

УТВЕРЖДАЮ
Первый проректор,
~~доктор технических наук~~
___А.В. Метелица

23

10 ____ 2025 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного автономного образовательного
учреждения высшего образования

«Южный федеральный университет» (ЮФУ)

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 учёной степени кандидата физико-
математических наук по специальности 2.3.5. Математическое и
программное обеспечение вычислительных систем, комплексов и
компьютерных сетей

Диссертационная работа Луценко В.В. посвящена повышению скорости работы узлов туманных вычислений в алгоритмах шифрования за счет оптимизации вычислительно сложных процедур модулярного кода и разработки программного обеспечения для их проектирования. Исследованы модулярные и немодулярные операции системы остаточных классов (СОК), изучена проблема выбора набора модулей, сравнения чисел и определения знака числа, деления чисел в СОК. На основе разработанных методов и алгоритмов возможна разработка программных средств реализации распределенной обработки данных в туманных вычислениях, характеризующихся высокой скоростью, которая достигается за счет модификации алгоритмов модулярной арифметики. Полученные результаты могут быть использованы в облачных и туманных структурах, работающих в условиях ограниченных вычислительных ресурсов.

Актуальность темы диссертационной работы

Развитие распределенных и, в частности, облачных вычислений сталкивается со сложностью обработки информации в реальном времени, что связано с большими нагрузками и задержками каналов связи. Для решения этой проблемы предложено переносить вычисления ближе к источнику данных, что привело к появлению туманных и граничных вычислений, которые позволяют снизить задержки и уменьшить нагрузку на облачные серверы. Однако, обеспечение безопасности гетерогенных туманных узлов является сложной задачей из-за их ограниченных вычислительных ресурсов, что не позволяет реализовать полноценную криптографическую защиту. Одним из подходов к увеличению скорости вычислений является применение системы остаточных классов, которая за счет параллельной структуры позволяет значительно ускорить выполнение арифметических операций. Кроме того, в ряде источников говорится, что СОК позволяет также снизить энергопотребление вычислительных узлов, что актуально для IoT устройств туманных систем, работающих автономно. Однако, СОК требует адаптации к туманным вычислениям как своей структуры, связанной с набором используемых модулей, так и реализации модульных и немодульных операций.

В связи с этим диссертационная работа В.В. Луценко посвящена решению актуальной задачи – исследованию и разработке 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.

Структура и основное содержание диссертационной работы

Диссертация имеет логичную структуру, что даёт возможность последовательно и полно исследовать предложенные в работе методы и алгоритмы. Диссертация состоит из введения, 3 глав, заключения, списка литературных источников из 119 наименований, и 7 приложений. Общий объём основного текста работы – 167 страниц, включая 42 таблицы и 18 рисунков.

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

В первой главе описана архитектура распределённой обработки данных в туманных вычислениях и рассмотрены криптографические методы обеспечения безопасности. Исследована возможность применения СОК для повышения скорости алгоритмов шифрования в туманных вычислениях, а также проблемы модулярной арифметики. На основе данного анализа сформулирована научная задача исследования: исследование и разработка 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.

Во второй главе рассмотрены реализации немодульных операций в СОК, а именно определения позиционной характеристики числа в СОК с использованием функции ядра Акушского. Исследованы методы определения критических ядер функции ядра, что позволило производить корректное вычисление позиционной характеристики. Предложен алгоритм, основанный на Китайской теореме об остатках (КТО) и ранге числа в СОК с использованием функции ядра. Доказано равенство рангов числа, определенного на основе КТО и функции ядра Акушского, при отсутствии критических ядер. Рассмотрено применение функции ядра к итерационному делению в СОК. Разработаны минимальные функции ядра Акушского с заданными свойствами для специальных наборов модулей, которые применяются для задачи определения знака в СОК. Для проблемы сравнения чисел предложен метод построения функции ядра со специальным ядром, равным степени 2, что позволило заменить операцию нахождения остатка от деления взятием младших бит числа. Таким образом, представлены методы реализации всех ключевых немодульных операций, необходимых для построения туманных вычислительных систем, работающих в системе остаточных классов.

В третьей главе представлена реализация разработанных во второй главе методов и алгоритмов в виде программного обеспечения, предназначенного для работы в распределённых туманных средах. Предложена архитектура программного комплекса для проектирования высокоскоростных вычислительных систем на основе модулярной арифметики. Архитектура программного комплекса включает модули выбор базиса СОК, поиска оптимальных весов для функции ядра Акушского, модулярных вычислений и вычисления позиционной характеристики для немодульных операций СОК. Проведено исследование эффективности наборов модулей специального вида СОК: $\{2^n - 1, 2^n, 2^n + 1\}$ и $\{2^n - 1, 2^n, 2^n + 1, 2^{n+1} - 1\}$. Предложен алгоритм построения компактных

базисов с использованием теоремы Диемитко. Рассмотрено моделирование модулярного сложения и умножения в СОК с использованием компактных базисов, что позволило получить выигрыш по скорости более 35% по сравнению с использованием библиотек NTL и MIRACL. Предложены алгоритмы поиска оптимальных весов для функции ядра с использованием метода Монте-Карло и генетического алгоритма.

Предложенный алгоритм обратного преобразования из СОК в позиционную систему счисления, основанный на использовании КТО и ранга числа функции ядра Акушского, в среднем на 10.5% быстрее метода на основе КТО при фиксированном количестве модулей и на 7.2% быстрее при динамическом изменении числа модулей.

Для оптимизации итерационного деления использованы новые методы вычисления функции ядра от половины числа. В результате, итерационное деление с вычислением функции ядра от половины числа оказалось на 12.2% быстрее классического итерационного деления.

Разработаны алгоритмы определения знака числа в СОК на основе минимальной функции ядра для наборов модулей $\{2^n - 1, 2^{n+a}, 2^n + 1\}$ и $\{2^n - 1, 2^{n+1} - 1, 2^{n+a}\}$, которые позволили повысить скорость в среднем на 17% по сравнению с известными методами.

Проведено моделирование методов сравнения чисел в СОК. Разработанный метод построения функций ядра Акушского для операции сравнения чисел в СОК позволил увеличить скорость сравнения в среднем на 15.1% по сравнению с классическими методами.

Также в третьей главе разработан программный комплекс для выполнения модульных и немодульных операций в СОК. Предложенный комплекс может быть использован в облачных и туманных структурах, работающих в условиях ограниченных вычислительных ресурсов.

В заключении подведены итоги и обобщены результаты проведенных исследований. **В приложениях** представлены результаты моделирования и свидетельства о государственной регистрации программ для ЭВМ.

Основные результаты диссертационной работы

В диссертационной работе Луценко В.В. получены следующие результаты:

1. Разработан метод для перевода из СОК в ПСС на основе КТО и ранга числа функции ядра Акушского, который за счет ухода от операции нахождения остатка от деления позволяет сократить время вычислений по сравнению с методом на основе Китайской теоремы об остатках и с приближённым методом на основе Китайской теоремы об остатках.

2. Разработаны модифицированные методы итерационного деления в СОК. Данные методы позволяют повысить скорость вычислений по сравнению с классическим итерационным делением за счет вычисления функции ядра на основе её значения для предыдущего частного.

3. Разработаны алгоритмы определения знака на основе минимальной функции ядра Акушского с заданными свойствами для специальных наборов модулей. Эти алгоритмы позволяют за счет уменьшения размера операндов и снижения вычислительной сложности операции нахождения остатка от деления с $O(n^2)$ до $O(n)$ повысить скорость определения знака по сравнению с классическими методами.

4. Разработан метод построения функций ядра Акушского для операции сравнения чисел. Сравнение чисел в СОК на основе построенных минимальных функций ядра Акушского, у которых $C(P) = 2^N$, позволяет повысить скорость вычислений за счет снижения размера операндов, а также замены операции нахождения остатка от деления взятием N младших бит числа.

5. Разработан алгоритм построения компактных базисов системы остаточных классов. Наборы базисов, полученные данным алгоритмом, позволяют снизить время выполнения модульных операций в СОК по сравнению с использованием модулей специального вида за счет большей степени параллелизма и соответствия критерию компактности.

6. Разработаны алгоритмы поиска оптимальных весов функции ядра Акушского. Использование генетического алгоритма для решения задачи поиска оптимальных весов функции ядра позволило сократить время поиска на 71.2% по сравнению с методом Монте-Карло. Для задач с большим числом модулей в системе остаточных классов целесообразнее использовать генетический алгоритм, который демонстрирует лучшее время выполнения, несмотря на возрастающую сложность задачи.

7. Разработан программный комплекс для выполнения модульных и немодульных операций в СОК на вычислительных узлах туманных сред. Комплекс показал высокую эффективность при выполнении указанных операций. Представленные вычислительные модули могут быть применены в облачных и туманных системах, работающих в условиях ограниченных вычислительных ресурсов.

Достоверность полученных результатов

Достоверность полученных в диссертации результатов подтверждается проведенным сравнительным анализом разработанных методов и алгоритмов с известными ранее с точки зрения скорости обработки данных. Результаты

диссертационного исследования прошли апробацию на конференциях и научных мероприятиях всероссийского и международного уровней, а также в научных публикациях, среди которых 5 в рецензируемых журналах, рекомендованных ВАК и 9 публикаций, индексируемых в базах научных работ Scopus и Web of Science. Кроме того, получено 8 свидетельств о государственной регистрации программ для ЭВМ.

Практическая значимость

Разработанные методы и алгоритмы позволяют повысить скорость обработки данных в туманных вычислениях за счет использования модулярной арифметики. Результаты исследования могут быть применены в облачных и туманных структурах, работающих в условиях ограниченных вычислительных ресурсов. Кроме того, разработанные методы и программные средства могут быть применены в других областях, где требуется параллельная реализация арифметических операций с числами большой разрядности.

Замечания

1. Название диссертационной работы включает разработку математической модели, однако ни в задачах, ни в положениях, выносимых на защиту математическая модель явным образом не описана.

2. В конце пункта 1.4.2, описывая преимущества СОК, автор указал наличие входного преобразования, подразумевая его модульные свойства и возможность параллельной реализации. Однако, сама необходимость прямого преобразования уже является недостатком СОК, требующими дополнительного времени перед основными вычислениями, которое необходимо учитывать при моделировании алгоритмов.

3. Подводя выводы по первой главе, автор формулирует научную задачу, в которой планирует повышать скорость вычислительно сложных операций в СОК на основе функции ядра Акушского, однако определения функции ядра и возможности ее применения для повышения скорости вычислений в первой главе не раскрыты.

4. В пункте 2.4. упоминается деление на 2, однако не описано, как оно производится в СОК. Процедура итерационного деления, представленные алгоритмы и пример имеют разные обозначения и порядок действий, что затрудняет понимание используемого подхода.

5. В утверждениях 2.5.2, 2.5.3 не указан исследуемый набор модулей.

6. Исследуемые в пункте 3.2.1 наборы модулей, приведенные в таблице 21 приложения Б, не являются взаимно простыми. Это относится к наборам $\{3, 4, 5, 9\}$, $\{15, 16, 17, 33\}$ и другим из указанной таблицы.

7. В диссертации имеются опечатки, пунктуационные ошибки, которые не влияют на понимание сути исследования. В частности, в таблице 1 «выбор параметров», в примере 2.3.3 «коэффициенты равны», написаны с ошибкой. В примере 2.5.1 в «используя (1.3)» пропущено слово «выражение». В Алгоритме 7 на шаге 6 вычитаемое необходимо умножить на P . Поскольку и в формуле (2.21), и в примере 2.3.5 данное умножение есть, в данном случае это опечатка.

Заключение

Указанные замечания не снижают научную и практическую ценность диссертационной работы и проведенных исследований. Диссертация является законченным научным исследованием, написанном на высоком уровне. Результаты диссертационного исследования представлены в статьях автора, а также докладывались на всероссийских и международных конференциях. Автореферат диссертации правильно и полно отражает содержание работы и оформлен надлежащим образом.

Диссертационная работа Владислава Вячеславовича Луценко соответствует требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а её автор, Владислав Вячеславович Луценко, заслуживает присуждения учёной степени кандидата физико-математических наук по этой специальности.

Отзыв подготовлен профессором кафедры прикладной математики и программирования, доктором технических наук (05.13.18. Математическое моделирование, численные методы и комплексы программ) Анатолием Борисовичем Усовым (344090, Ростов-на-Дону, ул. Мильчакова, 8А, тел. раб. +7(863)2975411, эл. почта: abusov@sfedu.ru).

Отзыв обсуждён и утверждён на заседании кафедры прикладной математики и программирования Института математики, механики и компьютерных наук им. И.И. Воровича Южного федерального университета от 28 октября 2025 г., протокол №4. Присутствовало на заседании 8 чел.

Результаты голосования: «за» – 8 чел., «против» – нет, «воздержались» – нет.

Заведующий кафедрой прикладной математики и программирования
Института математики, механики и компьютерных наук им. И.И. Воровича
ФГАОУ ВО «Южный федеральный университет»,

д.ф.-м.н., профессор

Г.А. Угольников

344090, г.Ростов-на-Дону, ул. Мильчакова, 8А
тел. раб. +7(863)297-54-11, e-mail: gaugolnickiy@sfedu.ru

Сведения об организации:

Федеральное государственное автономное образовательное учреждение
высшего образования «Южный федеральный университет»

Адрес: 344006 г. Ростов-на-Дону, ул. Б. Садовая, 105/42

Телефон: +7 (863) 218 40 00

E-mail: info@sfedu.ru

Веб-сайт: <https://www.sfedu.ru>

 20-21 г.