ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

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

Актуальность темы исследования. Диссертационная работа Бабенко Михаила Григорьевича направлена на разработку теоретических основ для построения систем удаленного распределенного хранения и обработки конфиденциальных данных. Важнейшими проблемами при построении систем, реализующих данный функционал, являются обеспечение надежности, конфиденциальности и эффективности хранения и обработки данных. Стандартные методы шифрования способны обеспечить конфиденциальность данных при хранении, но не допускают удаленной обработки данных. Поэтому в современных распределенных системах используются методы обработки, не требующие предоставления прозрачного доступа к данным. Подобные методы реализуются посредством инструмента гомоморфных вычислений, основным недостатком которого является большая вычислительная сложность. В работе предложена концепция мультиоблачного хранения и обработки данных, согласно которой программно объединяются ресурсы сразу нескольких вычислительных центров, и таким образом решается проблема уменьшения вычислительной сложности при организации гомоморфных вычислений.

Объединение ресурсов нескольких вычислительных центров открывает новые возможности с точки зрения производительности, но при этом возрастает количество компонентов, узлов, подсистем и т.д., каждый из которых является потенциальной причиной отказа и объектом кибератаки, что в совокупности порождает повышение неопределенности возникновения технических сбоев и хакерских атак. Наличие в работе новых подходов к оценке надежности и конфиденциальности хранимых и обрабатываемых данных в условиях повышенной неопределенности, соответствующих методов и алгоритмов, а также методов гомоморфной реализации операций,

расширяющих функционал гомоморфных вычислений, определяет высокую актуальность темы диссертационного исследования М.Г. Бабенко.

Теоретическая и практическая значимость полученных результатов, их научная новизна. В рамках вышеописанной общей проблемы поставлен ряд частных задач, решение которых оформлено в виде основных научных результатов, выносимых на защиту. Среди них можно выделить:

– структурную модель обработки данных в распределенных средах, объединяющую в себе краевые, туманные и облачные вычисления;

– адаптивную распределенную службу хранения WA-MRC-RRNS, основанную на избыточной системе остаточных классов (RRNS), которая сочетает в себе функционал взвешенной пороговой структуры доступа и системы контроля корректности результатов обработки данных с сохранением их конфиденциальности;

– алгоритмы, реализующие определение знака числа над кольцом вычетов с делителями нуля;

– метод сравнения чисел над кольцом вычетов, использующий введенное понятие модифицированной диагональной функции (MDF);

– теорему об условиях отсутствия критических ядер функции ядра Акушского, имеющую важное практическое значение для построения эффективных позиционных характеристик чисел, представленных в RNS;

– многочлены, позволяющие определять знак числа и сравнивать числа над полем Z_m с оценками их степеней;

– аппроксимирующие многочлены наилучшего приближения для функции определения знака числа над полем R при гомоморфизме колец;

– модифицированный нейросетевой метод определения знака числа над полем R;

– метод вычисления ранга числа, основанный на использовании функции ядра Акушского, не содержащей критических ядер;

– алгоритмы вычисления ранга числа, представленного в RNS, и теоремы, позволяющие осуществлять контроль результатов обработки закодированных чисел с использованием арифметических свойств классического и нормализованного рангов;

– конфигурируемую масштабируемую двухуровневую структуру доступа с обратным распространением ошибки на основе RRNS (2Lbp-RRNS);

– эффективные реализации алгоритмов кодирования и декодирования данных в 2Lbp-RRNS.

Все перечисленные результаты, полученные в рамках диссертационной работы, являются новыми и оригинальными.

Диссертант характеризует свою работу как теоретическую, что обоснованно, однако следует отметить, что большинство полученных научных результатов имеют ярко выраженное прикладное назначение.

Представленное в диссертационном исследовании теоретическое обоснование надежности и вычислительной стойкости предложенной адаптивной распределенной службы хранения WA-MRC-RRNS, сочетающей в себе функционал взвешенной пороговой структуры доступа и системы контроля корректности результатов обработки данных, является теоретической основой для реализации нестандартного перспективного подхода к гомоморфным вычислениям, основанного на системе остаточных классов. Предложенный подход к реализации удаленной обработки конфиденциальных данных позволяет расширить схемы гомоморфных вычислений, как правило, поддерживающие операции сложения и умножения, операциями определения знака и сравнения, которым посвящена значительная часть диссертационного исследования. Научная значимость этого результата состоит, во-многом, в его прикладной ценности.

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

Достоверность и обоснованность научных положений, выводов и рекомендаций подтверждена корректным применением выбранных методов исследования, строгими доказательствами математических утверждений и анализом эффективности разработанных моделей и алгоритмов. Результаты численных экспериментов в полной мере коррелируют с теоретическими выводами. Обоснованность положений, выносимых на защиту, подтверждается достоверностью полученных результатов и соответствием современному уровню научного знания в соответствующих областях математики и информатики.

Структура диссертации. Диссертация состоит из Введения, 6-ти Глав, Заключения, библиографии из 374 источников и 2-х приложений. Общий объем основного текста работы – 321 страница, включая 35 таблиц и 43 рисунка. Автореферат корректно и в полном объеме отражает содержание работы, в нем изложены основные положения и результаты диссертации.

Апробация результатов работы. Основные результаты диссертационного исследования прошли апробацию на научных мероприятиях в России и за рубежом. Среди российских конференций можно выделить: 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. Среди международных симпозиумов можно выделить: 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).

Всего по теме диссертационного исследования автором было опубликовано 89 статей, в том числе 36 статей в журналах из списков ВАК/Scopus/Web of Science. 53 публикации вышли в трудах российских и международных конференций. Получено 26 свидетельств о государственной регистрации программ для ЭВМ и 12 патентов на изобретения.

Высокий индекс цитируемости журналов (многие уровня Q1) и уровень конференций (некоторые ранга CORE Rank A), в которых опубликованы научные статьи диссертанта, говорит о высоком уровне научной значимости и качестве результатов выполненных исследований.

Основные результаты диссертационного исследования были использованы в рамках 12-ти научно-технических работ, среди которых проекты: Министерства науки и высшего образования Российской Федерации, Российского научного фонда, Российского фонда фундаментальных исследований, Совета по грантам Президента Российской Федерации. Диссертация не содержит заимствованных материалов или отдельных результатов без ссылок на авторов и источники заимствования.

Тематика работы 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»: п. 3 «Модели, методы, архитектуры, алгоритмы, языки и программные инструменты организации взаимодействия программ и программных систем»; п. 8 «Модели и методы создания программ и программных систем для параллельной и распределенной обработки данных, языки и инструментальные средства параллельного программирования»; п. 9 «Модели, методы, алгоритмы, облачные технологии и программная инфраструктура организации глобально распределенной обработки данных».

Замечания.

1. В Главе 3 при построении примеров, демонстрирующих корректность предложенных методов гомоморфного сравнения, для большей наглядности целесообразно было бы использовать числа, расположенные рядом в рассматриваемой алгебраической структуре.

2. Имеется ряд пунктуационных неточностей при оформлении списка публикаций автора.

Указанные замечания не являются критическими и не снижают научную и практическую ценность проведенных исследований.

Заключение.

Диссертационная работа Михаила Григорьевича Бабенко представляет собой завершенное научное исследование в рамках сложнейшей проблемы организации эффективного, надежного и безопасного удаленного

распределенного хранения и обработки конфиденциальных данных, в ней решены важные научные задачи. Совокупность разработанных теоретических положений можно квалифицировать как новое достижение в этой области. Диссертация и автореферат написаны понятным языком, имеют четкую структуру, внутреннее единство содержания, смысла и терминологии.

Диссертационная работа отвечает требованиям ВАК РФ, предъявляемым к докторским диссертациям по специальности 2.3.5 (05.13.11) – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а ее автор, Бабенко Михаил Григорьевич, заслуживает присуждения ученой степени доктора физико-математических наук по вышеуказанной специальности.

Доктор технических наук (специальность 05.13.15 «Вычислительные машины, комплексы и компьютерные сети»), член-корреспондент РАН,
заместитель директора по научной работе – директор Межведомственного суперкомпьютерного центра академии наук – филиала Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (МСЦ РАН – филиал ФГУ ФНЦ НИИСИ РАН)

Шабанов Борис Михайлович

«18» ноября 2022 г.