На правах рукописи

Бабенко Михаил Григорьевич

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, МЕТОДЫ И АЛГОРИТМЫ ОБРАБОТКИ ЗАШИФРОВАННЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ СРЕДАХ

Специальность 2.3.5 (05.13.11) —
Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
доктора физико-математических наук

Москва — 2022

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова Российской академии наук.

Научный консультант: Академик РАН, доктор физико-математических наук, Аветисян Арутюн Ишханович

Официальные оппоненты:

- Логачев Олег Алексеевич, доктор физико-математических наук, член-корр. Академии криптографии Российской Федерации, доцент кафедры информационной безопасности Факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский Государственный Университет имени М.В. Ломоносова»,
- Ильин Вячеслав Анатольевич, доктор физико-математических наук, главный научный сотрудник Курчатовского комплекса НБИКС-природоподобных технологий Федерального государственного бюджетного учреждения «Национальный исследовательский центр «Курчатовский институт»,
- Шабанов Борис Михайлович, доктор технических наук, доцент, директор Межведомственного Суперкомпьютерного Центра РАН, заместитель директора по научной работе Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук».

Ведущая организация: Объединенный институт ядерных исследований.

Защита состоится 08 декабря 2022 г. в 15 часов на заседании диссертационного совета 24.1.120.01 при Федеральном государственном бюджетном учреждении науки Институт системного программирования им. В.П. Иванникова РАН по адресу: 109004, г. Москва, ул. А. Солженицына, дом 25.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова РАН.

Автореферат разослан «__»_____ 2022 г.

Ученый секретарь
диссертационного совета 24.1.120.01,
кандидат физико-математических наук Зеленов С.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Облачные вычисления способны обеспечить значительные преимущества при организации удаленного распределенного хранения и обработки данных в виде доступности, масштабируемости, энергоэффективности, почти нулевых предварительных инвестиций в инфраструктуру, своевременного предоставления услуг и т.д. Однако, вместе с преимуществами возникают дополнительные проблемы, связанные с потерей, искажением, кражей данных. Аутсорсинг данных подразумевает делегирование прямого управления данными и их обработки, что увеличивает риски кражи информации в случае недобросовестного поведения провайдера облачных услуг.

Проблема надежности является критической для сохранения целостности и доступности данных в облачной среде. Разработка методов проектирования надежных сервисов, использующих распределенные системы обработки данных – важнейшее направление исследований в области аутсорсинга вычислений. Повышение эффективности необходимо для повышения качества облачных сервисов, но при этом не должно критически влиять на безопасность доверенных сервису данных. Стандартным подходом к обеспечению конфиденциальности данных является использование традиционных алгоритмов, основанных на гомоморфных вычислениях. Общая идея решения данной проблемы в контексте облачных вычислений состоит в том, чтобы делегировать обработку данных, не предоставляя к ним прозрачный доступ.

Гомоморфные вычисления, используемые, в частности, для полностью гомоморфного шифрования (Fully Homomorphic Encryption), способны решить описанную проблему. Гомоморфные вычисления позволяют третьей (возможно ненадежной) стороне обрабатывать информацию без раскрытия исходных данных. Гомоморфизм групп позволяет применять основные математические операции непосредственно к новой алгебраической структуре, сохраняя результаты данных операций с точностью до обратного гомоморфного преобразования. Другими словами, гомоморфные вычисления обеспечивают совместимость двух критических для аутсорсинга данных факторов: вычислений и конфиденциальности.

Основным ограничивающим фактором для построения безопасных и надежных систем обработки данных является высокая вычислительная сложность алгоритмов. Многочисленные попытки оптимизации существующих схем гомоморфных вычислений имели лишь незначительный успех и не решают указанную проблему. Требуется комплексный подход к уменьшению вычислительной сложности, включающий проработку всех этапов проектирования схемы обработки данных, начиная с построения модели, соответствующей требованиям, предъявляемым к современным распределенным вычислительным средам, включая возможность реализации механизмов обеспечения надежности и конфиденциальности обрабатываемых данных, и заканчивая разработкой эффек-

тивных алгоритмов реализации функционала схем обработки конфиденциальных данных.

Анализ современных систем распределенной обработки конфиденциальных данных, теоретических и практических исследований ведущих российских и зарубежных ученых позволяет сделать вывод, что на данный момент проблема снижения вычислительной сложности алгоритмов обработки данных остается открытой. Таким образом, научная проблема, на решение которой направлена данная работа, заключается в разработке фундаментальных основ для проектирования систем обработки и хранения конфиденциальных данных в гетерогенных средах. Для решения поставленной общей научной проблемы проведена ее декомпозиция на ряд частных задач:

- Разработка теории сравнения зашифрованных чисел и определения их знака над различными алгебраическими структурами.
- Модификация методов контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа.
- Разработка конфигурируемой масштабируемой двухуровневой структуры доступа на основе избыточной системы остаточных классов, допускающей реализацию гомоморфных вычислений и позволяющей осуществлять параллельную обработку данных с сохранением их конфиденциальности.
- Разработка алгоритма обнаружения и исправления ошибок в двухуровневой избыточной системе остаточных классов с использованием расстояния Хэмминга.

Существует множество перспективных теоретических решений, реализующих схемы гомоморфных вычислений, однако большинство из них ориентированы на использование единого сервиса хранения и обработки данных, что сильно ограничивает предоставляемые пользователю вычислительные возможности. Для расширения вычислительных возможностей, помимо оптимизации вычислительной сложности основных операций, предлагается программно объединить вычислительные возможности различных облачных сервисов в рамках парадигмы мультиоблачного хранения и обработки данных. Схема, реализующая мультиоблачный подход, должна обеспечивать надежность и конфиденциальность хранимых и обрабатываемых данных в условиях повышенной неопределенности, связанной с использованием различных облачных сервисов, каждый из которых характеризуется динамическим изменением основных свойств и параметров. Другими словами, с объединением ресурсов различных облачных сервисов объединяются и риски, связанные с потерей данных и утратой их конфиденциальности, характерные для каждого из них, что необходимо учитывать при построении мультиоблачных моделей распределенного хранения и обработки данных.

Успешные теоретические решения в области построения безопасных и надежных распределенных систем хранения и обработки данных предложи-

ли R.L. Rivest, T. Elgamal, A. Shamir, L. Adleman, C. Gentry, Z. Brakerski, V. Vaikuntanathan, A. Badawi, S. Halevi, A. Khedr, G. Gulak, И.Я. Акушский, В.М. Амербаев, Д.И. Юдицкий, Н.И. Червяков, А.Л. Стемпковский, А.А. Коляда, В.В. Князев, В.А. Торгашев, И.Т. Пак, Л.К. Бабенко и другие авторы.

Целью исследования является разработка теоретических основ, эффективных методов и алгоритмов определения знака числа, сравнения зашифрованных чисел, кодов обнаружения и исправления ошибок данных и арифметических операций, позволяющих повысить надежность хранения и эффективность обработки конфиденциальных данных в открытых распределенных средах.

Объектом исследования являются теория обеспечения надежности и конфиденциальности данных.

Предметом исследования выступают модели и методы распределенной обработки данных с использованием гомоморфных вычислений.

Методы исследования. При решении поставленных задач использовались методы теории чисел, теории алгоритмов, теории вероятностей и математической статистики, комбинаторики, арифметики конечных полей, нейросетевых моделей над кольцом вычетов, отказоустойчивого кодирования.

Научную новизну диссертации представляют следующие основные научные результаты и расширяющие существующий базис теории и практики обработки конфиденциальных данных в распределенных средах.

- Разработана теория построения многочленов наилучшего приближения функции определения знака числа, что улучшает и расширяет известные результаты.
- Предложен метод вычисления многочленов наилучшего приближения и решена задача об их количестве.
- Разработана теория сравнения зашифрованных чисел и определения их знака над кольцом с делителями нуля.
- Выделен класс монотонных функций ядра Акушского. Решена проблема возникновения критических ядер.
- Модифицированы методы контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа.
- Разработан метод обнаружения и исправления ошибок в двухуровневой системе остаточных классов (СОК) с использованием расстояния Хэмминга.
- Предложены оригинальные методы и алгоритмы повышения надежности и безопасности хранимых и обрабатываемых данных в распределенных средах.
- Построены многочлены, использующие интерполяционные многочлены Лагранжа, позволяющие определять знак числа и сравнивать числа над полем $\mathbb{Z}_m$, уточнены их степени.

- Предложена 2Lbp-RRNS конфигурируемая масштабируемая двухуровневая структура доступа на основе избыточной системе остаточных классов (ИСОК), допускающая реализацию гомоморфных вычислений и позволяющая осуществлять параллельную обработку данных с сохранением их конфиденциальности.
- Разработаны алгоритмы кодирования и декодирования данных в 2Lbp-RRNS для улучшения эффективности обработки данных в распределенных средах.

Практическая и теоретическая значимость. Работа носит теоретический характер. Полученные в ней результаты позволяют проектировать распределенные системы обработки конфиденциальных данных с использованием гомоморфных вычислений. Предложены новые модели построения подобных систем, а также эффективные реализации вычислительно сложных операций и алгоритмов кодирования, декодирования.

Применение вышеперечисленных результатов диссертационного исследования обеспечивает повышение эффективности систем распределенной обработки конфиденциальных данных в современных распределенных вычислительных системах.

Практическая и теоретическая значимость полученных результатов и вклад диссертанта в развитие соответствующей отрасли знаний подтверждается цитированием результатов в международных изданиях: 1181 ссылка в Google Scholar (h-index = 17), 568 ссылок в Scopus (h-index = 14).

Основные положения, выносимые на защиту:

- Теория сравнения зашифрованных чисел и определения их знака над различными алгебраическими структурами.
- Методы контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа.
- Алгоритм обнаружения и исправления ошибок в двухуровневой избыточной системе остаточных классов с использованием расстояния Хэмминга.
- Конфигурируемая масштабируемая двухуровневая структура доступа на основе избыточной системы остаточных классов, допускающая реализацию гомоморфных вычислений и позволяющая осуществлять параллельную обработку данных с сохранением их конфиденциальности.
- Комплекс программ, зарегистрированных в Роспатенте РФ.

Основные результаты диссертационного исследования были использованы в рамках следующих научно-технических работ:

Министерство науки и высшего образования Российской Федерации. «Исследование и разработка передовых методов защиты информации, сохранения конфиденциальности и предотвращения утечки данных при обработке данных в распределенных средах» (Проект 075-15-2020-788); «Северо-

Кавказский центр математических исследований» (Проект 075-02-2021-1749 и 075-02-2022-892); «Фундаментальные алгоритмы, технологии глубокого обучения и безопасности для облачного хранения и обработки данных» (Проект 075-15-2021-1010); «Разработка методов пространственного разделения и периодического обновления секрета на точках эллиптической кривой» (ФЦП, Проект: 14.B37.21.1128); «Разработка программного комплекса шифрования данных, на основе использования точек эллиптической кривой» (ФЦП, Проект: 07.P20.11.0029).

Российский научный фонд. «Эффективная, безопасная и отказоустойчивая система распределенного хранения и обработки конфиденциальных данных с регулируемой избыточностью для проектирования мобильных облаков на маломощных вычислительных устройствах» (Проект: 19-71-10033, 19-71-10033-П).

Российский фонд фундаментальных исследований. «Эффективная интеллектуальная система управления данными в краевых, туманных и облачных вычислениях с регулируемой отказоустойчивостью и безопасностью» (Проект: 20-37-51004 Научное наставничество); «Разработка методов и алгоритмов быстродействующего, отказоустойчивого математического сопроцессора для проектирования вычислительных систем с повышенным уровнем безопасности и низким энергопотреблением» (Проект: 20-37-70023 Стабильность); «Разработка новых отказоустойчивых мобильных систем связи с низким энергопотреблением на основе интеграции параллельной математики и искусственных нейронных сетей» (Проект: 18-07-00109-а); «Разработка и исследование концепции активной безопасности на точках эллиптической кривой» (Проект: 12-07-31087 мол_а).

Совет по грантам Президента Российской Федерации. «Безопасная и надежная распределенная система хранения больших данных с регулируемой избыточностью» (Проект: МК-341.2019.9); «Разработка методов и алгоритмов функционирования устройств для «Интернет вещей» с использование модулярной арифметики» (Проект: СП-1215.2016.5).

Разработан комплекс программ, позволяющий исследовать вопросы обеспечения безопасности и надежности хранимых и обрабатываемых данных в облаках в условиях неопределенности возникновения технических сбоев и различного рода хакерских атак, включающий в себя следующие компоненты: «Среда моделирования вычислений в системе остаточных классов на основе приближенных методов» (Свидетельство о государственной регистрации программы для ЭВМ № 2012610503 от 10.01.2012); «Ускоренный метод вычисления остатка от деления с использованием распределенной арифметики» (Свидетельство о государственной регистрации программы для ЭВМ № 2016612432 от 26.02.2016); «Программа управления устройством перевода чисел из системы остаточных классов в позиционную систему счисления на основе перевода в обобщенную позиционную систему счисления» (Свидетельство о государственной регистра-

ции программы для ЭВМ № 2016618312 от 26.07.2016); «Программа управления устройством перевода чисел из системы остаточных классов в позиционную систему счисления на основе Китайской теоремы об остатках с дробными числами» (Свидетельство о государственной регистрации программы для ЭВМ № 2016618315 от 26.07.2016); «Программа моделирования гомоморфного шифрования в облачных вычислениях» (Свидетельство о государственной регистрации программы для ЭВМ № 2017615372 от 15.05.2017); «Среда моделирования алгоритмов цифровой фильтрации изображений» (Свидетельство о государственной регистрации программы для ЭВМ № 2018612690 от 21.02.2018); «Модуль оценки рисков безопасности облачных, краевых и туманных вычислений в условиях вычислительной неопределенности» (Свидетельство о государственной регистрации программы для ЭВМ № 2018612694 от 21.02.2018); «Модуль кодирования и декодирования данных в системе остаточных классов» (Свидетельство о государственной регистрации программы для ЭВМ № 2019610808 от 18.01.2019); «Распределенная система надежного хранения и обработки данных в мультиоблачной среде» (Свидетельство о государственной регистрации программы для ЭВМ № 2019611375 от 24.01.2019); «Программный модуль деления с остатком чисел большой разрядности» (Свидетельство о государственной регистрации программы для ЭВМ № 2019619806 от 24.07.2019); «Программный комплекс моделирования методов распределения информации» (Свидетельство о государственной регистрации программы для ЭВМ № 2019619899 от 26.07.2019; «Программа модулярного нейросетевого кодирования данных» (Свидетельство о государственной регистрации программы для ЭВМ № 2019661394 от 28.08.2019); «Программа модулярного нейросетевого декодирования данных» (Свидетельство о государственной регистрации программы для ЭВМ № 2019661480 от 02.09.2019); «Программный модуль эффективной реализации арифметических операций в конечном поле» (Свидетельство о государственной регистрации программы для ЭВМ № 2019663760 от 23.10.2019); «Программный модуль сравнения чисел в системе остаточных классов» (Свидетельство о государственной регистрации программы для ЭВМ № 2019663930 от 25.10.2019); «Программа избыточного кодирования и декодирования модулярного кодам» (Свидетельство о государственной регистрации программы для ЭВМ № 2020610041 от 09.01.2020); «Программа подготовки файлов для распределенного хранения данных в облаках» (Свидетельство о государственной регистрации программы для ЭВМ № 2020618967 от 10.08.2020); «Программа восстановления полученных данных при распределенном хранении данных в облаках» (Свидетельство о государственной регистрации программы для ЭВМ № 2020619140 от 12.08.2020); «Программный модуль декодирования данных с использованием минимально избыточного модулярного кода» (Свидетельство о государственной регистрации программы для ЭВМ № 2020660256 от 01.09.2020); «Система моделирования исправления ошибок в модулярном коде» (Свидетельство о государственной регистрации программы для ЭВМ № 2020660257 от 01.09.2020); «Программный модуль сбо-

ра данных о технических характеристиках облачных провайдеров в реальном режиме времени» (Свидетельство о государственной регистрации программы для ЭВМ № 2020660392 от 03.09.2020); «Модуль выбора оснований системы остаточных классов для оптимизации минимально избыточного кода» (Свидетельство о государственной регистрации программы для ЭВМ № 2020660531 от 04.09.2020); «Программный модуль управления адаптивной безопасностью в мультиоблачной среде» (Свидетельство о государственной регистрации программы для ЭВМ № 2020660532 от 04.09.2020); «Программа управления устройством коррекции однократных ошибок на основе перехода к обобщенной позиционной системе счисления» (Свидетельство о государственной регистрации программы для ЭВМ № 2020665103 от 23.11.2020); «Программа управления устройством коррекции однократных ошибок на основе Китайской теоремы об остатках с дробными величинами» (Свидетельство о государственной регистрации программы для ЭВМ № 2020665416 от 26.11.2020); «Программа для умножения зашифрованных матриц с использованием CKKS схемы» (Свидетельство о государственной регистрации программы для ЭВМ № 2021616029 от 15.04.2021).

Разработаны маломощные и надежные устройства для реализации ресурсоемких арифметических операций с большими числами, такие как: «Устройство сравнения и определения знака чисел, представленных в системе остаточных классов» (Евразийский патент № 038389 от 20.08.2021); «Устройство определения знака числа, представленного в системе остаточных классов» (Патент № 2747371 Российская Федерация от 04.05.2021); «Устройство сравнения чисел, представленных в системе остаточных классов» (Патент № 2751992 Российская Федерация от 22.10.2020); «Устройство для обнаружения переполнения динамического диапазона, определения ошибки и локализации неисправности вычислительного канала в ЭВМ, функционирующих в системе остаточных классов» (Патент № 2483346 Российская Федерация от 27.05.2013); «Устройство для сравнения чисел, представленных в системе остаточных классов» (Патент № 2503992 Российская Федерация от 10.04.2013); «Устройство для определения знака модулярного числа» (Патент № 2503995 Российская Федерация от 10.04.2013); «Устройство деления модулярных чисел» (Патент № 2628179 Российская Федерация от 15.08.2017); «Устройство вычисления модулярного произведения Монтгомери» (Патент № 2652450 Российская Федерация от 26.04.2018); «Устройство обнаружения и коррекции ошибки модулярного кода» (Патент № 2653257 Российская Федерация от 07.05.2018); «Устройство для перевода чисел из системы остаточных классов и расширения оснований» (Патент № 2744815 Российская Федерация от 16.03.2021); «Устройство для основного деления модулярных чисел» (Патент № 2559771 Российская Федерация от 10.08.2015); «Устройство для основного деления модулярных чисел в формате системы остаточных классов» Патент № 2559772 Российская Федерация от 10.08.2015).

Достоверность и обоснованность полученных в диссертации результатов подтверждена корректным применением классических методов исследования, строгими доказательствами и анализом эффективности разработанных моделей и алгоритмов. Результаты согласуются с проведенными численными экспериментами.

Соответствие диссертации паспорту специальности. Тема и основные результаты диссертации соответствуют следующим областям исследований паспорта специальности ВАК 2.3.5 (05.13.11) – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»:

1. Модели, методы, алгоритмы, языки и программные инструменты для организации взаимодействия программ и программных систем;
2. Модели и методы создания программ и программных систем для параллельной и распределенной обработки данных, языки и инструментальные средства параллельного программирования;
3. Модели, методы, алгоритмы и программная инфраструктура для организации глобально распределенной обработки данных.

Апробация работы. Все результаты диссертационного исследования прошли апробацию на научных мероприятиях в России и за рубежом. Выделим наиболее значимые из них.

Российские конференции: International Siberian Conference on Control and Communications (SIBCON), 2015. International Conference Engineering and Telecommunication (En&T), 2020, 2019, 2016, 2015, 2014. Ivannikov ISPRAS Open Conference (ISPRAS), 2020, 2019. International Conference «Marchuk Scientific Readings 2020», dedicated to the 95th anniversary of the birthday of RAS Academician Guri. I. Marchuk (MSR-2020), 2020. International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE), 2021, 2020. International Conference Russian Supercomputing Days (RuSCDays), 2020. Conference of Open Innovations Association (FRUCT), 2010. International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2017, 2016. IEEE International Conference on Soft Computing and Measurements (SCM), 2017. International Conference BOINC-Based High Performance Computing: Fundamental Research and Development (BOINC: FAST), 2017. International Scientific Conference Intelligent Information Technologies for Industry (IITI), 2016 и др.

Международные симпозиумы: IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW, 2021, 2019, 2018 (Core Rank A). IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGrid, 2021 (Core Rank A). International Conference on Optimization and Learning, OLA, 2021. Latin American High Performance Computing Conference, CARLA, 2020, 2019, 2018, 2017. International Conference on High Performance Computing and Simulation, HPCS, 2019, 2018 (Core Rank

B). International Workshop on Database and Expert Systems Applications, DEXA, 2017 (Core Rank B). IEEE 8th International Conference on Application of Information and Communication Technologies (AICT). 6th International Conference on Swarm Intelligence (ICSI) held in conjunction with the 2nd BRICS Congress on Computational Intelligence (CCI).

Публикации. По теме диссертации автором было опубликовано 89 статей, в том числе 36 статей в журналах из списка, рекомендованного ВАК, или индексируемых в международных базах Scopus и/или Web of Science [1–36], 53 работы – в сборниках трудов российских и международных конференций [37–89], получено 26 свидетельств о государственной регистрации программ для ЭВМ и 12 патентов на изобретения.

Личный вклад автора. Диссертационная работа представляет собой многолетнее исследование автора, объединенное тематикой и методами исследования. Все выносимые на защиту результаты получены лично автором. Из совместных работ в диссертацию включены только те результаты, которые принадлежат непосредственно автору. В опубликованных совместных работах постановка и решение задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя. В статьях [1, 2, 4–6, 8, 10, 11, 15, 18, 29, 33, 39–41, 44–46, 48, 49, 52, 55, 57, 58, 61, 65, 69, 74, 77, 79–82, 84, 85, 88, 89] автором разработаны модели, методы и алгоритмы повышения надежности и безопасности распределенных систем хранения и обработки данных. В статьях [8, 11, 21] автором разработаны методы обнаружения, локализации и исправления ошибок в СОК. В статьях [4, 7, 9, 12, 14, 16, 20, 24, 26, 28, 31, 32, 42, 44, 48, 50, 51, 54, 56, 59, 60, 62–64, 67, 83] автором разработаны методы уменьшения вычислительной сложности алгоритмов выполнения операций определения знака, сравнения, деления закодированных чисел. В статьях [3, 4, 7–24, 26–31, 34–36, 39, 41, 42, 45, 47–55, 57–62, 68–87] автором исследованы свойства существующих схем, предложены и реализованы механизмы повышения их эффективности. В статьях [43, 56] автором разработаны методы обнаружения и исправления ошибок арифметических операций основанные на использовании свойств ранга числа. В статьях [25, 29, 33, 37, 38, 59, 63, 66] автором классифицированы существующие схемы и предложена структурная математическая модель обработки данных в распределенных средах. В статьях [7, 8, 23, 24, 26, 29, 59, 61, 69, 82] автором опубликованы результаты моделирования существующих и предложенных схем, полученные на основе разработанного комплекса программ.

Структура работы. Диссертация состоит из введения, 6 глав, заключения, библиографии из 378 наименований и 2 приложений. Общий объем основного текста работы – 321 страница, включая 35 таблиц и 43 рисунка.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе представлен проблемный обзор угроз информационной безопасности в современных распределенных средах хранения и обработки дан-

ных. Распределенные системы характеризуются высоким уровнем неопределенности, связанной с нестационарностью и динамическим изменением количества и состава их узлов и компонентов, что отрицательно влияет на эффективность вычислений, создавая дополнительные трудности в решении проблем планирования. Таким образом, требуется разработка новых стратегий управления ресурсами для эффективного решения проблемы неопределенности.

В рамках сформулированной цели исследования построена структурная модель обработки данных в распределенных средах (рис. 1).

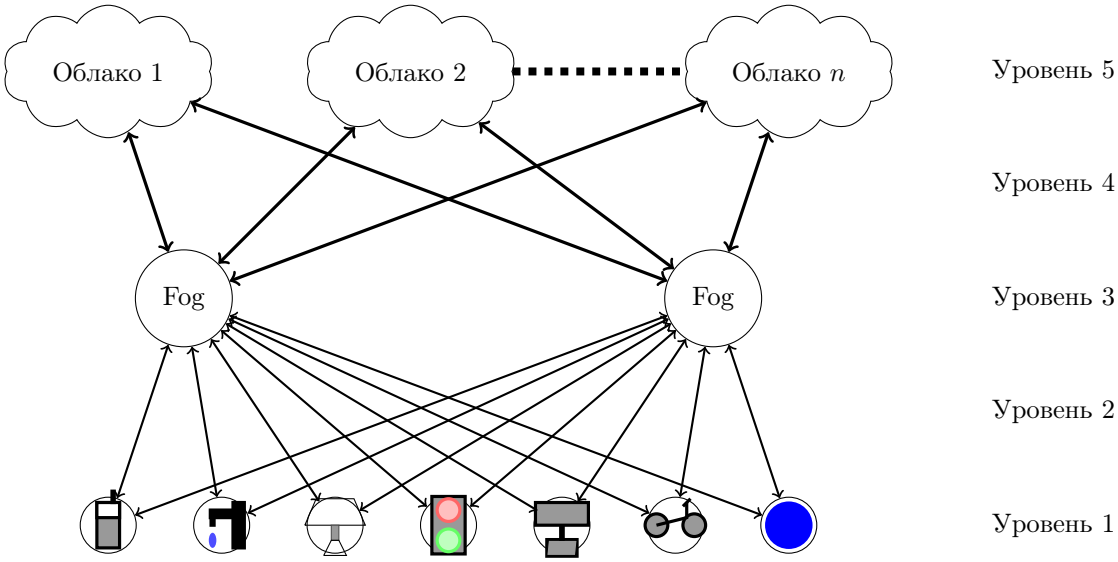


Рисунок 1 — Структурная схема работы Интернета вещей

Выделено пять уровней передачи, хранения и обработки данных. Для каждого из уровней выявлены основные угрозы безопасности данных и проанализированы современные методы уменьшения вероятности кражи, потери или искажения данных.

Уровень 1. Сенсоры, датчики, встроенные устройства, характеризуемые очень низким энергопотреблением и низким уровнем защиты информации. Как правило, используются в смартфонах, нестандартных вычислительных устройствах, бытовой технике, дверных замках, холодильниках и т.д. Абсолютное большинство указанных устройств работают от батареи, поэтому проблема снижения энергопотребления наиболее актуальна для данного уровня.

Уровень 2. Беспроводные сети передачи данных. Процесс передачи реализуется устройствами с низким энергопотреблением, поэтому характеризуется высоким уровнем неопределенности, что затрудняет организацию безопасности при передаче.

Уровень 3. Вычислительная инфраструктура, объединяющая ресурсы миллиардов подключенных туманных устройств. Туманные устройства – это надежные и безопасные гетерогенные вычислительные устройства с ограниченными вычислительными возможностями. Очевидные преимущества туманных вычислений – возможность распределенной обработки данных, увеличение ско-

рости работы приложений, минимизация задержек при передаче данных, улучшение качества обслуживания и качества взаимодействия. Основной проблемой на данном уровне является сложность организации распределенных вычислений.

Уровень 4. Всемирная сеть передачи данных Интернет. Характеризуется высоким уровнем надежности.

Уровень 5. Распределенные центры хранения и обработки данных, характеризующиеся возможностью динамического масштабирования и адаптации параметров для обеспечения различных уровней надежности и снижения рисков нарушения конфиденциальности, потери и утечки конфиденциальных данных, DDoS-атак и т.д.

Установлено, что в распределенных средах в условиях повышенной неопределенности фундаментальные подходы к снижению рисков конфиденциальности, целостности и доступности, использующие механизмы репликации данных, резервного копирования, структуры доступа, избыточную систему остаточных классов, коды стирания недостаточно эффективны и должны быть усовершенствованы. Предложено использование вышеперечисленных механизмов, адаптированных, оптимизированных и интегрированных в концепцию мультиоблачного хранения и обработки данных. Использование мультиоблачного подхода позволяет существенно повысить надежность распределенных систем и снизить вероятности потери, утечки информации, отказа в доступе в течение длительного времени.

Модель, наиболее адекватную мультиоблачному подходу с точки зрения организации распределенного хранения и обработки данных, реализуют пороговые структуры доступа. Однако, выбор оптимальной структуры доступа представляет собой сложную многокритериальную задачу, т.к. должен осуществляться не только на основе стандартных метрик, таких как сложность, скорость выполнения и т.д., но и учитывать особенности распределенной среды, связанные, в первую очередь, с высоким уровнем неопределенности. В работе приведено обоснование выбора алгоритмов реализации пороговых структур доступа с точки зрения обеспечения безопасности, надежности хранения, возможности осуществления контроля корректности операций с данными, гомоморфных вычислений и вводимой избыточности.

Возможность реализации гомоморфных вычислений является наиболее существенным аспектом при выборе параметров структуры доступа, т.к. помимо возможности распределенной обработки гомоморфные вычисления позволяют обеспечить безопасность обрабатываемых данных за счет обработки в закодированном виде.

Существующие схемы, построенные с использованием гомоморфизма колец, позволяют выполнять арифметические операции сложения и умножения закодированных чисел. В зависимости от применяемой схемы гомоморфных вычислений меняются подходы к выполнению указанных операций. Однако,

общей проблемой гомоморфных вычислений, независимо от используемого подхода (гомоморфные вычисления над кольцом вычетов с делителями нуля или над полем) и вида применяемых схем, является высокая сложность реализации и, как следствие, низкая скорость обработки данных. Наибольшие задержки наблюдаются при выполнении вычислительно сложных операций, к ним относятся операции определения знака числа и сравнения чисел. Эффективность выполнения указанных операций можно повысить путем разработки новых методов и оптимизации соответствующих алгоритмов вычисления приближенного (с необходимой точностью) или точного (когда это возможно) значения результата данных операций с сохранением свойства гомоморфности. Повышение эффективности вычисления результатов проблемных для гомоморфных вычислений операций равносильно ускорению процедуры кодирования/декодирования в целом, поэтому разработке методов выполнения операций определения знака числа и сравнения чисел уделено особое внимание в данном исследовании.

Вторая глава посвящена построению высокопроизводительной вычислительно стойкой структуры доступа, обладающей свойствами гомоморфизма колец, и обеспечивающей высокий уровень безопасности и надежности в нестационарной облачной среде. Предложена адаптивная распределенная служба хранения под названием WA-MRC-RRNS, которая реализует гомоморфное отображение и сочетает в себе функционал взвешенной пороговой структуры доступа и системы контроля корректности результатов обработки данных.

Использование взвешенной пороговой структуры доступа обусловлено доказанной теоремой о том, что вероятность потери данных при использовании взвешенной пороговой структуры доступа не превышает вероятности потери данных при использовании соответствующей классической пороговой структуры доступа.

Теорема 1. $Pr\left(k,n\right) \geq Pr\left(n_v = \left(K-1, K-1, \ldots, K-1\right), K, N\right)$ *для любого* $k = K \geq 2$.

Показано, что в пессимистическом сценарии при настройке (3,4), вероятность потери данных при использовании WA-MRC-RRNS в 777.02 раза ниже, чем при использовании соответствующей классической пороговой структуры доступа MRC-RRNS (рис. 2). В среднем же вероятность потери данных при использовании WA-MRC-RRNS ниже в $9.23 \cdot 10^{17}$ раза.

Выбор ИСОК (RRNS) в качестве основы для предложенной взвешенной пороговой структуры доступа обусловлен возможностью построения вычислительно стойкой схемы и реализации механизмов обнаружения/восстановления множественных ошибок данных. Кроме того, ИСОК позволяет динамически настраивать параметры, чтобы справиться с различными объективными предпочтениями, рабочими нагрузками и свойствами облака.

Высокая производительность предложенной схемы достигается за счет разработанных алгоритмов кодирования/декодирования, основанных на пере-

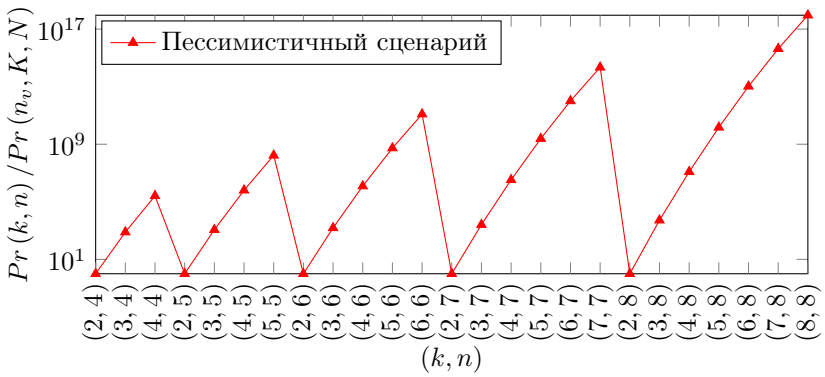


Рисунок 2 — Преимущество схемы WA-MRC-RRNS по сравнению с MRC-RRNS с точки зрения вероятности потери данных в пессимистичном сценарии

ходе к представлению в обобщенной позиционной системе счисления (MRC), нейронной сети конечного кольца и их эффективной программной реализации. Сравнение предложенной схемы WA-MRC-RRNS с другой известной взвешенной схемой WA-AR-RRNS с точки зрения производительности дало следующие результаты: при кодировании WA-MRC-RRNS быстрее WA-AR-RRNS в 13.73 раза, при декодировании WA-MRC-RRNS быстрее WA-AR-RRNS в 385.07 раза.

Отметим, что предложенная схема WA-MRC-RRNS также превосходит классическую пороговую схему AR-RRNS с точки зрения производительности (в 4.83 раза при кодировании и в 120.04 раза при декодировании), проигрывая лишь классической пороговой схеме MRC-RRNS в 2.42 раза при кодировании и в 1.16 раза при декодировании. Данные потери в производительности абсолютно оправданы многократным повышением надежности и безопасности, достигаемым за счет использования взвешенной схемы WA-MRC-RRNS вместо классической пороговой схемы MRC-RRNS.

WA-MRC-RRNS – адаптивная схема, позволяющая динамически регулировать настройки (n_v, K, N), чтобы справиться с отключениями, сбоями и изменением характеристик и параметров облачных сервисов. Настройки должны определяться экспериментально на основе накопленных статистических показателей. Статистический интервал времени должен быть установлен в соответствии с динамикой нестационарной среды и конфигурациями системы. Решение данных задач выходит за рамки данной работы и является предметом будущих исследований.

Для анализа предложенной схемы WA-MRC-RRNS с точки зрения безопасности данных, доказано утверждение, дающее оценку вероятности получения несанкционированного доступа к данным.

Утверждение 1. *В предлагаемой схеме WA-MRC-RRNS вероятность получения данных на основе долей из t различных хранилищ $\bar{I} = \{i_1, i_2, \ldots, i_t\}$ меньше или равна $Pr_C(L) \leq 2^{-\left(1-\frac{1}{W}\sum_{i\in\bar{I}} w_i\right)\cdot L} \cdot \prod_{i\in\bar{I}} Pr_{C_i} \cdot \prod_{i\notin\bar{I}} (1 - Pr_{C_i})$, где $\bar{I}$ –*

множество злоумышленников (множество облачных сервисов, вступивших в сговор), $\sum_{(i\in\bar{I})} w_i < W$, L *– размер исходных данных (в битах), а* Pr_{C_i} *– вероятность вступления в сговор i-го облака.*

Приведены вероятности получения несанкционированного доступа к данным для каждого из трех основных сценариев сговора: когда противоборствующая коалиция знает секретный ключ и не знает необходимое количество долей, не знает ни секретного ключа ни необходимого количества долей, а также не знает секретного ключа и знает необходимое количество долей. Для обеспечения безопасности данных предложено интегрировать WA-MRC-RRNS в разработанную конфигурируемую схему хранения данных AC-RRNS. Доказана вычислительная безопасность AC-RRNS.

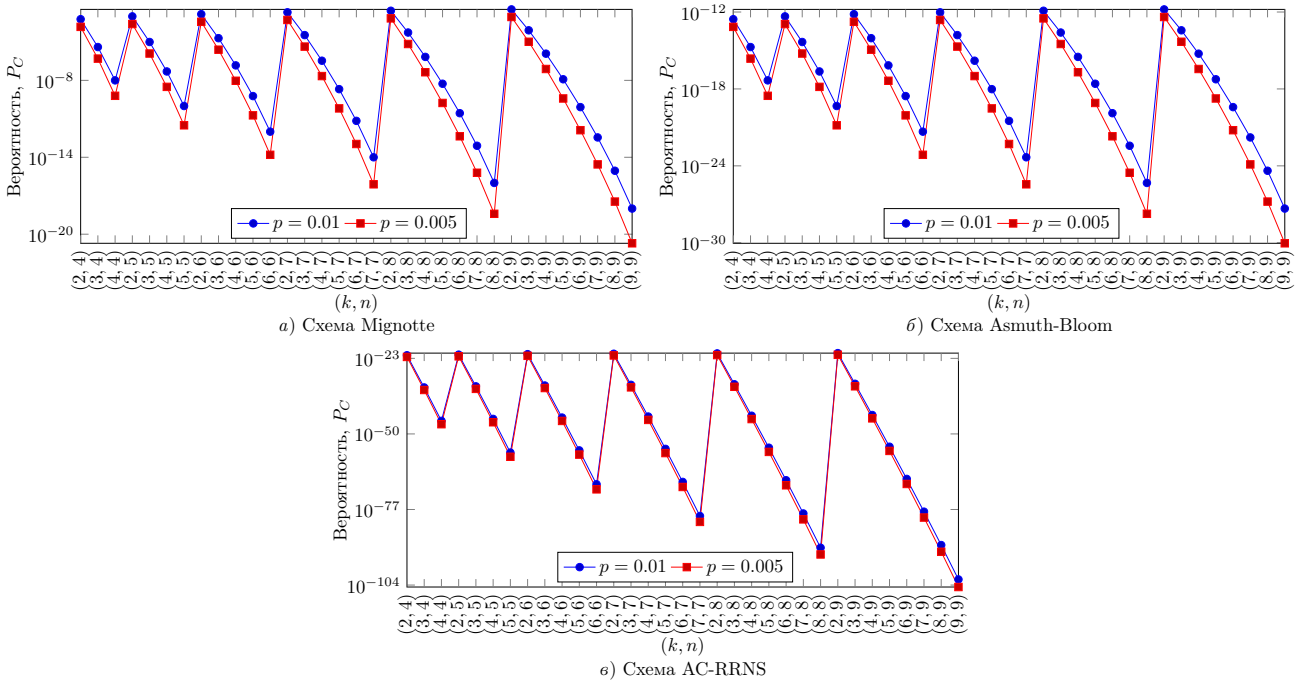
Утверждение 2. *Если при использовании структуры доступа AC-RRNS с параметрами* (k, n)*, коалиция злоумышленников знает менее* k *долей и секретный ключ* p_0*, то вероятность получения несанкционированного доступа к данным меньше* $1/2^{l-1}$.

Утверждение 3. *Если при использовании структуры доступа AC-RRNS с параметрами* (k, n) $l > k$*, вероятность получения несанкционированного доступа к данным на основе* k *или более известных долей без секретного ключа меньше* $\frac{1}{2^{l\cdot(k-1)}\cdot(2^{l-k}-1)}$.

Следствие 1. *Если в структуре доступа AC-RRNS с параметрами* (k, n) *при* $l > 2k$*, противоборствующая коалиция знает менее* k *долей и не знает секретного ключа, то несанкционированный доступ к данным может быть получен с вероятностью меньше* $\frac{1}{2^{l-k}}$*, что эквивалентно полному перебору.*

Сравнительный анализ предложенной схемы с известными структурами доступа, использующими аппарат ИСОК, такими как схема HORNS, основанная на схеме Mignotte, и схема Asmuth-Bloom, дал следующие результаты: HORNS обладает меньшей избыточностью, но в отличие от предложенной схемы, не является вычислительно безопасной, уязвима для атаки открытым текстом и не может быть использована для решения проблемы сговора; схема Asmuth-Bloom является асимптотически идеальной, подходит для обеспечения безопасности данных при сговоре, но вводит избыточность в k раз превышающую избыточность предложенной схемы (k – параметр схемы Asmuth-Bloom). Кроме того, использование AC-RRNS многократно снижает вероятность неавторизованного доступа к данным коалиции из k злоумышленников по сравнению со схемами HORNS и Asmuth-Bloom (рис. 3).

Таким образом, предложенная схема превосходит ранее разработанные аналоги по многим параметрам и соответствует требованиям, предъявляемым к гомоморфным кодам, используемым в распределенных средах хранения и обработки данных.



а) Схема Mignotte

б) Схема Asmuth-Bloom

в) Схема AC-RRNS

Рисунок 3 — Вероятность неавторизованного доступа коалиции из k злоумышленников для схем Mignotte, Asmuth-Bloom и AC-RNNS при длине модулей $l = 32$ бита

В третьей главе исследованы различные подходы к выполнению операций определения знака и сравнения чисел, разработаны методы и алгоритмы реализации указанных операций, позволяющие повысить производительность гомоморфных вычислений над кольцом вычетов с делителями нуля.

Установлено, что результаты операций определения знака числа и сравнения чисел, заданных над кольцом вычетов с делителями нуля, невозможно вычислить с помощью многочленов.

Теорема 2. *Если m – составное число, то в кольце $\mathbb{Z}_m[x]$ не существует многочлена $s(x) \in \mathbb{Z}_m[x]$, такого что $\forall x \in \mathbb{Z}_m$:* $\operatorname{sign}_m(x) = s(x)$.

Разработаны два алгоритма, реализующие определение знака числа для гомоморфных вычислений над кольцом вычетов с делителями нуля, основанных на СОК с четным и нечетным диапазоном.

Представлен обзор существующих и предложены новые методы сравнения чисел для гомоморфных вычислений над кольцом вычетов с делителями нуля на основе СОК.

Методы, основанные на переводе чисел из СОК в позиционную систему счисления, являются наиболее очевидными и наименее производительными способами сравнения чисел. С целью повышения производительности разработаны методы сравнения, основанные на вычислении позиционных характеристик, таких как диагональная функция, функция ядра Акушского, функция Pirlo и Impedovo. Все вышеперечисленные позиционные характеристики, кроме функ-

Алгоритм 1: Определение знака числа для случая, когда диапазон СОК – четное число

Input: $\{p_1, p_2, \ldots, p_{n-1}, p_n\}$ – модули СОК,
$X \xrightarrow{COK} (x_1, x_2, \ldots, x_n)$ – представление числа X в СОК,
$w_{i,j} = \left|p_i^{-1}\right|_{p_j}$ – синаптические веса
Output: $0\,(X \geq 0)$ или $1\,(X < 0)$

```
for i = 1, i < n, i++ do
    for j = i + 1, j ≤ n, j++ do
        x_j = |(x_j − x_i) · w_{i,j}|_{p_j}
```

Result: $\left\lfloor \frac{2x_n}{p_n} \right\rfloor$.

Алгоритм 2: Определение знака числа для случая, когда диапазон СОК – нечетное число

Input: $\{p_1, p_2, \ldots, p_{n-1}, p_n\}$ – модули СОК,
$X \xrightarrow{COK} (x_1, x_2, \ldots, x_n)$ – представление числа X в СОК,
$w_{i,j} = \left|p_i^{-1}\right|_{p_j}$ – синаптические веса
Output: $0\,(X \geq 0)$ или $1\,(X < 0)$

```
S_1 = (2x_1) div p_1;
for i = 1, i < n, i++ do
    for j = i + 1, j ≤ n, j++ do
        x_j = |(x_j − x_i) · w_{i,j}|_{p_j};
    S_{i+1} = (2 · (x_{i+1} + S_i)) div (p_{i+1} + 1)
```

Result: S_n

ции ядра Акушского, являются монотонными, и возможна ситуация, когда разные числа имеют одинаковую позиционную характеристику. В этом случае требуется выполнение дополнительных действий для сравнения чисел, представленных в СОК. Кроме того, для получения значений указанных позиционных характеристик используется ресурсозатратная операция вычисления остатка от деления на большой модуль. Для устранения этих недостатков введено понятие модифицированной диагональной функции, которое служит теоретической основой для разработки значительно более быстрого алгоритма сравнения. Модифицированная диагональная функция (MDF) является строго возрастающей и сочетает в себе преимущества диагональной функции и приближенного метода. Строгая монотонность MDF обеспечивает взаимооднозначное соответствие числа и его позиционной характеристики, поэтому не возникает ситуаций, когда

требуется выполнение дополнительных действий для сравнения чисел. Кроме того, вместо операции нахождения остатка от деления на большое число, при вычислении MDF используются значительно более простые в реализации вычисления по модулю, равному степени числа 2.

Разработанное устройство сравнения на основе MDF и его наиболее эффективные известные аналоги, применяемые для сравнения чисел в СОК с модулями общего вида, были синтезированы для технологии 65 нм с использованием нескольких образцов наборов модулей. Согласно полученным оценкам производительности, предложенный подход обеспечивает снижение задержки на $11-75\%$ (в зависимости от набора модулей) по сравнению с самыми быстрыми существующими реализациями известных методов сравнения чисел в СОК. Более того, наблюдается снижение аппаратных затрат (более чем на 41%) и значительное снижение энергопотребления, которое в ряде случаев превышает 100%. Таким образом, предложенный метод на основе MDF позволяет реализовывать наиболее эффективные на сегодняшний день устройства сравнения чисел, представленных в СОК с наборами модулей общего вида.

Особого внимания заслуживает функции ядра Акушского, свойства которой зависят от используемых при ее построении коэффициентов. Доказано, что для достижения монотонности при построении функции ядра необходимо использовать только неотрицательные коэффициенты.

Теорема 3. *Функция ядра Акушского монотонно возрастает тогда и только тогда, когда все ее коэффициенты $\bar{w}_i$ неотрицательны.*

Показано, что уже известная диагональная функция, ранее предложенная для реализации сравнения чисел в СОК, есть не что иное, как частный случай функции ядра со всеми коэффициентами равными единице. Сформулированы условия, при которых обеспечивается минимальный диапазон функции ядра (необходимый для получения наилучших характеристик устройства сравнения чисел в СОК). Установлено, что монотонная функция ядра минимального диапазона (MMCF) имеет только один коэффициент, равный единице (соответствующий наибольшему модулю), все остальные коэффициенты равны нулю. Сформулирована и доказана теорема об условиях отсутствия критических ядер функции ядра Акушского, имеющая важное практическое значение для построения эффективных позиционных характеристик чисел, представленных в СОК.

Теорема 4. *Для того, чтобы функция ядра $C(X)$, определяемая коэффициентами $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_n$, не содержала критических ядер, необходимо выполнение следующих условий для всех $k = 1, 2, \ldots, n$:*

1. $\sum_{i=1}^{n} \bar{w}_i > 0$.
2. *Отсутствие нижних критических ядер:* $C(p_k) = \sum_{i=1}^{n} \bar{w}_i \left\lfloor \frac{p_k}{p_i} \right\rfloor \geq 0$.

3. Отсутствие верхних критических ядер: $\sum_{i=1}^{n} \left(\left\lfloor \frac{p_k}{p_i} \right\rfloor + 1 \right) \cdot \bar{w}_i - \bar{w}_k > 0.$

Представленное исследование позволяет сделать вывод, что функция ядра Акушского является обобщением позиционных характеристик чисел, представленных в СОК, ее изучение углубит понимание свойств позиционных характеристик и, следовательно, позволит разрабатывать более высокопроизводительные подходы и методы реализации операций над закодированными числами.

В четвертой главе исследованы различные подходы к выполнению операций определения знака и сравнения чисел, оптимизированы известные и разработаны новые методы и алгоритмы реализации указанных операций, позволяющие повысить их эффективность в контексте гомоморфных вычислений над полем.

Гомоморфные вычисления над полем принято делить на два класса: целочисленные и вещественные, по формату обрабатываемых цифровых данных. Соответственно задачи определения знака числа и сравнения чисел следует рассматривать над полем $\mathbb{Z}_m$ и над полем $\mathbb{R}$.

Построены многочлены, использующие интерполяционные многочлены Лагранжа, позволяющие определять знак числа и сравнивать числа над полем $\mathbb{Z}_m$. Вычислительная сложность алгоритмов определения знака и сравнения чисел при использовании целочисленных гомоморфных вычислений зависит от количества арифметических операций сложения и умножения, которые необходимо выполнить для вычисления интерполяционного многочлена. Целочисленные гомоморфные вычисления поддерживают ограниченное количество умножений, поэтому от мультипликативной глубины алгоритма, реализующего ту или иную операцию, во многом зависит производительность системы. Мультипликативная глубина вычисления интерполяционного многочлена зависит от его степени. Доказана теорема, дающая оценку степени интерполяционного многочлена функции определения знака числа: показано, что степень многочлена равна $m - 2$.

Теорема 5. *Если* m *— простое число и* $m \geq 3$*, то в поле* $\mathbb{Z}_m[x]$ *существует единственный многочлен* $s(x) \in \mathbb{Z}_m[x]$*, такой что* $\forall x \in \mathbb{Z}_m \ : \operatorname{sign}_m(x) = s(x)$*. При этом* $\deg s(x) = m - 2$ *и*

$$s(x) = \sum_{i=1}^{m-2} a_i \cdot x^i,$$

где $a_{2j} = 0$ *и* $a_{2j-1} = -\sum_{i=1}^{\frac{m-1}{2}} \left(\frac{1}{i}\right)^{2j-1} + \sum_{i=\frac{m-1}{2}}^{m-1} \left(\frac{1}{i}\right)^{2j-1}$.

Доказана теорема, уточняющая оценку степени интерполяционного многочлена функции сравнения чисел: показано, что степень многочлена $2m - 2$, может быть уточнена до m.

Теорема 6. *Если m – простое число и $m \geq 3$, то в поле $\mathbb{Z}_m[x]$ существует многочлен $c(x,y) \in \mathbb{Z}_m[x,y]$ степени $\deg c(x,y) \leq 2m-2$, такой что $\forall x,y \in \mathbb{Z}_m$: $\mathrm{comp}_m(x,y) \equiv c(x,y) \bmod m$. $c(x,y)$ имеет вид*

$$c(x,y) = x^{m-1} - y^{m-1} + \sum_{t=1}^{m-1}\sum_{k=1}^{m-1} b_{t,k} \cdot x^t \cdot y^k,$$

где $\forall 1 \leq t < k \leq m-1$: $b_{t,k} = \sum_{1\leq i<j\leq m-1}\left(i^{m-1-k}\cdot j^{m-1-t} - i^{m-1-t}\cdot j^{m-1-k}\right)$, $b_{k,t} = -b_{t,k}$, $b(x,y) = \sum_{t=1}^{m-1}\sum_{k=1}^{m-1} b_{t,k}\cdot x^t\cdot y^k$, причем для $c(x,y) \in \mathbb{Z}_m[x,y]$ многочлен $b(x,y) \in \mathbb{Z}_m[x,y]$ определяется единственным образом.

Для аппроксимации функции определения знака числа над полем $\mathbb{R}$ исследована проблема построения многочлена наилучшего приближения указанной функции, где ошибка вычисляется:

$$\|f(x)\| = \int_{-1}^{0} |1 + f(x)|\,dx + \int_{0}^{1} |1 - f(x)|\,dx.$$

Показано, что если степень аппроксимирующего многочлена $n = 0$, то многочленами наилучшего приближения являются $Q_n(x) = a_0$, где $|a_0| \leq 1$. Доказано, что если степень аппроксимирующего многочлена $n \geq 1$, то не существует многочленов наилучшего приближения, являющихся четными функциями. Если степень аппроксимирующего многочлена $n \geq 1$, то существует единственный многочлен наилучшего приближения, являющийся нечетной функцией, который строится с помощью интерполяционной формулы Лагранжа, где в качестве узлов интерполяции используются нули многочлена Чебышева второго рода.

Теорема 7. *Если $n \geq 1$, то существует единственная нечетная функция $Q_n^1(x)$, являющаяся многочленом наилучшего приближения функции знака числа. В зависимости от n функция $Q_n^1(x)$ определяется следующим образом:*

1. *Если n – нечетное число, то*

$$Q_n^1(x) = x\sum_{i=1}^{\frac{n+1}{2}} \frac{1}{\sin\frac{i\pi}{n+3}} \prod_{j=1,j\neq i}^{\frac{n+1}{2}} \frac{x^2 - \sin^2\frac{j\pi}{n+3}}{\sin^2\frac{i\pi}{n+3} - \sin^2\frac{j\pi}{n+3}}$$

   и $\|Q_n^1(x)\| = 2\,\mathrm{tg}\,\frac{\pi}{2n+6}$.

2. *Если n – четное число, то*

$$Q_n^1(x) = x\sum_{i=1}^{\frac{n}{2}} \frac{1}{\sin\frac{i\pi}{n+2}} \prod_{j=1,j\neq i}^{\frac{n}{2}} \frac{x^2 - \sin^2\frac{j\pi}{n+2}}{\sin^2\frac{i\pi}{n+2} - \sin^2\frac{j\pi}{n+2}}$$

   и $\|Q_n^1(x)\| = 2\,\mathrm{tg}\,\frac{\pi}{2n+4}$.

Доказано, что если $n \geq 1$ и n – нечетное число, то не существует многочленов наилучшего приближения, являющихся функциями общего вида. Если $n \geq 1$ и n – четное число, то существует несчетное множество многочленов наилучшего приближения, являющихся функциями общего вида.

Теорема 8. *1. Если n – нечетное число, то не существует функций общего вида $Q_n(x)$, являющихся многочленами наилучшего приближения функции знака числа.*

2. Если n – четное число, то существует несчетное множество функций общего вида $Q_n(x)$, являющихся многочленами наилучшего приближения функции знака числа.

Для каждого рассмотренного случая построены аппроксимирующие многочлены и доказано, что каждый из них является многочленом наилучшего приближения. Для случаев, когда многочлена наилучшего приближения не существует, также доказаны соответствующие теоремы.

Пятая глава посвящена разработке высокопроизводительных методов и алгоритмов вычисления ранга чисел, представленных в СОК. Основным приложением функции ранга числа, представленного в СОК, являются алгоритмы обнаружения и исправления ошибок арифметических вычислений, и от эффективности его вычисления во многом зависит производительность указанных алгоритмов.

Рассмотрены три формы ранга числа: классическая форма ранга, следующая из Китайской теоремы об остатках, нормализованный ранг числа и ранг числа, построенный с использованием функции ядра Акушского. Исследован вопрос об интерполяции функции ранга числа с помощью алгебраических многочленов. Доказан ряд теорем, позволяющих утверждать, что не существует многочлена, заданного над $\mathbb{Z}_P$, позволяющего вычислить ранг числа, представленного в СОК, вне зависимости от его формы.

Предложен эффективный метод вычисления ранга числа, основанный на использовании функции ядра Акушского, не содержащей критических ядер. Доказаны теоремы, дающие оценку верхней и нижней границ разрядности констант при использовании приближенного метода для вычисления ранга числа. Показано, что наборы модулей, удовлетворяющие полученной оценке, не являются компактной последовательностью. Предложенный метод позволяет сократить объем необходимых вычислений и увеличить скорость вычисления ранга числа по сравнению с приближенным методом: для нахождения ранга числа с использованием приближенного метода необходимо выполнить n операций с числами, превышающими значение модуля, тогда как в предлагаемом методе необходимо выполнить $\frac{n(n-1)}{2}$ операций с числами, не превышающими значение модуля.

Разработаны алгоритмы вычисления ранга числа, представленного в СОК. Доказаны теоремы, позволяющие осуществлять контроль результатов

обработки закодированных чисел с использованием арифметических свойств классического ранга.

Теорема 9. *Если* $X \xrightarrow{COK} (x_1, x_2, \ldots, x_n)$ *и* $Y \xrightarrow{COK} (y_1, y_2, \ldots, y_n)$, *заданные в СОК с основаниями* $p_1, p_2, \ldots, p_n$, *удовлетворяют следующим условиям* $0 \le X < P$, $0 \le Y < P$ *и* $0 \le X - Y < P$, *то для них выполняется следующее соотношение*

$$r(X - Y) = r(X) - r(Y) + \sum_{x_i < y_i} \left| P_i^{-1} \right|_{p_i}.$$

Теорема 10. *Пусть заданы модули* $p_1, p_2, \ldots, p_n$ *и два целых числа* $X, Y \in \mathbb{Z}_P$ *в соответствующей СОК:* $X \xrightarrow{COK} (x_1, x_2, \ldots, x_n)$ *и* $Y \xrightarrow{COK} (y_1, y_2, \ldots, y_n)$. *Если существует такое* $j \in \overline{1, n}$, *для которого выполняется равенство* $X = p_j \cdot Y$, *то*

$$r(X) = p_j \cdot r(Y) - \sum_{i=1}^{n} \left| P_i^{-1} \right|_{p_i} \cdot \left\lfloor \frac{p_j \cdot y_i}{p_i} \right\rfloor.$$

В шестой главе представлена конфигурируемая масштабируемая двухуровневая пороговая структура доступа на основе ИСОК (2Lbp-RRNS), разработанная для надежного и безопасного хранения данных в мультиоблачных системах. Предложенная структура допускает использование гомоморфных вычислений и позволяет осуществлять параллельную обработку данных с сохранением их безопасности.

Разработанная схема 2Lbp-RRNS является расширением классической схемы 2L-RRNS. Высокая эффективность и производительность 2Lbp-RRNS достигается за счет использования расстояния Хэмминга.

Получена верхняя граница для количества обнаруживаемых и исправляемых ошибок при использовании традиционных пороговых двухуровневых схем 2L-RRNS и предложенных пороговых двухуровневых схем 2Lbp-RRNS.

Теорема 11. *2Lbp-RRNS способна обнаруживать* N_D^{2Lbp} *и исправлять* N_E^{2Lbp} *ошибок, где* $N_D^{2Lbp} = \sum_{i=1}^{n_1} n_{2,i} - \sum_{i=1}^{k_1} k_{2,i}$, $N_E^{2Lbp} \le \sum_{i=1}^{n_1} n_{2,i} - \sum_{i=1}^{k_1} k_{2,i} - 1$.

Показано, что предложенная схема 2Lbp-RRNS обладает лучшими корректирующими свойствами по сравнению с традиционной схемой 2L-RRNS, позволяет обнаруживать в среднем в 1.58 раза и исправлять в среднем в 3.37 раза больше ошибок (рис. 4).

Предложены эффективные реализации алгоритмов кодирования и декодирования данных в 2Lbp-RRNS: эффективность при кодировании достигается за счет использования метода Паскаля и нейронной сети конечного кольца (FRNN), эффективность декодирования обусловлена использованием перехода

Алгоритм 3: Коррекция ошибок в 2Lbp-RRNS

Input: (k_1, n_1), $(k_{2,1}, n_{2,1})$, …, (k_{2,n_1}, n_{2,n_1}),
$S_1 \xrightarrow{COK} \left(S_{1,1}, S_{1,2}, \ldots, S_{1,n_{2,1}}\right)$, $S_2 \xrightarrow{COK} \left(S_{2,1}, S_{2,2}, \ldots, S_{2,n_{2,2}}\right)$, …,
$S_{n_1} \xrightarrow{COK} \left(S_{n_1,1}, S_{n_1,2}, \ldots, S_{n_1,n_{2,n_1}}\right)$,
$(p_{1,1}, \ldots, p_{1,n_1})$, $\left(p_{2,1,1}, \ldots, p_{2,1,n_{2,1}}\right)$, …, $\left(p_{2,n_{1,1}}, \ldots, p_{2,n_1,n_{2,n_1}}\right)$
Output: S, $flag$

1 2L-RRNS вычисляет S и $flag$. Если флаг $flag \neq -1$, S восстанавливается, иначе S не восстанавливается.

2 Выбирая из $S_{i,1}, S_{i,2}, \ldots, S_{i,n_{2,i}}$ подмножества $k_{2,i}$ элементов из фиксированного набора из $n_{2,i}$ элементов, вычисляем возможные значения S_i^l для каждого из S_i.

3 Выбирая подмножества k_1 элементов из полученных S_i^l, восстанавливаем возможные значения S^j функцией CRTtoBin.

4 Кодируем каждое S^j в 2L-RRNS-представление $\tilde{S}^j$ и вычисляем HD между $\tilde{S}^j$ и $\bar{S}$.

5 Выберем $\tilde{S}^j$, для которого HD минимально. Если минимальное HD между $\tilde{S}^j$ и $\bar{S}$ больше $N_E^{2Lbp} = \sum_{i=1}^{n_1} n_{2,i} - \sum_{i=1}^{k_1} k_{2,i} - 1$, то возвращается $flag = -1$; в противном случае $S = S^j$ и $flag = 1$.

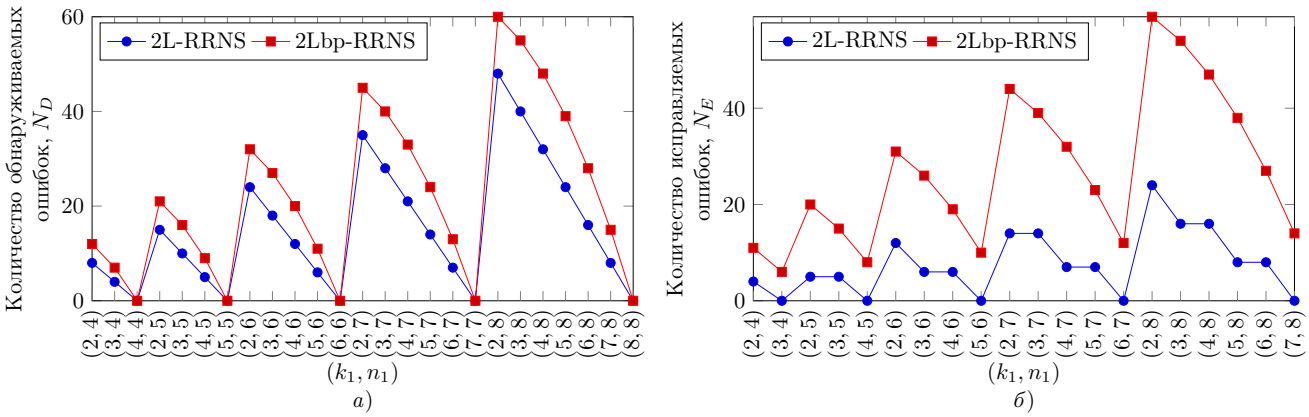


Рисунок 4 — *а*) обнаружение ошибок в 2L-RRNS и 2Lbp-RRNS; *б*) исправление ошибок в 2L-RRNS и 2Lbp-RRNS

к представлению в обобщенной позиционной системе счисления (MRC), FRNN и сверточной нейронной сети (CNN).

Отметим, что при кодировании/декодировании данных в 2Lbp-RRNS, для реализации обратного преобразования вариативно может быть использован один из алгоритмов: Mignotte (основанный на Китайской теореме об остатках), MRC8 или MRC16 (основанные на MRC и отличающиеся лишь размером окна, 8 или 16 бит, при реализации FRNN). Для определения наиболее оптимально-

Алгоритм 4: Кодирование в 2Lbp-RRNS на основе MRC

Input: $settings = (k_1, n_1), (k_{2,1}, n_{2,1}), \ldots, (k_{2,n_1}, n_{2,n_1})$,
S – входные данные,
$(p_{1,1}, \ldots, p_{1,n_1}), (p_{2,1,1}, \ldots, p_{2,1,n_{2,1}}), \ldots, (p_{2,n_1,1}, \ldots, p_{2,n_1,n_{2,n_1}})$,
$W_{1,i} = (w_{1,i,0}, \ldots, w_{1,i,l})$, $W_{2,i,j} = (w_{2,i,j,0}, \ldots, w_{2,i,j,l})$ – синаптические веса FRNN
Output: $S_{i,j}$

```
for i = 1, i ≤ n_1, i++ do
    S_i = FRNN(S, p_{1,i}, W_{1,i});
for i = 1, i ≤ n_1, i++ do
    for j = 1, j ≤ n_{2,i}, j++ do
        S_{i,j} = FRNN(S_i, p_{2,i,j}, W_{2,i,j})
```

Result: $S_{i,j}$

го из перечисленных алгоритмов, выполнен сравнительный анализ производительности схем 2Lbp-RRNS, использующих указанные алгоритмы, учитывающий полный цикл хранения данных: кодирование-загрузка и выгрузка-декодирование для различных параметров облачных хранилищ. Результаты анализа показали, что производительность MRC16 при кодировании-загрузке колеблется в диапазоне 0.406-0.837 МБ/с, а при выгрузке-декодировании в диапазоне 0.54-1.093 МБ/с в зависимости от параметров хранилищ. Для сравнения, показатели наиболее близкого по производительности алгоритма Mignotte при кодировании-загрузке колеблются в диапазоне 0.13-0.257 МБ/с, а при выгрузке-декодировании в диапазоне 0.16-0.292 МБ/с (рис. 5).

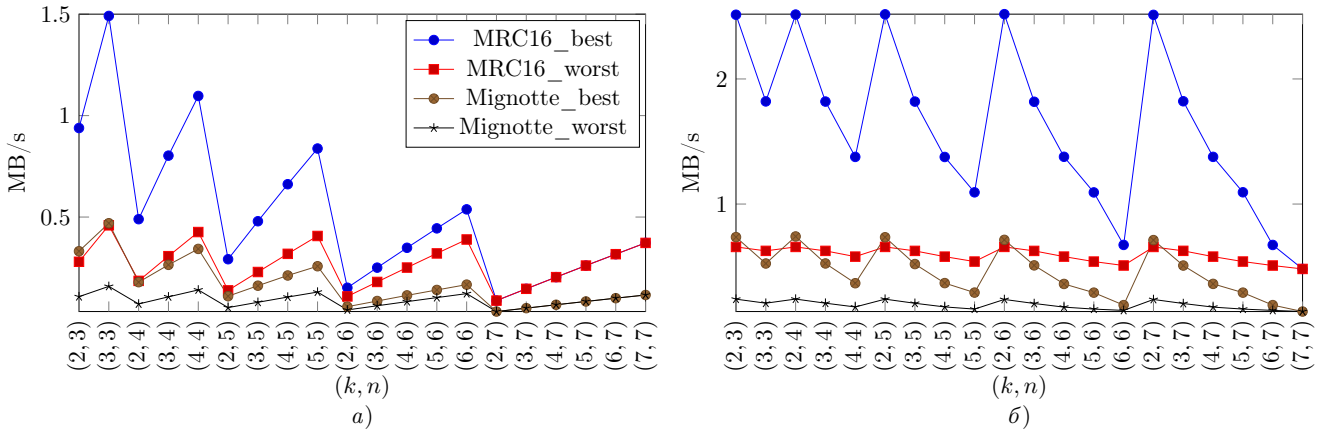


Рисунок 5 — *а*) скорость кодирования-загрузки при настройках $(3, 4)$ уровня 1; *б*) скорость выгрузки-декодирования при настройках $(3, 4)$ уровня 1

Алгоритм 5: Декодирование в 2Lbp-RRNS на основе MRC

Input: $settings = (k_1, n_1)$, $(k_{2,1}, n_{2,1})$, …, (k_{2,n_1}, n_{2,n_1}),
$\tilde{S}$ – представление S в 2L-RRNS,
$(p_{1,1}, \ldots, p_{1,n_1})$, $\left(p_{2,1,1}, \ldots, p_{2,1,n_{2,1}}\right)$, …, $\left(p_{2,n_1,1}, \ldots, p_{2,n_1,n_{2,n_1}}\right)$,
I_D – структура доступа,
$\hat{W}_1 = (\hat{w}_{1,1}, \ldots, \hat{w}_{1,n_1})$, $\hat{W}_{2,i} = \left(\hat{w}_{2,i,1}, \ldots, \hat{w}_{2,i,n_{2,i}}\right)$ – синаптические веса DNN

Output: S

$S_{list} = []$; $p_{list} = []$; $\hat{W}_{list} = []$; //вспомогательные списки
for $i = 1$, $i \leq k_1$, $i++$ **do**
    $j = I_D[i]$;
    $S_i = \mathrm{DNN}\left(\left(S_{j,1}, \ldots, S_{j,n_{2,j}}\right), \left(p_{2,j,1}, \ldots, p_{2,j,n_{2,j}}\right), \hat{W}_{2,j}\right)$;
    $S_{list}.\mathrm{append}(S_i)$; $p_{list}.\mathrm{append}(p_{1,j})$; $\hat{W}_{list}.\mathrm{append}(\hat{w}_{1,j})$;
$S = \mathrm{DNN}\left(S_{list}, p_{list}, \hat{W}_{list}\right)$

Result: S

Таким образом, MRC16 является более сбалансированным и быстрым алгоритмом, превосходящим MRC8 и Mignotte. Также показано преимущество в производительности, достигаемое за счет параллельной реализации предложенной схемы. Все экспериментальные данные получены для восьми реальных облачных хранилищ.

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию методов и алгоритмов, необходимых для построения надежной и безопасной системы распределенного хранения и обработки конфиденциальных данных с использованием гомоморфных вычислений. Основным сдерживающим фактором для широкого практического использования гомоморфных вычислений является их высокая вычислительная сложность, складывающаяся из сложностей проблемных операций, таких как определение знака закодированного числа, сравнение закодированных чисел и контроль результатов обработки закодированных данных без их декодирования. Основные полученные и представленные в работе результаты исследования можно сформулировать следующим образом:

- Разработана теория построения многочленов наилучшего приближения функции определения знака числа, что улучшает и расширяет известные результаты.

- Предложен метод вычисления многочленов наилучшего приближения и решена задача об их количестве.
- Разработана теория сравнения зашифрованных чисел и определения их знака над кольцом с делителями нуля.
- Выделен класс монотонных функций ядра Акушского. Решена проблема возникновения критических ядер.
- Модифицирована теория контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа.
- Разработан метод обнаружения и исправления ошибок в двухуровневом СОК с использованием расстояния Хэмминга.
- Предложены оригинальные методы и алгоритмы повышения надежности и безопасности хранимых и обрабатываемых данных в распределенных средах.
- Построены многочлены, использующие интерполяционные многочлены Лагранжа, позволяющие определять знак числа и сравнивать числа над полем $\mathbb{Z}_m$, уточнены их степени.
- Предложена конфигурируемая масштабируемая двухуровневая структура доступа на основе ИСОК (2Lbp-RRNS), допускающая реализацию гомоморфных вычислений и позволяющая осуществлять параллельную обработку данных с сохранением их конфиденциальности.
- Разработаны алгоритмы кодирования и декодирования данных в 2Lbp-RRNS для улучшения эффективности обработки данных в распределенных средах.

Полученные результаты позволили:

Снизить:
- время выполнения операции в 1.75 раз
- аппаратные затраты в 1.41 раз
- энергопотребление в 2 раза

для устройства сравнения зашифрованных чисел по сравнению с самыми быстрыми существующими реализациями.

Увеличить скорость гомоморфных шифров:
- кодирования в 13.73 раз
- декодирования в 120.04 раз

Повысить надежность и отказоустойчивость:
- увеличить в 1.58 раз количество обнаруживаемых ошибок
- увеличить в 3.37 раз количество исправляемых ошибок

для двухуровневой ИСОК.

Увеличение скорости доступа к данным:
- загрузки в 1.67 раз
- скачивания в 4.53 раза

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ
Статьи автора в журналах, рекомендованных ВАК РФ, Scopus, Web of Science

1. Бабенко, М.Г. Безопасная и надежная передача данных в MANET на основе принципов вычислительно стойкого разделения секрета / Н.И. Червяков, М.А. Дерябин, А.С. Назаров, М.Г. Бабенко, Н.Н. Кучеров, А.В. Гладков, Г.И. Радченко // *Труды Института системного программирования РАН.* — 2019. — Т. 31. — № 2. — С. 153–169.
2. Бабенко, М.Г. Новая схема хранения информации в облачной среде на основе системы остаточных классов и схем разделения секрета / Н.И. Червяков, М.Г. Бабенко, Н.Н. Кучеров и др. // *Современная наука и инновации.* — 2017. — Т. 4. — № 20. — С. 21–25.
3. Бабенко, М.Г. Обучение многослойного персептрона с учителем в задаче распознавания с помощью корреляционного показателя / Н.А. Вершков, М.Г. Бабенко, В.А. Кучуков, Н.Н. Кучукова // *Труды Института системного программирования РАН.* — 2021. — Т. 33. — № 1. — С. 33–46.
4. Бабенко, М.Г. Разработка нового нейросетевого метода вычисления модульного умножения в системе остаточных классов / Н.И. Червяков, М.Г. Бабенко, А.Н. Черных и др. // *Нейрокомпьютеры: разработка, применение.* — 2016. — № 10. — С. 41–48.
5. Бабенко, М.Г. Разработка схемы разделения секрета видеоизображения на основе матрицы Адамара в нейросетевом модулярном базисе / Н.И. Червяков, М.Г. Бабенко // *Нейрокомпьютеры: разработка, применение.* — 2014. — №. 9. — С. 25–29.
6. Бабенко, М.Г. Алгебраические аспекты эффективной реализации методов защиты информации в облачных вычислениях с использованием системы остаточных классов / Н.И. Червяков, М.Г. Бабенко, Н.Н. Кучеров // *Инфокоммуникационные технологии.* — 2016. — Т. 14. — № 4. — С. 343–349.
7. Бабенко, М.Г. Эффективное сравнение чисел в системе остаточных классов на основе позиционной характеристики / М.Г. Бабенко, А.Н. Черных, Н.И. Червяков и др. // *Труды Института системного программирования РАН.* — 2019. — Т. 31. — № 2. — С. 187–201.
8. Babenko, M. 2Lbp-RRNS: Two-Levels RRNS With Backpropagation for Increased Reliability and Privacy-Preserving of Secure Multi-Clouds Data Storage / V. Miranda-López, A. Tchernykh, M. Babenko et al. // *IEEE Access.* — 2020. — Vol. 8. — P. 199424–199439.
9. Babenko, M. An Efficient Method for Comparing Numbers and Determining the Sign of a Number in RNS for Even Ranges / A. Tchernykh, M. Babenko, E. Shiriaev, et al. // *Computation.* — 2022. — Vol. 10. — P. 17.

10. Babenko, M. AC-RRNS: Anti-collusion secured data sharing scheme for cloud storage / A. Tchernykh, M. Babenko, N. Chervyakov et al. // *International Journal of Approximate Reasoning*. — 2018. — Vol. 102. — P. 60–73.
11. Babenko, M. AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security / N. Chervyakov, M. Babenko, A. Tchernykh et al. // *Future Generation Computer Systems*. — 2019. — Vol. 92. — P. 1080–1092.
12. Babenko, M. An Approximate Method for Comparing Modular Numbers and its Application to the Division of Numbers in Residue Number Systems / N.I. Chervyakov, M.G. Babenko, P.A. Lyakhov, I.N. Lavrinenko // *Cybernetics and Systems Analysis*. — 2014. — Vol. 50. — № 6. — P. 977–984.
13. Babenko, M.G. Comparative analysis of homomorphic encryption algorithms based on learning with errors / M.G. Babenko, E.I. Golimblevskaia, E.M. Shiriaev // *Proceedings of the Institute for System Programming of the RAS*. — 2020. — Vol. 32. — № 2. — P. 37–52.
14. Babenko, M. Improved Modular Division Implementation with the Akushsky Core Function / M. Babenko, A. Tchernykh, V. Kuchukov // *Computation*. — 2022. — Vol. 10. — P. 9.
15. Babenko, M.G. Development of Homomorphic Encryption Scheme Based on Polynomial Residue Number System / N.I.Chervyakov, M.G. Babenko, N.N. Kucherov // *Siberian Electronic Mathematical Reports-Sibirskie Elektronnye Matematicheskie Izvestiya*. — 2015. — Vol. 12. — P. C33–C41.
16. Babenko, M. Comparison of modular numbers based on the Chinese remainder theorem with fractional values / N.I. Chervyakov, A.S. Molahosseini, P.A. Lyakhov, M.G. Babenko, I.N. Lavrinenko, A.V. Lavrinenko // *Automatic Control and Computer Sciences*. — 2015. — Vol. 49. — № 6. — P. 354–365.
17. Babenko, M. A Division Algorithm in a Redundant Residue Number System Using Fractions / N. Chervyakov, P. Lyakhov, M. Babenko et al. // *Applied Sciences*. — 2020. — Vol. 10. — № 2. — P. 695.
18. Babenko, M. Dynamic performance–Energy tradeoff consolidation with contention-aware resource provisioning in containerized clouds / R.M. Canosa-Reyes, A. Tchernykh , J.M. Cortes-Mendoza et al. // *PLoS ONE*. — 2022. — Vol. 17. — № 1. — P. e0261856.
19. Babenko, M. A High-Speed Division Algorithm for Modular Numbers Based on the Chinese Remainder Theorem with Fractions and Its Hardware Implementation / N. Chervyakov, P. Lyakhov, M. Babenko et al. // *Electronics*. — 2019. — Vol. 8. — № 3. — P. 261.
20. Babenko, M. High performance parallel computing in residue number system / M. Deryabin, N. Chervyakov, A. Tchernykh, M. Babenko, M. Shabalina // *International Journal of Combinatorial Optimization Problems and Informatics*. — 2018. — Vol. 9. — № 1. — P. 62.
21. Babenko, M. En-AR-PRNS: Entropy-Based Reliability for Configurable and Scalable Distributed Storage Systems / A. Tchernykh, M. Babenko,

A. Avetisyan, A.Yu. Drozdov // *Mathematics*. — 2022. — Vol. 10. — № 1. — P. 84.

22. Babenko, M. Multiple Error Correction in Redundant Residue Number Systems: A Modified Modular Projection Method with Maximum Likelihood Decoding / M. Babenko, A. Nazarov, M. Deryabin, N. Kucherov, A. Tchernykh, N.V. Hung, A. Avetisyan, V. Toporkov // *Applied Sciences*. — 2022. — Vol. 12. — № 1. — P. 463.
23. Babenko, M. Performance evaluation of secret sharing schemes with data recovery in secured and reliable heterogeneous multi-cloud storage / A. Tchernykh, V. Miranda-López, M. Babenko et al. // *Cluster Computing*. — 2019. — Vol. 22. — № 4. — P. 1173–1185.
24. Babenko, M. Positional characteristics for efficient number comparison over the homomorphic encryption / M. Babenko, A. Tchernykh, N. Chervyakov et al. // *Programming and Computer Software*. — 2019. — Vol. 45. — № 8. — P. 532–543.
25. Babenko, M. Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities / B. Pulido-Gaytan, A. Tchernykh, J.M. Cortés-Mendoza, M. Babenko, G. Radchenko, A. Avetisyan, A.Yu. Drozdov // *Peer-to-Peer Networking and Applications*. — 2021. — Vol. 14. — № 3. — P. 1666–1691.
26. Babenko, M. RNS Number Comparator Based on a Modified Diagonal Function / M. Babenko, M. Deryabin, S.J. Piestrak et al. // *Electronics*. — 2020. — Vol. 9. —№ 11. — P. 1784.
27. Babenko, M. Reliability improvement of information systems by residue number system code / A. Nazarov, N. Chervyakov, A. Tchernykh, M. Babenko // *International Journal of Combinatorial Optimization Problems and Informatics*. — 2018. — Vol. 9. — № 1. — P. 81.
28. Babenko, M. Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem / N.I. Chervyakov, A.S. Molahosseini, P.A. Lyakhov, M.G. Babenko, M.A. Deryabin // *International Journal of Computer Mathematics*. — 2017. — Vol. 94. — № 9. — P. 1833–1849.
29. Babenko, M. Scalable Data Storage Design for Nonstationary IoT Environment With Adaptive Security and Reliability / A. Tchernykh, M. Babenko, N. Chervyakov et al. // *IEEE Internet of Things Journal*. — 2020. — Vol. 7. — № 10. — P. 10171–10188.
30. Babenko, M. Search for the Global Extremum Using the Correlation Indicator for Neural Networks Supervised Learning / N. Vershkov, M. Babenko, V. Kuchukov, N. Kuchukova // *Programming and Computer Software*. — 2020. — Vol. 46. — № 8. — P. 609–618.
31. Babenko, M. The Study of Monotonic Core Functions and Their Use to Build RNS Number Comparators / M. Babenko, S.J. Piestrak, N. Chervyakov, M. Deryabin // *Electronics*. — 2021. — Vol. 10. — № 9. — P. 1041.

32. Babenko, M. Towards the Sign Function Best Approximation for Secure Outsourced Computations and Control / M. Babenko, A. Tchernykh, B. Pulido-Gaytan, A. Avetisyan, S. Nesmachnow, X. Wang, and F. Granelli // *Mathematics*. — 2022. — Vol. 10. — № 12. — P. 2006.
33. Babenko, M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability / A. Tchernykh, U. Schwiegelsohn, E.G. Talbi, M. Babenko // *Journal of Computational Science*. — 2019. — Vol. 36. — P. 100581.
34. Babenko, M. The architecture of a fault-tolerant modular neurocomputer based on modular number projections / N.I. Chervyakov, P.A. Lyakhov, M.G. Babenko et al. // *Neurocomputing*. — 2018. — Vol. 272. — P. 96–107.
35. Babenko, M. An efficient method of error correction in fault-tolerant modular neurocomputers / N.I. Chervyakov, P.A. Lyakhov, M.G. Babenko et al. // *Neurocomputing*. — 2016. — Vol. 205. — P. 32–44.
36. Babenko, M. A new model to optimize the architecture of a fault-tolerant modular neurocomputer / N.I. Chervyakov, P.A. Lyakhov, M.G. Babenko et al. // *Neurocomputing*. — 2018. — Vol. 303. — P. 37–46.

Другие публикации автора по теме диссертации

37. Babenko, M. A Survey on Privacy-Preserving Machine Learning with Fully Homomorphic Encryption / L.B. Pulido-Gaytan, A. Tchernykh, J.M. Cortés-Mendoza, M. Babenko, G. Radchenko // *Communications in Computer and Information Science*. — 2020. — Vol. 1327. — P. 115–129.
38. Babenko, M. About Cloud Storage Systems Survivability / N. Kucherov, I. Dvoryaninova, M. Babenko et al. // 2020 International Workshop on Data Mining and Knowledge Engineering (YRID). — *CEUR-WS Proceedings*. — 2020. — Vol. 2842. — P. 43–50.
39. Babenko, M. Adaptive encrypted cloud storage model / E. Lopez-Falcon, A, Tchernykh, N. Chervyakov, M. Babenko, E. Nepretimova, V. Miranda-López, A.Yu. Drozdov, G. Radchenko, A. Avetisyan // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2018. — P. 329–334.
40. Babenko, M. Analysis of secured distributed cloud data storage based on multilevel RNS / A. Tchernykh, M. Babenko, N. Chervyakov et al. // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2018. — P. 382–386.
41. Babenko, M. Architecture Development of Cloud-Based Fail-Safe Privacy Data Storage and Processing System / N.N. Kucherov, M.G. Babenko, A.S. Nazarov, I.S. Vashchenko // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2020. — P. 366–369.

42. Babenko, M. The Accuracy Estimation of the Interval-Positional Characteristic in Residue Number System / M. Babenko, M. Deryabin, A. Tchernykh // 2019 International Conference on Engineering and Telecommunication (En&T). — IEEE, 2019. — P. 1–5.
43. Babenko, M. About One Property of Number Rank in RNS / M. Babenko, E. Golimblevskaia // 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). — IEEE, 2021. — P. 212–216.
44. Babenko, M. Euclidean Division Method for the Homomorphic Scheme CKKS / M. Babenko, E. Golimblevskaia // 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). —IEEE, 2021. — P. 217–220.
45. Babenko, M. Bi-objective analysis of an adaptive secure data storage in a multi-cloud / E.C. Lopez-Falcon, V. Miranda-López, A. Tchernykh, M. Babenko, A. Avetisyan // *Communications in Computer and Information Science*. — 2019. — Vol. 979. — P. 307–321.
46. Babenko, M.G. Development of a secure system for distributed data storage and processing in the clouds based on the concept of active security in RNS / N.I. Cherviakov, M.G. Babenko, M.N. Shabalina // 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). — IEEE, 2017. — P. 558–560.
47. Babenko, M.G. Effective implementation of Wang method using approximate method in RNS / N.I. Cherviakov, M.G. Babenko, M.N. Shabalina // 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). — IEEE, 2017. — P. 514–515.
48. Babenko, M.G. Research of effective methods of conversion from positional notation to RNS on FPGA / N.I. Chervyakov, M.G. Babenko, V.A. Kuchukov // 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2017. — P. 277–281.
49. Babenko, M. Comparative Performance Analysis of Information Dispersal Methods / M. Deryabin, N. Chervyakov, A. Tchernykh, V. Berezhnoy, A. Djurabaev, A. Nazarov, M. Babenko // 2019 24th Conference of Open Innovations Association (FRUCT). — IEEE, 2019. — P. 67–74.
50. Babenko, M. Comparative analysis of the scalar point multiplication algorithms in the NIST FIPS 186 elliptic curve cryptography / M. Babenko, A. Tchernykh, A. Redvanov, A. Djurabaev // 3rd International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE). — *CEUR-WS Proceedings*. — 2021. — Vol. 2913. — P. 21–31.
51. Babenko, M. Computation of positional characteristics of numbers in RNS based on approximate method / N.I. Chervyakov, M.G. Babenko, M.A. Deryabin et al. // 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW). — IEEE, 2016. — P. 177–179.

52. Babenko, M. Computationally secure threshold secret sharing scheme with minimal redundancy. / M.G. Babenko, A. Tchernykh, E. Golimblevskaia et al. // 2nd International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE). — *CEUR-WS Proceedings*. — 2020. — Vol. 2638. — P. 23–32.
53. Babenko, M. Cryptanalysis of secret sharing schemes based on spherical spaces / N.I. Chervyakov, M.G. Babenko, M.A. Deryabin, A.S. Nazarov // 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT). — IEEE, 2014. — P. 1–5.
54. Babenko, M. Cryptographic Primitives Optimization Based on the Concepts of the Residue Number System and Finite Ring Neural Network / A. Tchernykh, M. Babenko, B. Pulido-Gaytan et al. // *Communications in Computer and Information Science*. — 2021. — Vol. 1443. — P. 241–253.
55. Babenko, M. Data Reliability and Redundancy Optimization of a Secure Multicloud Storage Under Uncertainty of Errors and Falsifications / A. Tchernykh, M. Babenko, V. Kuchukov et al. // 2019 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). — IEEE, 2019. — P. 565–572.
56. Babenko, M. Determining the rank of a number in the residue number system / M. Babenko, N. Kucherov, A. Tchernykh et al. // 3rd International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE). — *CEUR-WS Proceedings*. — 2021. — Vol. 2913. — P. 8–20.
57. Babenko, M. Development of Information Security's Theoretical Aspects in Cloud Technology with the Use of Threshold Structures / N. Chervyakov, M. Babenko, M. Deryabin, A. Garianina // 2014 International Conference on Engineering and Telecommunication (En&T). — IEEE, 2014. — P. 38–42.
58. Babenko, M. Development of a control system for computations in BOINC with homomorphic encryption in residue number system / M. Babenko, N. Kucherov, A. Tchernykh et al. // 3rd International Conference BOINC-Based High Performance Computing: Fundamental Research and Development (BOINC:FAST). — *CEUR-WS Proceedings*. — 2017. — Vol. 1973. — P. 77–84.
59. Babenko, M. Experimental Evaluation of Homomorphic Comparison Methods / M. Babenko, A. Tchernykh, B. Pulido-Gaytan et al. // 2020 Ivannikov ISPRAS Open Conference (ISPRAS). — IEEE, 2020 — P. 69–74.
60. Babenko, M. Experimental analysis of large prime numbers generation in residue number system / N.I. Chervyakov, M.G. Babenko, D.S. Konyaeva et al. // 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies"(IT&QM&IS). — IEEE, 2017. — P. 315–318.
61. Babenko, M. Experimental analysis of secret sharing schemes for cloud storage based on RNS / V. Miranda-López, A. Tchernykh, J.M. Cortés-Mendoza

et al. // *Communications in Computer and Information Science*. — 2018. — Vol. 796. — P. 370–383.
62. Babenko, M. Fast modular multiplication execution in residue number system / N.I. Chervyakov, M.G. Babenko, V.A. Kuchukov et al. // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS). — IEEE, 2016. — P. 30–32.
63. Babenko, M. Homomorphic Comparison Methods: Technologies, Challenges, and Opportunities / M. Babenko, A. Tchernykh, E. Golimblevskaia et al. // 2020 International Conference Engineering and Telecommunication (En&T). — IEEE, 2020. — P. 1–5.
64. Babenko, M. Improvement of the Approximate Method for the Comparison Operation in the RNS / E. Shiryaev, E. Golimblevskaia, M. Babenko et al. // 2020 International Conference Engineering and Telecommunication (En&T). — IEEE, 2020. — P. 1–6.
65. Babenko, M. Increasing reliability and fault tolerance of a secure distributed cloud storage / N.N. Kucherov, M.G. Babenko, A. Tchernykh et al. // 2nd International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE). — *CEUR Workshop Proceedings*. — 2020. — Vol. 2638. — P. 166–180.
66. Babenko, M.G. Homomorphic Encryption Methods Review / N.N. Kucherov, M.A. Deryabin, M.G. Babenko // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2020. — P. 370–373.
67. Babenko, M. The Application of Modular Arithmetic for Matrix Calculations / V. Kuchukov, M. Babenko // 2019 Ivannikov Ispras Open Conference (ISPRAS). — IEEE, 2019. — P. 49–54.
68. Babenko, M. LR-GD-RNS: Enhanced Privacy-Preserving Logistic Regression Algorithms for Secure Deployment in Untrusted Environments / J.M. Cortés-Mendoza, G. Radchenko, A. Tchernykh, B. Pulido-Gaytan, M. Babenko, A. Avetisyan, P. Bouvry, A. Zomaya // 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid). — IEEE, 2021. — P. 770–775.
69. Babenko, M. Multi-objective Configuration of a Secured Distributed Cloud Data Storage / L.E. García-Hernández, A. Tchernykh, V. Miranda-López, M. Babenko, A. Avetisyan, R. Rivera-Rodriguez, G. Radchenko, C.J. Barrios-Hernandez, H. Castro, A.Yu. Drozdov // *Communications in Computer and Information Science*. — 2020. — Vol. 1087. — P. 78–93.
70. Babenko, M. Efficient Hardware Implementation of Forward Conversion WNS-RNS on FPGA / A. Nazarov, M. Babenko, E. Golimblevskaia // 2020 International Conference Engineering and Telecommunication (En&T). — IEEE, 2020. — P. 1–4.
71. Babenko, M. Hardware Implementation of the Reverse Conversion RNS-WNS on FPGA / A. Nazarov, M. Babenko, E. Golimblevskaia // 2020 International

Conference Engineering and Telecommunication (En&T). — IEEE, 2020. — P. 1–5.

72. Babenko, M. Neural network method for base extension in residue number system / M.G. Babenko, E. Shiriaev, A. Tchernykh, E. Golimblevskaia // 2nd International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE). — *CEUR-WS Proceedings*. — 2020. — Vol. 2638. — P. 9–22.
73. Babenko, M. Privacy-Preserving Logistic Regression as a Cloud Service Based on Residue Number System / J.M. Cortés-Mendoza, A. Tchernykh, M. Babenko et al. // *Communications in Computer and Information Science*. — 2020. — Vol. 1331. — P. 598–610.
74. Babenko, M. Protocol for Secure and Reliable Data Transmission in MANET based on Modular Arithmetic / M. Deryabin, M. Babenko, A. Nazarov et al. // 2019 International Conference on Engineering and Telecommunication (En&T). — IEEE, 2019. — P. 1–5.
75. Babenko, M. RRNS Base Extension Error-Correcting Code for Performance Optimization of Scalable Reliable Distributed Cloud Data Storage / M. Babenko, A. Tchernykh, B. Pulido-Gaytan et al. // 2021 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). — IEEE, 2021. — P. 548–553.
76. Babenko, M. Realization problems of cryptographic transformations by transfer of modular data in security systems / N.I. Chervyakov, M.G. Babenko, A.S. Nazarov, A.I. Garianina // 2015 International Siberian Conference on Control and Communications (SIBCON). — IEEE, 2015. — P. 1–5.
77. Babenko, M. Secure Verifiable Secret Short Sharing Scheme for Multi--Cloud Storage / M. Deryabin, N. Chervyakov, A. Tchernykh, M. Babenko, N. Kucherov, V. Miranda-López, A. Avetisyan // 2018 International Conference on High Performance Computing Simulation (HPCS). — IEEE, 2018. — P. 700–706.
78. Babenko, M. Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack / M. Babenko, N. Chervyakov, A. Tchernykh et al. // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2018. — P. 270–274.
79. Babenko, M. The Data Transfer Development in MANET Networks on the Base of Chinese Remainder Theorem / N.I. Chervyakov, M.G. Babenko, N.N. Kucherov et al. // *Advances in Intelligent Systems and Computing*. — 2016. — Vol. 451. — P. 3–13.
80. Babenko, M. The Development of Probabilistic Algorithm of Monitoring a Result Correctness for Cloud Computing in Residue Number System / N.I. Chervyakov, A.S. Nazarov, M.G. Babenko et al. // 2015 International Conference on Engineering and Telecommunication (En&T). — IEEE, 2015. — P. 45–49.

81. Babenko, M. The development of secure mobile computing network based on secret sharing schemes / N.I. Chervyakov, M.G. Babenko, M.A. Deryabin et al. // 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW). — IEEE, 2016. — P. 180–184.
82. Babenko, M. The Effective Neural Network Implementation of the Secret Sharing Scheme with the Use of Matrix Projections on FPGA / N.I. Chervyakov, M.G. Babenko, N.N. Kucherov, A.I. Garianina // *Lecture Notes in Computer Science*. — 2015. — Vol. 9142. — P. 3–10.
83. Babenko, M. The Fast Algorithm for Number Comparing in Three-Modular RNS / N. Chervyakov, M. Babenko, A. Tchernykh et al. // 2016 International Conference on Engineering and Telecommunication (En&T). — IEEE, 2016. — P. 26–28.
84. Babenko, M. Toward digital twins' workload allocation on clouds with low-cost microservices streaming interaction / A. Tchernykh, A. Facio-Medina, B. Pulido-Gaytan, R. Rivera-Rodriguez, J.M. Cortés-Mendoza, G. Radchenko, M. Babenko, I. Chernykh, I. Kulikov, S. Nesmachnow // 2020 Ivannikov Ispras Open Conference (ISPRAS). — IEEE, 2020. — P. 115–121.
85. Babenko, M. Towards Mitigating Uncertainty of Data Security Breaches and Collusion in Cloud Computing / A. Tchernykh, M. Babenko, N. Chervyakov et al. // 2017 28th International Workshop on Database and Expert Systems Applications. — IEEE, 2017. — P. 137–141.
86. Babenko, M. Towards Optimizing Cloud Computing Using Residue Number System / N. Kucherov, E. Kuchukova, A. Tchernykh, V. Kuchukov, M. Babenko / International Conference «Marchuk Scientific Readings 2020» (MSR-2020). — *Journal of Physics: Conference*. — 2021. — Vol. 1715. — P. 012052.
87. Babenko, M. Unfairness Correction in P2P Grids Based on Residue Number System of a Special Form / M. Babenko, N. Chervyakov, A. Tchernykh et al. // 2017 28th International Workshop on Database and Expert Systems Applications (DEXA). — IEEE, 2017. — P. 147–151.
88. Babenko, M. WA-RRNS: Reliable Data Storage System Based on Multi-cloud / A. Tchernykh, M. Babenko, V. Miranda-López et al. // 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). — IEEE, 2018. — P. 666–673.
89. Babenko, M. Weighted Two-Levels Secret Sharing Scheme for Multi-Clouds Data Storage with Increased Reliability / V. Miranda-López, A. Tchernykh, M. Babenko et al. // 2019 International Conference on High Performance Computing Simulation (HPCS). — IEEE, 2019. — P. 915–922.