

ОТЗЫВ

официального оппонента Морозова Александра Юрьевича на диссертационную работу Луценко Владислава Вячеславовича «Разработка математической модели, методов и алгоритмов для повышения скорости обработки данных в туманных вычислениях с использованием модулярной арифметики», представленную на соискание ученой степени кандидата физико-математических наук по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Актуальность темы. В связи с ростом объемов обрабатываемой информации все большую актуальность приобретают распределенные вычисления. Значительные нагрузки на облачные дата-центры заставляют все чаще обращаться к концепции туманных и периферийных вычислений. Поддержание конфиденциальности информации, обрабатываемой на периферийных устройствах, требует применения быстрых и надежных средств шифрования. Использование системы остаточных классов (СОК) ввиду ее распределенной природы неоднократно использовалось для реализации туманных вычислений. Однако значительную сложность представляет собой реализация немодульных операций: деления, сравнения, определение знака числа, а также преобразование из СОК в позиционную систему счисления. Широко используемые методы, такие как Китайская теорема об остатках (КТО) и метод перевода чисел из СОК в обобщенную позиционную систему счисления (ОПСС), в основном исчерпали свои возможности и требуют новых инновационных подходов. Применение функции ядра Акушского позволяет повысить производительность немодульных операций в СОК, а также преобразование чисел из СОК в позиционную систему счисления.

Научная новизна. Основными результатами, составляющими научную новизну диссертационной работы, являются:

1. Оптимизация параметров функции ядра Акушского для компактных базисов СОК.
2. Модификация методов и алгоритмов перевода из позиционной системы счисления в СОК и из СОК в позиционную систему счисления, определения знака и сравнения чисел в СОК, отличающиеся от известных меньшей размерностью операндов и эффективной реализацией операций без необходимости нахождения остатка по большому модулю.
3. Разработка программного комплекса для выполнения немодульных операций вычислительными узлами распределенной среды, позволяющий повысить скорость и отказоустойчивость решения задач распределенной обработки данных.

Практическая значимость. В процессе исследования были получены математическая модель, методы и алгоритмы, позволяющие повысить скорость обработки данных в туманных вычислениях за счет использования модулярной арифметики. Полученные результаты могут быть использованы в различных распределенных вычислительных структурах, таких как группы беспилотных аппаратов, орбитальная группировка спутников и т.п., для реализации эффективных вычислений с использованием групп вычислительных устройств небольшой мощности. Полученные результаты были использованы при выполнении следующих проектов: гранта РНФ № 19-71-10033 «Эффективная, безопасная и отказоустойчивая система распределенного хранения и обработки конфиденциальных данных с регулируемой избыточностью для проектирования мобильных облаков на маломощных вычислительных устройствах»,

гранта РНФ № 22-71-10046 «Разработка новых методов и алгоритмов для повышения надежности и безопасности хранения, передачи и обработки данных в туманных вычислениях», гранта РНФ № 24-21-00149 «Разработка модульных искусственных нейронных сетей ориентированных на туманные вычисления», гранта Северо-Кавказского федерального университета «Интеллектуальный блок управления распределенной системой хранения данных в гетерогенных средах с регулируемой избыточностью и безопасностью», гранта РНФ № 25-71-30007 «Новые технологии для проектирования облачных сервисов машинного обучения, сохраняющих конфиденциальность», в Северо-Кавказском центре математических исследований в рамках соглашения № 075-02-2024-1451 с Министерством науки и высшего образования Российской Федерации.

Достоверность и обоснованность научных результатов. Все основные теоретические положения и выводы, сформулированные в диссертационной работе Луценко В.В., являются обоснованными, обеспечиваются строгостью проведения математических доказательств, при получении которых был использован научно-методический аппарат математического анализа, теории чисел и численных методов, а также подтверждается проведенным сравнительным анализом разработанных методов и алгоритмов с известными ранее с точки зрения эффективности обработки данных. По теме работы опубликовано значимое количество работ в рецензируемых изданиях, в том числе международных. Проведена апробация исследований на российских и международных конференциях.

Содержание и структура диссертации.

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи работы, выбраны объект и предмет исследования, показана научная новизна, практическая и теоретическая ценность полученных результатов, приведены основные положения, выносимые на защиту.

В первой главе сформулирована научная проблема, заключающаяся в том, что существующие методы оптимизации криптографических алгоритмов, используемых для защиты данных в туманных и периферийных вычислениях, позволяют получить значительный рост эффективности лишь при использовании дорогостоящего и энергозатратного аппаратного обеспечения. Такой подход противоречит сути туманных вычислений, в которых используется оборудование, не обладающее высокой вычислительной мощностью и часто использующее батареи для питания. Решение проблемы предлагается за счет использования математического аппарата СОК для ускорения вычислений без существенного роста аппаратных затрат.

Во второй главе сформулированы методы и алгоритмы для решения основной проблемы СОК – выполнения немодульных операций. Для нахождения позиционной характеристики числа, представленного в СОК, предлагается использовать функцию ядра Акушского. Предлагаемый подход отличается от общеизвестного тем, что в работе рассмотрена проблема критических ядер Акушского и предложены методы решения этой проблемы. Кроме того, в процессе исследования были исследованы методы перевода числа, представленного в СОК, в позиционную систему счисления, а также предложен метод перевода, основанный на китайской теореме об остатках и ранга функции Акушского, который позволил отказаться от вычислительно сложных операций деления и взятия по модулю. Предложен алгоритм итерационного деления и определения знака числа, позволяющие снизить вычислительные затраты. Исследованы свойства функции ядра Акушского, разработан метод построения минимальных функций ядра, а также

предложены наборы модулей и веса функции ядра, позволяющие уменьшить размер операндов, что, в свою очередь, позволяет значительно снизить вычислительные затраты и энергопотребление аппаратной составляющей.

Третья глава посвящена реализации разработанных математических методов и алгоритмов. Вычислительная система, работающая в СОК, включает в себя набор модулей, позволяющих получить оптимальные параметры для минимизации вычислительной нагрузки. Вычислительный комплекс включает в себя модуль выбора параметров для оптимизации базиса СОК и весов функции ядра Акушского, модуль вычисления позиционных характеристик для выполнения немодульных операций: перевода числа из СОК в позиционную систему счисления, деления чисел, представленных в СОК, определения знака и сравнения чисел. В процессе исследований было произведено тестирование и сравнение производительности созданного вычислительного комплекса с методами библиотеки NTL. Проведено моделирование программных реализаций разработанных методов и алгоритмов для решения задач в распределенной среде, результаты моделирования приведены в доступном для сравнения виде. В результате проведенного исследования можно сделать вывод о возможности снижения вычислительной сложности алгоритмов для снижения вычислительных затрат.

В заключении подведены итоги и обобщены результаты проведенных исследований.

В приложениях представлены результаты моделирования, свидетельства о государственной регистрации программ для ЭВМ.

Замечания по диссертации.

1. Описывая архитектуру распределенной обработки данных, автор утверждает (стр. 15, п. 3), что серьезной угрозой безопасности IoT является отсутствие стандартов безопасности. В качестве примера можно привести международный стандарт ISO/IEC 30141:2024, который как раз описывает архитектуру устройств и сервисов, связанных с IoT, обязательные меры безопасности и порядок их реализации: в физических аспектах устройств и в программных. В нашей стране также действует национальный стандарт ГОСТ Р 57580-2021, касающийся защиты информации в IoT-системах, включает требования к физической безопасности устройств, шифрованию данных и безопасности связи.
2. В разделе 2.1 автор вводит понятие критических ядер, не дав четкого определения данному понятию.
3. В разделе 3.2.2 автор утверждает, что оптимальными весами для функции ядра Акушского являются веса, при которых $C_p = 2^N$, не приводя при этом доказательства утверждения.
4. В алгоритме 14 не определено изменение случайной величины ξ на каждом шаге.
5. В тексте диссертации присутствуют незначительные погрешности в виде опечаток и пунктуационных ошибок, не искажающие смысла изложения. Например, на странице 90 в «в параграфах 2.5.1, 2.5.1» очевидно имелось ввиду «в параграфах 2.5.1 и 2.5.2». На странице 96 при ссылке таблица 27 указана дважды, а нужна ссылка на таблицы 26-28. В таблице 24 имеется набор модулей {1823, 1997, 1997} в котором или присутствует опечатка, или он не взаимно простой и не соответствует выбранному динамическому диапазону.

Отмеченные недостатки не влияют на положительную оценку всех научных и практических результатов диссертации.

Заключение. Диссертация Луценко В.В. «Разработка математической модели, методов и алгоритмов для повышения скорости обработки данных в туманных вычислениях с использованием модулярной арифметики» выполнена на актуальную тему, является законченной научно-квалификационной работой, обладает научной новизной и имеет практическую ценность. Автореферат отражает основные полученные научные результаты диссертационной работы. Таким образом, считаю, что диссертация Луценко Владислава Вячеславовича соответствует всем требованиям Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.5 - Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (физико-математические науки).

Официальный оппонент
старший научный сотрудник отдела Математического
моделирования гетерогенных систем, Федеральное
государственное учреждение «Федеральный
исследовательский центр «Информатика и
управление» Российской академии наук»,
доктор физико-математических наук

Морозов А.Ю.

Согласен на обработку персональных данных
доктор физико-математических наук

Морозов А.Ю.

«27» 10 2025 г.

Контактные данные организации: Федеральное государственное учреждение
«Федеральный исследовательский центр «Информатика и управление» Российской
академии наук», 119333, г. Москва, ул. Вавилова, д. 44, кор. 2, e-mail: frccsc@frccsc.ru,
тел.: + 7 (499) 135-62-60