«УТВЕРЖДАЮ»

Директор ОИЯИ

_____Трубников Г.В.

« 18 » ноября 2022 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

На диссертационную работу Бабенко Михаила Григорьевича «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах», представленную на соискание ученой степени доктора физико-математических наук по специальности 2.3.5 (05.13.11) – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертация Бабенко М.Г. носит теоретический характер и направлена на разработку математических моделей, методов и алгоритмов обработки зашифрованных конфиденциальных данных с использованием гомоморфных вычислений в распределенных вычислительных системах.

Актуальность проведенного исследования обусловлена тем, что имеющиеся разработки не могут полностью решить проблему повышения эффективности и надежности процессов обработки конфеденциальных данных в распределенных средах. Системы распределенного хранения и обработки данных обладают рядом достоинств, но их использование может привести к проблемам, связанным с надежностью представления данных, такими как потеря, искажения или кража. Они должны обеспечивать баланс между вычислительной сложностью алгоритмов, используемых в системе, и сохранением конфиденциальности данных. Поэтому разработка фундаментальных основ для проектирования систем обработки и хранения конфиденциальных данных в гетерогенных средах является актуальным направлением исследований по повышению качества облачных сервисов.

Целью работы 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.

Анализ содержания работы

Общий объем диссертации составляет 415 страниц. Основной текст диссертации изложен на 321 страницах, включая 42 рисунка и 35 таблиц. Работа состоит из введения, шести глав, заключения, библиографии из 374 наименований и 2 приложений.

Во Введении обоснованы актуальность, новизна и практическая значимость диссертационного исследования, сформулированы его цели и задачи. Также в данном разделе изложены основные результаты исследования, представлена его структура и дано краткое содержание по главам.

В первой главе дан обзор угроз информационной безопасности в современных распределенных системах хранения и обработки данных. Построена структурная модель обработки данных в распределенных средах и показано, что в условиях повышенной неопределенности известные фундаментальные подходы к снижению рисков конфиденциальности, целостности и доступности недостаточно эффективны и должны быть усовершенствованы. Предложено использование концепции мультиоблачного хранения и обработки данных. Проведен анализ структур доступа, на основании которого выбран алгоритм реализации пороговых структур доступа и представлена его модификация.

Во второй главе предложена адаптивная распределенная служба хранения WA-MRC-RRNS, которая производит гомоморфное отображение. Данная служба использует взвешенную пороговую структуру доступа. Доказана теорема о том, что вероятность потери данных при использовании такой взвешенной пороговой структуры доступа не превышает вероятности потери данных при использовании соответствующей классической пороговой структуры доступа. В качестве основы для предложенной взвешенной пороговой структуры доступа выбрана избыточная система остаточных

классов. Предлагаемая схема превосходит известные аналоги и соответствует требованиям, предъявляемым к гомоморфным кодам.

Третья глава посвящена исследованию различных подходов к реализации вычислительно сложных операций в кольце вычетов с делителями нуля, таких как определение знака числа, сравнение чисел и обратное преобразование из системы остаточных классов в позиционную систему счисления. Разработаны алгоритмы определения знака числа и сравнения чисел для гомоморфных вычислений над кольцом вычетов с делителями нуля на основе системы остаточных классов. В частности, в работе предложено устройство сравнения чисел на основе модифицированной диагональной функции, которое показывает преимущество в скорости работы и требуемых аппаратных затратах по сравнению с известными аналогами. Кроме того, исследована функция ядра Акушского, сформулирована и доказана теорема об условиях отсутствия критических ядер функции ядра. Показано, что функция ядра Акушского является обобщением позиционных характеристик чисел, и ее дальнейшее исследование открывает возможности к проектированию более высокопроизводительных методов.

Четвертая глава посвящена разработке и оптимизации методов и алгоритмов определения знака и сравнения гомоморфно закодированных чисел над полем. Построены многочлены, использующие интерполяционные многочлены Лагранжа, которые позволяют определять знак числа и сравнивать числа над полем целых чисел. Сформулированы и доказаны теоремы, дающие оценку степени интерполяционного многочлена функций определения знака числа и сравнения чисел. Построены аппроксимирующие многочлены для функции определения знака числа, а также предложен нейросетевой метод определения знака числа над полем действительных чисел.

В пятой главе рассматриваются методы повышения производительности алгоритмов обнаружения и исправления арифметических ошибок обработки закодированных данных с использованием свойств ранга числа. Проведено

исследование возможности интерполяции ранга числа с помощью алгебраических многочленов. Предложены новые высокопроизводительные методы вычисления ранга числа.

В шестой главе представлены разработанные методы повышения надежности систем обработки конфиденциальных данных с использованием двухуровневой избыточной системы остаточных классов. Предлагаемая автором конфигурируемая масштабируемая двухуровневая пороговая структура доступа с обратным распространением ошибки на основе избыточной системы остаточных классов и использующая механизмы обратного распространения ошибки и расстояние Хэмминга обеспечивает надежное и безопасное хранение данных в мультиоблачных системах. Сравнение предлагаемого подхода с известными аналогами и показало, что предложенная схема обладает лучшими корректирующими свойствами.

В Заключении изложены краткие выводы по основным результатам диссертационного исследования.

Диссертационная работа оформлена в соответствии с требованиями и хорошо структурирована. Прослеживается логичная последовательность изложения материала, сопровождаемая иллюстрациями, что делает текст ясным и понятным. Автореферат полностью соответствует содержанию диссертационной работы.

Оценка новизны, обоснованности и научной значимости результатов

Предложенные в диссертационной работе модели, методы и алгоритмы повышения эффективности систем надежного хранения и обработки конфиденциальных данных в распределенных средах в условиях нестабильной работы сервисов являются новыми.

Обоснованность представленных в работе результатов обеспечивается строгостью математических доказательств и результатами экспериментов.

Диссертация носит теоретический характер, при этом представленные в работе результаты по повышению эффективности систем распределенной

обработки конфиденциальных данных в современных распределенных вычислительных системах имеют несомненную практическую значимость.

Публикации и конференции

Основные результаты диссертационного исследования были использованы в ряде научно-технических работ, представлены на российских и международных конференциях, отражены в большом количестве научных проектов и публикаций, представлены на всероссийских и международных конференциях.

Основные результаты по теме диссертационного исследования были опубликованы в 89 научных работах. Из них 36 научных статей опубликованы в журналах из списка, рекомендованного ВАК, или индексируемых в международных базах Scopus и/или Web of Science. Кроме того, по теме исследования получено 26 свидетельств о государственной регистрации программ для ЭВМ и 12 патентов на изобретения.

Замечания по диссертации

1) В разделе «Введение» расшифрованы не все аббревиатуры, что затрудняет восприятие текста. При таком большом объеме работы и обилии аббревиатур желательно было бы составить и включить в работу список аббревиатур и обозначений с расшифровкой.
2) Поскольку работа носит теоретический характер, было бы полезно расширить рекомендации по применению предлагаемых решений на практике и разъяснить накладываемые на них ограничения.
3) В тексте имеются незначительные опечатки итехнические недостатки оформления. Так, для написания степенных функций наряду со стандартным видом «…$^{+10}$» в некоторых таблцах используется форма «…E+10». Также, десятичная запятая должна обозначаться символом «,» вместо «.».

Заключительная оценка

Диссертационная работа «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах» соответствует

требованиям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени доктора наук, а ее автор, Бабенко Михаил Григорьевич, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.5 (05.13.11) – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей.

Отзыв составлен доктором технических наук Кореньковым Владимиром Васильевичем, директором Лаборатории информационных технологий имени М.Г. Мещерякова Объединенного института ядерных исследований.

Отзыв рассмотрен и утвержден на заседании Общелабораторного семинара Лаборатории информационных технологий им. М.Г. Мещерякова 13 октября 2022 г., протокол № 1 от 13 октября 2022 г.

Сведения о ведущей организации: Международная межправительственная организация Объединенный институт ядерных исследований

Адрес: 141980, Россия, Московская обл., г. Дубна, ул. Жолио-Кюри, 6

Электронная почта: post@jinr.ru

Телефон: +7(496)216-50-59 (секретариат)

ОКПО 08626319; ОГРН 1035002200221

ИНН/КПП 9909125356/501063001

Отзыв составил:

Директор ЛИТ им. М.Г. Мещерякова ОИЯИ,
доктор технических наук

/Кореньков В.В./