

ОТЗЫВ

официального оппонента 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 по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Актуальность темы исследования. Диссертация Луценко Владислава Вячеславовича посвящена решению важной научной задачи исследования и разработки математической модели, методов и алгоритмов для повышения скорости обработки данных в сетях туманных вычислений за счет использования модулярной арифметики. Для эффективного решения данной задачи требуется разработка математического аппарата для оптимизации модульных и немодульных операций в системе остаточных классов (СОК). Построение систем обработки информации на базе маломощных устройств, обеспечивающих сокращение времени расчетов путем параллельного выполнения модульных операций на основе СОК, является одним из перспективных направлений вышеупомянутой задачи. Однако в СОК существует ряд вычислительно сложных немодульных операций. Для их эффективной реализации необходимо решить дополнительную нетривиальную задачу оптимального выбора параметров немодульных операций и разработки общего метода, позволяющего увеличить скорость выполнения немодульных операций в задачах обработки информации. Все вышесказанное обуславливает несомненную актуальность темы диссертационной работы.

Структура и содержание диссертации. Диссертация состоит из введения, трех глав, заключения, списка литературы, включающего 119 использованных источников, и семи приложений. Общий объем работы составляет 167 страниц.

Во введении показана актуальность темы диссертации, сформулированы цель и основные задачи работы, обоснованы научная новизна и практическая значимость результатов проведенного исследования, представлены основные положения, выносимые на защиту.

Первая глава посвящена методам шифрования, которые могут быть применены на маломощных устройствах. В частности, особое внимание уделено возможности применения СОК для повышения скорости рассматриваемых алгоритмов шифрования. Показано, что применение методов и алгоритмов выполнения модульных операций СОК, а также немодульных операций на основе функции ядра Акушского позволяет повысить скорость выполнения алгоритмов шифрования на вычислительных узлах туманной платформы.

Во второй главе разработаны математические методы и алгоритмы оптимизации модулярных вычислений в СОК. Разработан алгоритм для определения критических ядер функции ядра Акушского. Рассмотрена задача обратного преобразования чисел из СОК в позиционную систему счисления. Предложен метод, использующий Китайскую теорему об остатках (КТО) и ранг числа, вычисляемый с помощью функции ядра. Доказано равенство рангов числа, определенного на основе КТО и функции ядра Акушского, при отсутствии критических ядер. Изучены методы определения знака числа в СОК,

основанные на КТО, приближенном методе на базе КТО, обобщенной позиционной системе и диагональной функции. Разработаны минимальные функции ядра Акушского для специальных наборов модулей, позволяющие сократить размеры операндов и выполнять операции по модулю 2^N , что дает преимущество перед классическими методами. Рассмотрен алгоритм сравнения чисел с использованием функции ядра Акушского и проблема монотонности функции ядра, необходимая для корректного сравнения чисел в СОК. Разработан метод построения функции ядра Акушского для операций сравнения чисел.

В третьей главе разработаны алгоритм построения компактных базисов СОК и алгоритмы поиска оптимальных весов функции ядра Акушского. Продемонстрированы их преимущества в сравнении с алгоритмами подобного назначения. Предложена архитектура программного комплекса для реализации высокоскоростных вычислительных систем на основе модулярной арифметики. Программный комплекс предназначен для работы в распределенных туманных средах. В рамках данного программного комплекса реализованы разработанные модель, методы и алгоритмы. Проведены вычислительные эксперименты с целью оценки эффективности выполнения модульных и немодульных операций в СОК.

В заключении представлены основные результаты диссертации, проведено их обсуждение, сформулированы выводы об эффективности их использования и намечены возможные направления дальнейших исследований.

Автореферат адекватно отражает структуру и содержание диссертации в целом.

Соответствие паспорту научной специальности. Судя по тексту диссертации, тема, содержание и основные результаты работы в полной мере соответствуют областям исследования паспорта специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Научная новизна диссертационной работы заключается в том, что:

- 1) Разработаны оригинальные алгоритмы выбора оптимальных параметров функции ядра Акушского для вычисленных компактных базисов СОК.
- 2) Модифицированы методы и алгоритмы перевода из СОК в позиционную систему счисления, деления, определения знака и сравнения чисел в СОК, отличающиеся от известной меньшей размерности операндов и эффективной реализацией операций без необходимости нахождения остатка по большому модулю, за счет выбора оптимальных параметров функции ядра Акушского.
- 3) Разработан новый программный комплекс для выполнения немодульных операций в туманных узлах, позволяющий повысить скорость распределенной обработки данных в туманных вычислениях.

Теоретическая значимость. Разработанные математическая модель, методы и алгоритмы в совокупности представляют теоретическую базу для оптимизации вычислительно сложных процедур модулярного кода и достижения высокой скорости работы вычислительных узлов при выполнении модулярной арифметики в рамках туманных вычислений.

Практическая значимость. Результаты диссертации использованы в рамках ряда проектов Российского научного фонда. Отдельные результаты получены при поддержке Минобрнауки РФ. Их практическая ценность состоит в ускорении процессов обработки

данных с помощью ограниченных вычислительных ресурсов облачных и туманных структур. Результаты диссертации могут быть применены в таких направлениях исследований, как криптография и искусственные нейронные сети.

Достоверность и обоснованность научных результатов диссертационной работы обеспечиваются корректным применением математических моделей, методов анализа, теории чисел и численных методов, а также подтверждаются экспериментальными расчетами, сравнением с известными теоретическими оценками и результатами сравнительного анализа предложенных методов с существующими аналогами.

Апробация. Основные результаты диссертации отражены в двадцати четырех публикациях, включая пять работ в журналах, рекомендованных ВАК РФ, две статьи в изданиях, входящих в международные базы цитирования Web of Science и Scopus, а также девять публикаций в трудах конференций. Получено восемь свидетельств о государственной регистрации программ для ЭВМ. Указанный личный вклад автора не вызывает сомнений.

Замечания. Диссертация производит самое благоприятное впечатление. Вместе с тем хотелось бы высказать следующие замечания:

1) При формулировании научной новизны, в некоторых случаях автор делает акцент не на новизну или характерную особенность разработанных теоретических элементов, а на новые эффекты, которые достигаются за счет использования указанных теоретических элементов.

2) В третьей главе представлен программный комплекс программного обеспечения, предназначенный для работы в распределенных туманных средах. Однако вычислительные эксперименты проведены в режиме моделирования на одном отдельно взятом узле. Проведение более масштабного эксперимента применительно к решению ряда задач, различающихся объемом и структурой потока данных, требуемым уровнем их безопасности и другими характеристиками, позволило бы более адекватно оценить преимущества разработанных модели, методов и алгоритмов.

3) К сожалению, в работе не затронуты вопросы отказоустойчивости вычислительной системы, которая работает в модульном коде в рамках распределенной туманной среды. Было бы полезно оценить возможные накладные расходы на поддержку отказоустойчивости подобной системы в такой среде.

4) Также стоило рассмотреть вопросы распределения обработки потока данных в распределенной туманной среде с разнородными узлами с целью согласования времени, стоимости и надежности вычислений с эффективностью использования узлов среды и балансировки вычислительной нагрузки.

Указанные замечания не являются критическими и ни в коей мере не ставят под сомнение положительную оценку диссертационной работы, ее высокий научный уровень и практическую значимость.

Заключение. Диссертационная работа Луценко Владислава Вячеславовича выполнена на высоком научном уровне по актуальному направлению исследований. Ее содержание полностью соответствует поставленным целям и задачам, обладает внутренним единством и правильно отражает логическую последовательность выполнения основных этапов исследования. Диссертация изложена в хорошем научном

стиле, ясно и доказательно. Основные результаты, положения и выводы диссертации являются достоверными и обоснованными.

В целом диссертация Луценко Владислава Вячеславовича является самостоятельно подготовленной, завершенной научно-квалификационной работой, в которой на основании выполненных автором исследований решается актуальная задача исследования и разработки математических методов и алгоритмов выполнения вычислительно сложных операций СОК на основе функции ядра Акушского, способных повысить скорость при выполнении алгоритмов шифрования вычислительными узлами туманной среды, работающими в системе остаточных классов.

Считаю, что диссертация соответствует всем требованиям Положения ВАК РФ о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а ее автор, Луценко Владислав Вячеславович, заслуживает присуждения ему искомой ученой степени кандидата физико-математических наук по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Официальный оппонент

заведующий лабораторией параллельных и
распределенных вычислительных систем,
ФГБУН Институт динамики систем и теории
управления имени В.М. Матросова Сибирского
отделения Российской академии наук,
доктор технических наук, доцент

Феоктистов А.Г.

Согласен на обработку персональных данных
доктор технических наук, доцент

Феоктистов А.Г.

Контактные данные организации: Федеральное государственное бюджетное учреждение науки Институт динамики систем и теории управления имени В.М. Матросова Сибирского отделения Российской академии наук (ИДСТУ СО РАН), 664033, г. Иркутск, ул. Лермонтова, д. 134, e-mail: info@idstu.sci.ru, тел.: +7 (3952) 42-71-00

31.10.2025