хеллмэна и задачи дискретного логарифмирования для произвольной конечной мультипликативной группы сводится [2] к оценкам длины максимальной ветви дерева Пратта порядка этой группы.

Пусть $G(t,m)$ — произвольная циклическая группа порядка m с операцией, которую будем в дальнейшем обозначать $+$, требующей для своего выполнения t битовых операций, и пусть $L(t,m)$ обозначает минимальное количество битовых операций, необходимых для решения задачи дискретного логарифмирования в группе $G(t,m)$, то есть при известных $a, b \in G(t,m)$ найти $n \in Z_m$ такое, что

$$a = nb, \tag{4}$$

здесь nb есть $b + \cdots + b$, где элемент b повторяется n раз.

Будем предполагать, что решение уравнения (4) существует.

Не ограничивая общности дальнейших рассуждений, будем считать b образующим группы $G(t, m)$.

Пусть $D(t, m)$ — не убывающая по m оценка количества битовых операций, необходимых для решения задачи Диффи-Хеллмэна в $G(t, m)$: при известных a_1, a_2 и b, таких, что $a_1 = n_1 b, a_2 = n_2 b$, найти

$$a_3 = (n_1 n_2)b. \tag{5}$$

Пусть $D^*(t, m)$ — также неубывающая по m оценка количества битовых операций, необходимых для решения той же задачи при помощи алгоритмов, количество битовых операций в которых удовлетворяет неравенству

$$D^*(t, m) \leq tD^*(C, m),$$

для некоторой абсолютной константы C (например таких, которые используют только операции, совокупная сложность которых не более, чем совокупная сложность используемых групповых операций).

Назовём задачу дискретного логарифмирования в группе $G(t, m)$ сертифицированной, если заранее известны все простые числа, стоящие в узлах дерева Пратта числа m,а также хотя бы один первообразный корень для каждого такого простого числа.

Теорема 2 ([2]) *Для сертифицированной задачи дискретного логарифмирования*

$$L(t, m) \leq s \log^2 m D(\dots D(D(t, m), m) \dots), \tag{6}$$

где справа изображена s- кратная композиция функции $D(t, m)$ по первому аргументу, а логарифм берётся по некоторому постоянному основанию, не зависящему от t, m.

$$L(t, m) \leq ts \log^2 m (D^*(C, m))^s. \tag{7}$$

Данная теорема обобщает результаты Маурера на случай $s > 1$ для негладких чисел.

Для оценки параметра $s(m)$ необходимо изучить распределение простых делителей чисел вида $p - 1$ для простых p. Некоторые свойства этого распределения приведены ниже.

Отметим, что после публикации этой теоремы Шуф показал, что любой вероятностный алгоритм, решающий задачу Диффи-Хеллмэна в произвольной группе фиксированного порядка с вероятностью не меньше константы ("generic algorithm"), не может иметь сложность меньше $O(\sqrt{p})$, где p - максимальный простой делитель порядка. В теореме 2 исходная группа фиксирована, а её результат применим для алгоритмов, работающих лишь в исходной группе и группах, состоящих из её элементов с операциями специального вида, получаемых из исходной и связанными с оракулом Диффи-Хеллмэна.

В 2008 году, K. Ford, С.В.Конягин, F.Luca доказали, что для почти всех натуральных чисел m выполнено $c_1 \log_2 \log_2 m \leq s(m) \leq c_2 (\log_2 m)^{1-0.0378}$ с некоторыми абсолютными константами c_1, c_2. Там же высказана гипотеза о том, что точная верхняя оценка совпадает с приведённой

здесь нижней. В этом случае предыдущая теорема даёт "почти" полиномиальную зависимость между сложностями задач дискретного логарифмирования и Диффи-Хеллмэна.

Для группы точек на эллиптической кривой хорошо известны эндоморфизмы $[n]$ – n-кратного сложения точек с собой. Пусть используемая циклическая группа точек $< P >$ кривой имеет простой порядок p. Пусть $p-1 = \prod_{i=1}^{t} {q_i}^{\alpha_i}$ - разложение $p-1$ на простые множители. В стандарте ГОСТ Р 34.10-2012 не указано никаких требований на это разложение.

Пусть по двум точкам эллиптической кривой над простым полем из r элементов $Q, P \in E[\mathbb{F}_r]$, связанным равенством

$$Q = [n]P,$$

надо найти n, определённое по модулю p. Обозначим сложность этой задачи $DLE(r,p)$, а сложность вычисления $[n_1 n_2]P$ по паре $([n_1]P, [n_2]P)$ обозначим $DHE(r,p)$. Будем полагать, что эта последняя задача не проще одной операции на эллиптической кривой $E[\mathbb{F}_r]$. Символом log будем обозначать логарифм по некоторому фиксированному основанию, значение которого каждый раз будет некоторой эффективной абсолютной константой.

Теорема 3 ([13]) $DLE(r,p) \leq \log p DHE(r,p) \sum_{i=1}^{t} \pi {q_i}^{\alpha_i}$.

В случае если ${q_i}^{\alpha_i}$ для любого i невелики, получаем полиномиальную эквивалентность задач дискретного логарифмирования и Диффи-Хеллмэна. Построенный алгоритм с оракулом, а также некоторые его модификации, описанные в первой главе диссертации, применены в ОАО "Концерн "Автоматика" к анализу систем защиты информации. Представленные нижние оценки для сложности задачи дискретного логарифмирования использованы в качестве одного из оснований для увеличения мощности используемого простого поля, о чем имеется акт внедрения.

Приведённый анализ может быть усилен применением спаривания Эйта [13].

Во второй главе получены новые оценки на число и величину простых чисел вида $p-1$, где p простое число. Пусть $N(M)$ — количество элементов в множестве M, $v(n)$ - количество различных простых делителей числа n, $v_{>t}(n)$ - количество различных простых делителей числа n, больших t.

Теорема 4 ([23]) *Для любого положительного* ε

$$N(p \leq x | \text{для любого простого} \quad q : p-1 = qn, n \in \mathbb{N}, q > e^{lnx/lnlnx} \text{выполнено}$$

$$v(q-1) \in [(1-\varepsilon)lnln\frac{x}{n}, (1+\varepsilon)lnln\frac{x}{n}]) = \frac{x}{lnx} + \overline{o}(\frac{x}{lnx}).$$

Теорема 5 ([5]) *Для любого* $\varepsilon \in (0, \frac{1}{3})$ *и* $t = e^{(lnx)^{\frac{1-\varepsilon}{2e}}}$

$$N(p \leq x | v(p-1) \in [(1-\varepsilon)lnlnx, (1+\varepsilon)lnlnx], v_{>t}(p-1) > \frac{1}{2}v(p-1)) = \frac{x}{lnx} + \overline{o}(\frac{x}{lnx}).$$

Ранее было известно лишь среднее значение функции $v(p-1)$ по простым p.

Кроме того, в диссертации получена новая оценка для функции Эйлера для почти всех натуральных чисел.

Теорема 6 ([24]) *Для некоторой абсолютной константы c справедливо равенство*

$$N\left(n \le x | \varphi(n) > \frac{cn}{\ln\ln\ln n}\right) = x + \overline{o}(x)$$

В третьей главе исследуется идея построения протокола распределения ключей на основе некоммутативной операции, выдвинутая В.М. Сидельниковым. Представлен анализ стойкости некоторых естественных примеров некоммутативных операций [1].

Предположим, что в открытом доступе имеется описание некоторой группы G и двух ее коммутативных подгрупп H и R, при этом предполагается, что не единичные элементы $h \in H, r \in R$ не коммутируют. Абоненты A и B для выработки общего секретного ключа поступают следующим образом. Каждый из них независимо друг от друга случайно вырабатывает по одному элементу из H и R и в последующем держит их в секрете. Значком $\in_R$ будем обозначать случайный выбор.

A		**B**
$h_A \in_R H, r_A \in_R R$ $g_A = h_A r_A$		$h_B \in_R H, r_B \in_R R$
	$\xrightarrow{g_A}$	
		$g_B = h_B r_B$
	$\xleftarrow{g_B}$	
$h_A g_B r_A$	$=$	$h_B g_A r_B$

Из определений вытекает, что

$$h_A g_B r_A = h_A(h_B r_B) r_A = (h_A h_B)(r_B r_A) = (h_B h_A)(r_A r_B) =$$
$$h_B(h_A r_A) r_B = h_B g_A r_B = g$$

Тем самым, общий секретный ключ g выработан.

Теорема 7 ([1]) *Описанный выше протокол В.М.Сидельникова нестоек (предложены полиномиальные алгоритмы нахождения общего секретного ключа по открытой информации) для циклических подгрупп мультипликативной группы матриц, образов эллиптических модулей в кольце эндоморфизмов конечного поля, а также их факторов по степени автоморфизма Фробениуса.*

Статья [1] написана в соавторстве. Сама идея построения протокола распределения ключей на основе некоммутативной операции, предложена В.М.Сидельниковым. Идея использования одной некоммутативной полугруппы вместо двух принадлежит В.В.Ященко. Указанная выше теорема доказана автором диссертации.

Далее в диссертации построен некоторый более стойкий пример [21, 3] ассоциативной операции для протокола В.М.Сидельникова на основе обобщённых символов Лежандра и Якоби. Приведены примеры, когда эта операция быстро вычисляется.

Если в первой главе диссертации анализировалось использование задачи дискретного логарифмирования в схемах открытого распределения ключей, то в четвёртой главе [26, 30] проанализировано использование этой задачи в схемах шифрования и электронной подписи Эль-Гамаля. Впервые показано, что задача универсальной подделки подписи ГОСТ Р 34.10-1994 эквивалентна решению сравнения

$$r \equiv R^r \pmod{p}. \tag{8}$$

Умение решать это сравнение относительно $r \in \{1, \ldots, p-1\}$ даст возможность подписывать любое сообщение, то есть осуществлять универсальную подделку. Отметим, что решение рассматриваемого сравнения не сводится сразу к задаче дискретного логарифмирования. Аналогичные рассмотрения для схем цифровой подписи Эль-Гамаля и DSA приводят к сравнению вида $r \equiv CR^r \pmod{p}, r \in \{1, \ldots, p-1\}$, что снова приводит к сравнению (8) с условием $r = C_1 r', r' \in \{1, \ldots, p-1\}$. С помощью китайской теоремы об остатках рассматриваемые сравнения могут быть легко решены для $r \in \{1, \ldots, p(p-1)\}$.

$$\begin{cases} r \equiv c_1 \pmod{p-1} \\ r \equiv CR^{c_1} \pmod{p} \end{cases} \tag{9}$$

для произвольного $c_1 \pmod{p(p-1)}$.

Получены некоторые оценки на число первообразных корней, удовлетворяющих условию Бризолиса:

$$(g, p-1) = 1. \tag{10}$$

Эти первообразные корни дают решение задачи Бризолиса

$$x \equiv R^x \pmod{p}; x, R \in \{1, \ldots, p-1\}, R - \text{первообразный корень} \pmod{p} \tag{11}$$

в виде $x = g, R \equiv g^{g^{-1} \pmod{p-1}} \pmod{p}$.

Теорема 8 ([28]) *Пусть p, d - простые, $d \mid p-1, d \geq \sqrt{p}+1$. Тогда существует (x, R) - решение уравнения (11) такое, что $ord_p R = d$.*

Теорема 9 ([28]) *Пусть $p = 2^s q + 1 > 2^{2^s}$, где p - простое, и выполнено одно из двух условий:*
1) q - простое нечётное, или
2) q - любое нечётное, $q \mid ord_p 2$.
Тогда сравнение (11) выполнено при

$$x = 2^{2^s}, R \equiv g^{qt + ind_g 2(\frac{q+1}{2})^{2^s - s}} \pmod{p}$$

для любого g - первообразного корня по модулю p, и $t \in \mathbb{N}$. Кроме того, для t, при которых показатель в последнем сравнении нечётный, R будет первообразным корнем по модулю p.

Теорема 10 ([28]) *Пусть $p \geq 5$ простое, тогда случайное нечётное число $g \in \{1, \ldots, p-1\}$ будет первообразным корнем по модулю p, удовлетворяющим условию (10) с вероятностью не меньше:*
1) $\frac{3\varphi(p-1)}{p-1} - 1$ при $p \equiv 1 \pmod{4}$;
2) $\frac{4\varphi(p-1)}{p-1} - \frac{7}{4} - \frac{1}{2(p-1)}$ при $p \equiv -1 \pmod{4}$.

Некоторые близкие к последней теореме формулы получены Кобели и Захареску (1999). Однако указанная выше теорема из них не следует. В случае *1)* для чисел типа Софи Жермен она улучшает результат Захареску асимптотически. В остальных случаях даёт лучшую оценку для простых p с числом десятичных знаков, меньшим нескольких сотен (конкретное значение зависит от константы в O(), которая в работе Захареску не приведена).

В пятой главе рассматривается задача дискретного логарифмирования на гиперэллиптических кривых.

Получены более простые доказательства некоторых теорем о свойствах дивизоров неособой гиперэллиптической кривой [22]. Эти доказательства, в отличие от известных, используют представление Мамфорда дивизоров в виде пары многочленов.

Напомним, что дивизор, имеющий неотрицательные коэффициенты, называется приведённым, если его степень не превосходит рода кривой. Доказано следующее свойство представления Мамфорда:

Теорема 11 ([25]) *Если два приведённых дивизора эквивалентны (отличаются на дивизор рациональной функции), то представляющие их пары многочленов совпадают.*

Другими словами, пары многочленов, степень которых ограничена родом кривой и удовлетворяющие условиям представления Мамфорда, взаимнооднозначно соответствуют классам дивизоров.

Далее предложен новый алгоритм приведения матрицы с целыми рациональными коэффициентами к Смитовой нормальной форме (СНФ) [25, 19], необходимой при работе с дивизорами. Данный алгоритм обладает тем свойством, что рост возникающих коэффициентов ограничен некоторой постоянной величиной, не зависящей, вообще говоря, от размера матрицы. Тем самым, он эффективнее алгоритма, предложенного для этих целей в известной книге Д.Кнута."Искусство программирования". Одновременно с СНФ данный алгоритм вычисляет и матрицу приводящих к ней преобразований. В алгоритме Сторйоханна 2013 года матрица преобразования строится после СНФ исходной матрицы с помощью нескольких дополнительных матричных умножений. Предложенный алгоритм строит матрицу преобразований параллельно с СНФ и имеет лучшие константы в главном члене оценки его сложности, чем алгоритм Сторйоханна.

Для решения задачи дискретного логарифмирования на якобиане гиперэллиптической кривой (группа классов дивизоров) над конечным полем характеристики 2 может быть применён спуск Вейля, а именно гомоморфизм исходной кривой на некоторую кривую над меньшим по мощности полем.

Получен результат, описывающий ядро спуска Вейля [25]. Метод спуска Вейля в случае поля K характеристики 2 заключается в построении гомоморфизма ϕ из группы точек $E(K)$ эллиптической кривой E

$$y^2 + xy + x^3 + \alpha x^2 + \beta = 0, \alpha, \beta \in K, \tag{12}$$

над большим полем $K = GF(2^{nr})$ в группу классов дивизоров некоторой гиперэллиптической кривой над относительно меньшим подполем $k = GF(2^r)$ поля K.

А именно, ϕ индуцировано композицией следующих замен переменных:

$$x = 1/f(u); \quad y = \sqrt{\beta} + \frac{v}{f^2(u)} \tag{13}$$

для некоторого многочлена $f(u) = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i u^{2^i}, \lambda_i \in K; \lambda_0 \neq 0, \lambda_{m-1} \neq 0$. В новых координатах (см. [25, §2, гл.1, часть 1]) кривая E будет иметь вид

$$v^2 + f(u)v + h(u) = 0, \tag{14}$$

где $h(u) = f(u) + \alpha f(u)^2 + \sqrt{\beta} f(u)^3$.

Сделаем следующую замену переменных:

$$\begin{cases} \widetilde{u} = \lambda_0 u + \lambda'' \\ \widetilde{v} = v + g(\widetilde{u})t(\widetilde{u}), \end{cases}$$

где $g(\widetilde{u}) = f(\frac{\widetilde{u}-\lambda''}{\lambda_0})$, а $\lambda'' \in K$ выбрано так, что $g(\widetilde{u}) \in k[\widetilde{u}]$,

$$t(\widetilde{u}) = Tr_{K/k}\left(\frac{v}{g(\widetilde{u})}\right) + \frac{v}{g(\widetilde{u})}.$$

В новых переменных кривая (14) запишется следующим уравнением над k:

$$\widetilde{v}^2 + g(\widetilde{u})\widetilde{v} + g(\widetilde{u})(1 + ag(\widetilde{u}) + bg(\widetilde{u})^2) = 0, \text{где } a, b \in k. \tag{15}$$

Теорема 12 ([25]) *Пусть n - нечётное число и род кривой (15) не равен $2^{m-1} - 1$ (в этом случае он равен 2^m). Тогда для построенного методом спуска Вейля гомоморфизма ϕ выполнено:*

$P(0, \sqrt{\beta}) \notin Ker\phi$ и степени вхождения двойки в порядки точек кривой E и их образов совпадают.

С точки зрения практики, данная теорема подтверждает эффективность применения спуска Вейля для решения задачи дискретного логарифмирования на эллиптических кривых над полем характеристики 2. Помимо упрощения арифметики, связанным с переходом в меньшее поле, мы можем применять на гиперэллиптической кривой алгоритм с факторной базой, который имеет субэкспоненциальную сложность. Таким образом, использование полей большой простой характеристики предпочтительнее. Результатов о характеристиках ядра спуска Вейля раньше не было.

В шестой главе диссертации получен новый блочный алгоритм решения больших разреженных систем линейных уравнений над полем из двух элементов [8, 29, 9, 31, 11, 10]. В результате исследований получено несколько различных версий этого алгоритма. Показана эффективность предлагаемого нового метода по сравнению с известными алгоритмами Монтгомери и Видемана-Копперсмита.

Задача решения больших разреженных систем линейных уравнений над полем из двух элементов возникает, в частности, как этап в алгоритме факторизации целых рациональных чисел методом квадратичного решета или решета числового поля. Задача факторизации целых чисел возникает, в частности, при атаке на схему RSA.

Алгоритм Видемана-Копперсмита работает с произвольной исходной матрицей линейной системы. Алгоритм Монтгомери, также как и предлагаемый новый алгоритм, работает с симметричной матрицей исходной системы. Однако общий случай сводится к случаю симметричной матрицы.

Пусть $N, M \in \mathbb{N}$, и требуется найти нетривиальное решение системы линейных однородных уравнений вида

$$DX = 0, D \in \mathbb{F}^{M\times N}, X \in \mathbb{F}^{N\times n}, M < N, \tag{16}$$

где n – так называемый блочный параметр, обычно равный длине машинного слова, 32 или 64, или кратный этой длине.

Выберем случайно блок $Y \in \mathbb{F}^{N\times n}$ и рассмотрим систему

$$AX = B, A \in \mathbb{F}^{N\times N}, B, X \in \mathbb{F}^{N\times n}, \tag{17}$$

где $A = D^T D \in \mathbb{F}^{N\times N}$, в этих условиях вырожденная симметричная матрица. $B = AY$. Заметим, что любое решение X_D системы (16) позволяет построить X_A - решение системы (17) по формуле

$$X_A = X_D + Y.$$

Обратно, если есть X_A - решение системы (17), то $D^T D(X_A - Y) = 0$. Если $rangD = M$, то из полученного равенства находим, что $D(X_A - Y) = 0$. То есть, $X_A - Y$ - решение системы (16).

Обозначим $dim_{(16)}X$ размерность пространства, полученого в пересечении пространства $\langle X\rangle$, образованного столбцами произвольного блока X, с ядром линейного оператора D. Обозначим $dim_{(17)}X$ размерность пространства, полученого в пересечении пространства, образованного столбцами блока X, с ядром линейного оператора $A = D^T D$, а $dim'_{(17)}X$ - размерность пространства, полученого в пересечении пространства, образованного столбцами блока X, с ядром линейного оператора $A' = DD^T$.

Теорема 13 ([9]) *В приведённых обозначениях*

$$1) dim_{(16)}X \geq dim_{(17)}X - (M - rangD),$$

$$2) dim_{(16)}D^T X \geq dim'_{(17)}X - (M - rangD).$$

Пусть теперь требуется решить симметричную систему линейных уравнений:

$$Ax = B, A \in \mathbb{F}^{N\times N}, B \in \mathbb{F}^{N\times n}, \tag{18}$$

где A — симметричная матрица, а $\mathbb{F} = GF(2)$ — поле из двух элементов. Пусть n — длина машинного слова (32, 64 или 128), а d — оценка сверху на число ненулевых элементов в каждой строке матрицы A (плотность марицы).

Во всех рассматриваемых методах решения разреженных систем само решение ищется в пространстве Крылова $\langle B, AB, A^2B, \dots\rangle$. Предлагаемый алгоритм использует следующую теорему

Теорема 14 ([9]) *Пусть пространство Крылова $\langle W\rangle$ (здесь W – это конкатенация столбцов блоков $B, AB, A^2B, \dots$) построено в виде суммы непересекающихся A-ортогональных пространств $\langle W_i\rangle, i = 0, 1, \dots, m$ с начальным блоком вида $W_0 = B = AY$, на первых m из которых A-скалярное произведение невырождено. Пусть $\langle W_m\rangle$ A-ортогонально всему $\langle W\rangle$. Пусть вычислено AW_m и X вида*

$$X = \sum_{i=0}^{m-1} W_i ({W_i}^T A W_i)^{-1} {W_i}^T B, \tag{19}$$

$dim\langle W_m\rangle = \mu > 0$.

Тогда не более чем за $2\frac{(n+\mu-1)(n+\mu)}{2}N$ *битовых операций с вероятностью не меньше* $1 - \frac{1}{2^n}$ *(при условии статистической независимости* $\langle Y\rangle$ *и* $\langle W\rangle$*) может быть вычислено решение системы (18).*

Алгоритм Монтгомери, изложенный в его работе 1995 года, фактически, использует это утверждение без формулировки и доказательства.

Суть предлагаемого метода состоит в последовательном построении приближений Паде к некоторому ряду, коэффициенты которого зависят от матрицы линейной системы и блока векторов, стоящего в её правой части. Из этих приближений получаются блоки W_i, о которых шла речь в предыдущей теореме.

Предложенный в [8] алгоритм впервые дал рекуррентные формулы для построения приближений Паде к матричному ряду. Отметим также, что эти теоремы применимы не только к кольцу матриц, но и к другим некоммутативным кольцам, в которых недоопределённая система имеет невырожденное решение.

Определим [8] A-скалярное произведение двух матричных многочленов $(\varphi(\lambda), \psi(\lambda)) \in \mathbb{F}^{n\times n}$ как коэффициент при λ^{-1} в произведении $\varphi(\lambda)^T\alpha\psi(\lambda)$. Обозначим $(C, D) = C^TAD \in \mathbb{F}^{n\times n}$ матрицу попарных A-скалярных произведений вектор-столбцов матриц $C, D \in \mathbb{F}^{N\times n}$. Из этого определения и симметричности матрицы A следует, в частности, что $(C, D) = (D, C)^T$.

Далее из матричных приближений Паде строятся A-ортогональные блоки, образующие пространство Крылова. Это делается при помощи формулы:

$$Q^{(s)}(A, B) = \sum_{i=0}^{s} A^iBQ_i^{(s)} \tag{20}$$

с использованием следующей далее леммы

Лемма 1 ([27, 8]) *Пусть* $\alpha_i = B^TA^iB$, *тогда* $(\varphi(A, B), \psi(A, B)) = (\varphi(\lambda), \psi(\lambda))$.

Формула (20) является линейной по Q и B, а также удовлетворяет свойству

$$(\varphi(\lambda)\cdot\psi(\lambda))(A, B) = \psi(A, \varphi(A, B)). \tag{21}$$

Эта формула позволяет сократить до константы степень используемых в алгоритме многочленов, что приводит к существенной экономии вычислительных ресурсов.

Предложенный метод построения приближений Паде оптимизирован для удобства программирования.

Для получения линейной по размеру матрицы оценки сложности построения всех необходимых матричных приближений Паде предложена процедура синхронизации.

Суть её состоит в том, что после k-ого шага вычисление блочных векторов $A^iB, i = 0, 1, \ldots, k$ заменяется на вычисление блочных векторов вида

$$A^iQ^{(k)}(A, B), A^iQ^{(k-1)}(A, B), i = 0, 1, \ldots,$$

Очередные приближения Паде строятся как линейные комбинации приближений $Q^{(k)}(\lambda), Q^{(k-1)}(\lambda)$ с коэффициентами, являющимися многочленами ограниченной степени,

откуда и получается линейный характер оценки сложности их построения. Необходимая для этого построения оперативная память даже меньше, чем для хранения исходной матрицы.

Основными операциями рассматриваемого алгоритма являются: умножение разреженной матрицы из $\mathbb{F}^{N\times N}$ на блочный вектор из $\mathbb{F}^{N\times n}$, умножение блочных векторов друг на друга (скалярное произведение), умножение блочных векторов на матрицы из $\mathbb{F}^{n\times n}$ (линейная комбинация).Рассмотрим две последние операции. Согласно статье Монтгомери 1995 года, сложность этих операций оценивается величиной $O(nN)$ операций с машинными словами. Однако для более быстрой реализации этих операций можно применить хорошо известный алгоритм "четырёх русских", дающий, как мы покажем ниже, для умножения блока на маленькую матрицу существенно меньшее время.

Копперсмит для умножения блока на маленькую матрицу предложил фактически тот же алгоритм, что и алгоритм "четырёх русских", а для умножения блоков друг на друга - новый алгоритм.

Выбором оптимальных параметров в настоящей работе для этих алгоритмов получены следующие оценки

Лемма 2 ([31]) *Сложность вычисления скалярного произведения не более* $3\frac{nN}{log_2\frac{N}{2}-log_2log_2\frac{N}{2}}$, *а сложность вычисления линейной комбинации не более* $2\frac{nN}{log_2\frac{N}{2}}$.

Эти оценки приводят к тому, что рассматриваемые операции не влияют в общем случае на коэффициент при главном члене в оценке сложности всего алгоритма решения разреженной системы методом типа Ланцоша, хотя и близки при конкретных значениях параметров.

Получены результаты, учитывающие время на обмен между вычислительными узлами. Определим константу c следующим образом. Пусть время выполнения одной арифметической операции с машинными словами, умноженное на некоторую константу c, равно времени передачи одного машинного слова между вычислительными узлами. В современной компьютерной технике обмен между оперативной памятью и процессором осуществляется с $c \approx 5$, а между отдельными частями оперативной памяти: $c \approx 20$.

Теорема 15 ([10, 31]) *Оценка времени работы параллельной реализации с использованием блочного фактора алгоритма Видемана-Копперсмита с матричным умножением (с построением базиса всех приближений "по дереву") при* $N \geq 2^{26}$ *и*

$$N > \frac{71log_2(32N)log_2(4N)}{cn}\left(\frac{240log_2(log_2(32N))log_2(\frac{60}{17n}log_2(log_2(32N)))}{17}\right)^4$$

имеет вид

$$94N^{1+\frac{3}{4}}n^{-\frac{1}{4}}c^{\frac{3}{4}}(log_2(32N)log_2(4N))^{\frac{1}{4}}.$$

С помощью алгоритма Видемана-Копперсмита, который был модифицирован Томэ, 12 декабря 2009 года был установлен рекорд целой факторизации чисел RSA. Асимптотическая оценка времени работы этой версии из статьи Томэ 2007 года с учётом распараллеливания умножения разреженной матрицы на блочный вектор:

$$O(N^{1+\frac{2}{3}}(logNloglogN)^{\frac{1}{3}}).$$

В реальных вычислениях 2009 года эта величина оказалась равной 120 суткам. Пиковое использование оперативной памяти 1 ТВ.

Предлагаемые в диссертации алгоритмы построены с использованием блочных аппроксимаций Паде. Преимуществом этих алгоритмов по сравнению с алгоритмом Монтгомери 1995 года является более простая процедура вычисления скалярных произведений V^TAV без участия блоков из пространства Крылова. В алгоритме Монтгомери эту операцию труднее всего распараллелить. Её упрощение приводит к лучшим параллельным свойствам всего алгоритма и, в конце концов, к тому, что время работы сокращается практически до естественной границы — времени на построение пространства Крылова.

Проведённый анализ производительности соответствующих программ [31] показал лучшие параллельные свойства алгоритма, построенного на основе приближений Паде (оптимизированный алгоритм), по сравнению с существовавшими до этого программными реализациями других аналогичных алгоритмов. Это означает лучшую эффективность использования дополнительных вычислительных узлов.

Проведённый ИВМ РАН (с.н.с. Замарашкин Н.Л.) анализ производительности соответствующих программ [31] показал лучшие параллельные свойства алгоритма, построенного на основе приближений Паде, по сравнению с существовавшими до этого программными реализациями других аналогичных алгоритмов. Это означает, что можно эффективно использовать значительно больше дополнительных вычислительных узлов, существенно сокращая общее время работы программы.

Там же отмечено, что важным свойством предложенного подхода является то, что между "синхронизациями" можно считать коэффициенты ряда на не связанных между собой вычислителях. Наличие "синхронизации" позволяет избежать роста необходимой оперативной памяти в процессе работы алгоритма. Это обстоятельство делает предлагаемый алгоритм принципиально лучше, чем алгоритм Видемана-Копперсмита, и может позволить в будущем совсем отказаться от использования кластера при решении больших разреженных систем, ограничившись связанными в сети Интернет вычислителями, оперативная память которых может вместить матрицу исходной линейной системы. Связывающие их каналы должны допускать обмен, который проводится 200 раз за весь алгоритм, при размере матрицы порядка $2 \cdot 10^8$. Современная динамика развития компьютерной техники показывает, что через 3-4 года таким требованиям будут удовлетворять персональные компьютеры, связанные сетью Интернет. Это значит, что для решения разреженных систем может быть привлечена вычислительная мощность, на несколько порядков превышающая мощность кластеров.

Предлагаемый алгоритм имеет дополнительный параметр (в тексте обозначен k), который позволяет управлять распараллеливанием. А именно, можно вручную задавать количество обменов между узлами, независимо вычисляющими свои части исходного ряда. Тем самым заключительный этап, требующий применения кластера с большой оперативной памятью, дробиться на k_1 этапов, обрабатывающих многочлены в k_1 раз меньшей степени. При этом k_1 раз приходится пересчитывать образующие. Оптимальное значение параметра k_1 выбирается в соответствии с пропускной способностью общей сети. Общее время работы программы будет подчиняться следующей зависимости:

$$k_1 L + \frac{c_1 N^2}{k_1},$$

где L - сложность решения задачи на кластере, c_1 - коэффициент, связанный с пропускной

способностью внешней сети. Арифметические вычисления показывают для матрицы порядка $2 \cdot 10^8$ и сети 1Гбит/сек время порядка 6 суток. Для сети 100Мбит/сек - 15 суток.

Для удобства читателя сгруппируем лучшие верхние оценки для разных алгоритмов при работе на одном кластере в таблицу

	Время
Wiedemann-Coppersmith with matrix polynomial multiplication	$94N^{1+\frac{3}{4}}n^{-\frac{1}{4}}c^{\frac{3}{4}}$ $((log_2 32N)(log_2 4N))^{\frac{1}{4}}$
Wiedemann-Coppersmith-Thomé	$O(N^{1+\frac{2}{3}}(log_2 N log_2 log_2 N)^{\frac{1}{3}})$
Montgomery (1995) Алгоритм-K	$\frac{2c}{n}N^2$

Здесь n - длина машинного слова, а c — описанный выше коэффициент запаздывания передачи машинного слова по сравнению с производством одной операции с машинными словами. Число узлов выбрано так, чтобы минимизировать время работы соответствующего алгоритма.

Эти оценки хорошо согласуются с результатами, полученными в ходе практической реализации нового алгоритма [31]. В рассмотренных диапазонах время сокращалось близко к обратно пропорциональной зависимости от числа используемых вычислительных узлов, что является наилучшим показателем эффективности распараллеливания [31](Таблицы 14, 15).

Приведём результаты численных экспериментов, проведённых в ИВМ РАН для матрицы «m512t» размером $5,5 \cdot 10^6$ и плотностью 51 на кластере Академии наук в одинаковых условиях.

Метод Монтгомери («m512t», МВС-1000, программа "Алгоритм-K"): 45 часов.

Первая версия предложенного метода («m512t», МВС-1000): 17 часов.

Реализованная первая версия была запрограммирована с отклонениями от оптимальной версии алгоритма для упрощения программирования. Показано, что программа, реализующая оптимальную версию нового алгоритма, будет работать примерно 8 часов столько же сколько и новейшая версия алгоритма Монтгомери с блочным фактором. При этом замеры времени показали, что ресурс использования параллельных вычислений для нового алгоритма выше, чем для алгоритма Монтгомери.

Суммируем преимущества предлагаемого алгоритма.

По сравнению с алгоритмом Монтгомери:

- Возможно распараллеливание высокого уровня (как в алгоритме Видемана-Копперсмита). Можно вести речь о решении в Интернете на вычислителях, память которых вмещает только саму задачу.

- Линейные комбинации, скалярные произведения, умножения на разреженную матрицу не чередуются, а группируются.
- Точка насыщения больше, чем для Монтгомери с блочным фактором. Меньше линейных комбинаций в 1,5 раза.

По сравнению с алгоритмом Видемана-Копперсмита:

- Требуемая память не растёт в процессе работы ("синхронизация" приводит к тому, что степень приближений не растёт). Есть возможность исключить использование кластера.
- Трудоёмкость меньше (отсутствует логарифмический множитель в главном члене асимптотики).
- Проще анализ вероятности срабатывания.

Вот результаты замеров времени работы различных программ на 400 и 900 вычислительных узлах современных кластеров.

Алгоритм	400, МВС-1000 $(5,5 \cdot 10^6)$	400, Ломоносов $(33 \cdot 10^6)$	900, Ломоносов $(33 \cdot 10^6)$
P.Montgomery, Алгоритм-К	**45 часов**	-	-
P.Montgomery, J.Papadopulos	-	**80 часов**	-
P.Montgomery, J.Papadopulos, И.А.Поповян, Ю.В.Нестеренко	-	-	**54 часа**
М.А.Черепнёв, Н.Л.Замарашкин	**8 часов**	*9,4 часов*	*6,27 часа*

Наклонным шрифтом указано время, рассчитанное (эксперимент не проводился) исходя из того, что при фиксированном числе вычислительных узлов время растет не быстрее, чем N^2, а увеличение в k раз числа используемых вычислительных узлов даёт уменьшение времени как минимум в $\sqrt{k}$ раз. Кроме того, узлы "Ломоносова"в 36,8 раз мощнее узлов МВС-1000 (99,5 Гфлопс против 2,7 Гфлопс), отношение соответствующих констант c примерно равно $1,8$, а $\sqrt{2,25} = 1,5$.

Отметим, что предложенный подход позволил сконструировать целую серию алгоритмов, которые имеют преимущества перед известными алгоритмами в случае использования вычислителя специфической структуры и мощности. Возможны и дальнейшие упрощения предложенной процедуры вычисления последовательных приближений Паде, что повлияет на сокращение времени работы всего алгоритма.

Кроме того, с теоретической точки зрения изложенный подход связывает между собой алгоритмы, основанные на ортогонализации пространства Крылова, и алгоритмы, основанные на поиске соотношения для рекуррентной последовательности. Давно замечено, что реализации этих подходов имеют практически одинаковую эффективность. Изложенный подход позволяет понять теоретические причины этого явления и использовать преимущества обоих методов.

Разработанный в диссертации алгоритм решения больших разреженных систем линейных однородных уравнений над $GF(2)$, который можно использовать для атаки на схему RSA, применён в ОАО "Концерн "Автоматика" при анализе систем защиты информации (получены новые параметры безопасности) о чем имеется акт внедрения.

В заключении шестой главы предложены две модификации алгоритма Видемана-Копперсмита, показывающие связь между этим алгоритмом и алгоритмом Монтгомери. Изменения коснулись той части алгоритма, где необходимо использовать кластер с большой оперативной памятью. Первым описан вариант с полной заменой техники построения матричных приближений, предложенной Копперсмитом, на алгоритм построения приближений Паде для рядов по отрицательным степеням, разработанный автором диссертации.

Во втором варианте исходная техника Копперсмита дополнена анализом скалярных произведений получаемых приближений [12]. Для получения решающего преимущества этот вариант необходимо дополнить процедурой "синхронизации". Построенный таким способом алгоритм будет обладать дополнительными преимуществами по сравнению с описанным в этой работе оптимизированным алгоритмом. Это является следствием того, что построение приближений к рядам по положительным степеням несколько проще.

Идеи шестой главы могут быть применены и к обобщению других матричных алгоритмов на случай кольца коэффициентов [18].

В седьмой главе разработанная техника перенесена на случай большого простого поля [32, 14, 15, 33]. Такая задача является ядром алгоритма дискретного логарифмирования с факторной базой.

Разработан способ параллельных вычислений на системе с s узлами, для которой параллельная сложность (без пересылок) примет вид [32]

$$\mathcal{O}\left(\frac{dN^2}{s}+\frac{N^2}{q}+Ns\right), \tag{22}$$

где q - параметр алгоритма, а число пересылок линейно зависит от q. Этот результат получен в соавторстве с Н.Л.Замарашкиным. Конструкция использования приближений Паде и идея синхронизации, реализованные в виде формул, принадлежат М.А.Черепневу, а идея использования малой вероятности вырождения матриц над большим простым полем и упрощение алгоритма в этом случае принадлежат Н.Л.Замарашкину.

Апробация работы.

Результаты работы неоднократно обсуждались на следующих

кафедрах МГУ им. М.В.Ломоносова:

— Теории чисел механико-математического факультета,

— Алгебры механико-математического факультета,

— Вычислительной математики механико-математического факультета,

— Математического анализа механико-математического факультета,

— Дискретной математики механико-математического факультета,

— Оптимального управления механико-математического факультета,

— Математической кибернетики факультета вычислительной математики и кибернетики,

в других организациях:

— в лаборатории по математическим проблемам криптографии МГУ имени М.В.Ломоносова,

— на кафедре компьютерного и математического моделирования Института математики, физики и информатики Тамбовского государственного университета им. Г.Р.Державина,
— в Академи криптографии РФ,
— в в.ч. 43753,
— в ФИЦ ИУ РАН,
— в ОАО "Концерн "Автоматика",
— в НПО "Квант",
— в Институте вычислительной математики РАН,
— в Математическом институте им. В.А.Стеклова РАН,
— в Институте проблем информатики РАН
— в Институте проблем информационной безопасности МГУ имени М.В.Ломоносова
на конференциях:
— Математика и безопасность информационных технологий (2003, 2004, 2007, 2008, Москва),
— Проблемы теоретической кибернетики (1999, Нижний Новгород; 2002, Казань),
— Ломоносовские чтения (2005, 2008, Москва),
— 12-th workshop on computer algebra (2008, Дубна),
— Applications of Computer Algebra (2008, Austria),
— Колмогоровские чтения (2009, Тамбов),
— Parallel Computer Algebra (2010, Тамбов),
— "Russian supercomputing days" (2015г. Москва).

Получены: Патент РФ на изобретение [7], два государственных свидетельства на регистрацию программного обеспечения [16, 17], акты внедрения результатов исследования от ОАО "Концерн "Автоматика" и в.ч. 43753.

Заключение

В диссертации разработан ряд новых алгоритмов существенно упрощающих задачи дискретного логарифмирования и факторизации и некоторых смежных задач, а также получены новые характеристики существующих алгоритмов.

В первой главе доказана полиномиальная эквивалентность сертифицированной задачи дискретного логарифмирования и задачи Диффи-Хеллмэна при применении алгоритмов, использующих операции не сложнее групповой и работающих в исходной группе и связанных с нею по дереву Пратта группах, в случае, когда растущий порядок исходной группы имеет дерево Пратта с ограниченными длинами ветвей. В общем случае, получена формула, связывающая сложности этих задач. Предложенный в данной главе подход применён к анализу стойкости Российского стандарта цифровой подписи ГОСТ Р 34.10-2012 эллиптических кривых. Показано, что в случае, когда $p-1$ "хорошо"раскладывается на простые множители, задачи дискретного логарифмирования и Диффи-Хеллмэна в группе простого порядка p, на стандартных эллиптических кривых, полиномиально эквивалентны. Предложено несколько подходов и алгоритмов решения задачи дискретного логарифмирования на стандартных эллиптических кривых. Данные результы могут свидетельствать о слабости действующего стандарта эллиптических кривых. Предложены способы его усовершенствования.

Во второй главе получены оценки на величину и количество простых делителей чисел вида $p-1$, которые характеризуют дерево Пратта и могут быть применены к описанным атакам на ГОСТ Р 34.10-2012, а также к атакам на его старую версию: ГОСТ Р 34.10-94, которые представлены в четвёртой главе.

В третьей главе проанализированы наиболее распространённые в алгебре некоммутативные операции на предмет применения их в схеме открытого распределения ключей В.М.Сидельникова. Построены полиномиальные алгоритмы решения задачи факторизации относительно рассматриваемых операций. Тем самым доказана нестойкость рассматриваемой схемы при использовании этих операций. Предложена новая некоммутативная операция с использованием символов степенного вычета, стойкая относительно рассмотренных атак.

В четвёртой главе предложена атака на старый стандарт цифровой подписи ГОСТ Р 34.10-1994. Универсальная подделка подписи в этом стандарте сведена к решению сравнения $x = R^x \mod p)$ относительно $x \in \{0, \ldots, p-1\}$. Получены новые оценки на число решений этого сравнения относительно пар (R, x). Доказательства оценок конструктивные, то есть позволяют строить указанные пары вероятностным полиномиальным алгоритмом. Это делается при помощи построения первообразных корней $\mod p)$, наименьший положительный вычет которых взаимно прост с $p-1$. В некоторых случаях получены точные формулы, выражающие такие пары. Отметим здесь, что ГОСТ Р 34.10-1994 являлся основой для формирования последующих стандартов ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, для которых рассматриваемое сравнение модифицируется с использованием операции сложения точек на эллиптической кривой и может быть подвергнуто аналогичному анализу.

Пятая глава посвящена исследованию алгоритма спуска Вейля для решения задачи дискретного логарифмирования в группе точек элиптической кривой. Изучены свойства представления Мамфорда дивизоров гиперэллиптических кривых. При помощи этого представления доказана теорема, характеризующая ядро спуска Вейля при использовании полей характеристики 2. Эта теорема выделяет случай, в котором образ гомоморфизма, называемого спуском Вейля, является нетривиальным и даже содержит ту же степень двойки, что и прообраз. Поэтому спуск Вейля может быть эффективно применён для решения задачи дискретного логарифмирования на гиперэллиптических кривых над полем характеристики 2.

В шестой главе получены новые блочные алгоритмы решения больших разреженных систем линейных уравнений. Предложенные новые алгоритмы последовательного построения приближений Паде к произвольным формальным рядам по отрицательным и положительным степеням формальной переменной с матричными коэффициентами применены к построению ортогонального базиса пространства Крылова и решению соответствующей системы линейных уравнений. Идея использования блочных приближений для построения базиса пространства Крылова высказана и реализована впервые. Указанные алгоритмы демонстрируют возможность одновременного использования полезных свойств известных алгоритмов, основанных отдельно на последовательной ортогонализации пространства Крылова (алгоритм Монтгомери) и на построении приближений формальных рядов с матричными коэффициентами (алгоритм Видемана-Копперсмита). Данный подход имеет хорошие параллельные свойства, позволяющие отказаться от использования большого кластера при решении больших разреженных систем линейных уравнений. Поэтому, при анализе стойкости систем защиты информации, основанных на сложности задачи факторизации целых чисел, надо учитывать возможность применения нового метода на больших вычислительных ресурсах, связанных медленными каналами (Интернет).

Программа, реализующая алгоритм из шестой главы, которую можно использовать для атаки на схему RSA, внедрена в ОАО "Концерн "Автоматика", о чем имеется акт внедрения.

В седьмой главе техника 6 главы перенесена на случай большого конечного поля. Полученный алгоритм решения разреженных линейных систем над таким полем может быть применён к решению задачи дискретного логарифмирования в конечном поле.

Публикации автора по теме диссертации

[Публикации из списка ВАК:]

[1] Сидельников В.М., Черепнёв М.А., Ященко 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-Хеллмэна.// Дискретная математика.-1996.-т.8-вып.3-с.22-30.

[3] Черепнев М.А. Схемы открытого распределения ключей на основе некоммутативной группы.// Дискретная математика.-2003.-т.15-вып.2-с.47-51.

[4] Панфилов Б.А., Черепнёв М.А., Панфилов Ю.Б. Электронные замки на основе смешанной системы счисления, реализованной с помощью резистивной матрицы памяти на базе полярнозависимого электромассопереноса в кремнии.// Радиотехника и электроника.-2005.-т.50-№12-с.1523-1527.

[5] Черепнёв М.А. Некоторые свойства больших простых делителей чисел вида $p-1$.// Математические заметки-2006.-80:6- p.920-925

[6] Панфилов Б.А., Черепнев М.А. Симметричная криптосистема шифрования на основе смешанной системы счисления.// Радиотехника и электроника.-2008.-т.53-№10-с.1314-1316.

[7] Патент на изобретение №2358082. Способ создания электронного кодового устройства повышенной криптографической стойкости (варианты)/Панфилов Б.А., Черепнёв М.А., Панфилов Ю.Б. заявка №2006123305, от 10.06.2009.;Приоритет 30.06.2006; Срок действия 30.06.2026

[8] Черепнев М.А. Блочный алгоритм типа Ланцоша решения разреженных систем линейных уравнений.// Дискретная Математика-2008.-т.20-вып.1-с.145-150.

[9] 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.

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

[11] Cherepniov 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)

[12] 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 (Фундаментальная и прикладная математика): -Volume 193, -Issue 4 (2013), -p.622-630.

[13] Черепнёв М.А. Обращение спариваний для решения задачи дискретного логарифмирования. Фундаментальная и прикладная математика, 2013, Т.18, Вып.4, стр.185-195. Journal of Mathematical Science: Volume 206, Issue 6 (2015), page 734-741.

[14] Черепнёв М.А. Замечание о ядре группового гомоморфизма метода спуска Вейля. Фундаментальная и прикладная математика 2014, Т.19, Вып.6, стр. 211-222. Journal of Mathematical Sciences, Vol. 221, No. 3, March, 2017 p. 452-460

[15] Черепнев М.А., Замарашкин Н.Л. Универсальный блочный метод Ланцоша-Паде для систем линейных уравнений над большими простыми полями. Фундаментальная и прикладная математика 2014, Т.19, Вып.6, стр. 223-247. Journal of Mathematical Sciences, Vol. 221, No. 3, March, 2017 p. 461-478.

[16] BFFblockLanzosPade свидетельство о регистрации прав на ПО. Авторы: Замарашкин Н.Л., Черепнев М.А., Желтков Д.А., Салуев Т.Г.,Тыртышников Е.Е. Номер: 2015662444. Дата получения: 24 ноября 2015 г.Описание: Параллельный алгоритм для решения линейных систем над большим простым полем - блочный вариант алгоритма Ланцоша-Паде.

[17] GF2blockLanzosPade свидетельство о регистрации прав на ПО. Авторы: Замарашкин Н.Л., Черепнев М.А., Желтков Д.А., Салуев Т.Г.,Тыртышников Е.Е. Номер: 2015662694. Дата получения: 30 ноября 2015 г. Описание: Параллельный блочный метода Ланцоша-Паде для систем линейных алгебраичеких уравнений над полем GF(2).

[18] Черепнев М.А. Обобщение алгоритма Риссанена на блочно-ганкелевы матрицы. Дискретная математика, Т.28, вып.1, 2016 с.150-155.

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

[**Другие публикации:**]

[20] Черепнёв М.А. О некотором свойстве дискретного логарифма.// Тез. докл. XII международной конференции «Проблемы теоретической кибернетики», Нижний новгород.-1999.-с.246.

[21] Черепнёв М.А. Схемы открытого распределения ключей на основе некоммутативной операции.// Тез. докл. Тез. докл. XIII международной конференции "Проблемы теоретической кибернетики Казань.-2002.-с.190.

[22] Исследования класса математических алгоритмов на эллиптических кривых в целях обеспечения достоверности документов и идентификации отправителей в системе межведомственного электронного документооборота. Отчёт о НИР (заключит.)/МГУ; Руководитель Ю.В.Нестеренко; Черепнёв М.А., Поповян И.А., Назаров В.В., Герман О.Н.-Шифр темы "Локон-А"ГР № 02/243.-М.,2002.-177с.

[23] Черепнёв М.А. Некоторые свойства больших простых делителей чисел вида $p-1$.// Материалы конференции МаБИТ 2003.-2003.-с.218-220.

[24] Черепнёв М.А. О величине простых делителей чисел вида $p-1$.//Материалы конференции МаБИТ 2004.-2004.-с.243-246.

[25] Исследования класса математических алгоритмов на эллиптических кривых в целях обеспечения достоверности документов и идентификации отправителей в системе межведомственного электронного документооборота. Отчёт о НИР (заключит.)/МГУ; Руководитель Ю.В.Нестеренко; Черепнёв М.А., Поповян И.А., Назаров В.В., Герман О.Н.-Шифр темы "Локон-Б"ГР № 2/15-40.-М.,2004.

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

[27] 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.

[28] 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.

[29] Черепнев М.А. Алгоритмы построения матричных приближений Паде.// Материалы Четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ 30-31.10.2008 (МаБИТ-2008)-М.:МЦНМО,2009.-с.21-22.

[30] Гашков С.Б., Применко Э.А., Черепнев М.А. Криптографические методы защиты информации. Учебное пособие-М.:Академия.-2010.-298с.

[31] Исследование проблем теории чисел и алгебраической геометрии, связанных с анализом и синтезом шифрсистем : Отчет о НИР (заключит.)/Академия криптографии; Руководитель М.М.Глухов; М.А.Черепнев, Н.Л.Замарашкин и др.- Шифр темы "Идеал-3"; ГР №239-09.-М., 2010.-42с.

[32] Федеральная целевая программа "Универсальный метод решения линейных систем над конечным полем на экзофлопных вычислителях"/ ИВМ РАН, Руководитель Тыртышников Е.Е.; Черепнев М.А., Замарашкин Н.Л. и др. ГР № 2014-14-576-0054, 2014г. -91с.

[33] Черепнев М.А., Замарашкин Н.Л. Универсальный блочный метод Ланцоша-Паде для систем линейных уравнений над большими простыми полями. Труды международной конференции “Russian supercomputing days” (28-29 сентября 2015г. Москва), М., изд-во МГУ, стр. 509-520.