ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного на базе
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Министерства науки и высшего образования РФ
по диссертации на соискание ученой степени доктора наук

аттестационное дело № _____

решение диссертационного совета от 08 декабря 2022 года № 2022/11

О присуждении Бабенко Михаилу Григорьевичу, гражданину РФ, ученой степени доктора физико-математических наук.

Диссертация «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах» по специальности 2.3.5 – «математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 08 сентября 2022 года, протокол № 2022/02 диссертационным советом 24.1.120.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Бабенко Михаил Григорьевич, 1985 года рождения.

Диссертацию на соискание ученой степени кандидата физико-математических наук «Методы и алгоритмы моделирования вычислительных структур на эллиптических кривых с параллелизмом машинных операций» защитил в 2011 году в диссертационном совете, созданном на базе Государственного образовательного учреждения высшего профессионального образования «Ставропольский государственный университет».

Работает научным сотрудником в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25).

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25).

Научный консультант – доктор физико-математических наук, академик РАН, Аветисян Арутюн Ишханович, Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук, директор.

Официальные оппоненты:

1. Логачев Олег Алексеевич, доктор физико-математических наук, член-корр. Академии криптографии РФ, доцент кафедры информационной безопасности Факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский Государственный Университет им. М.В. Ломоносова»,
2. Ильин Вячеслав Анатольевич, доктор физико-математических наук, главный научный сотрудник Курчатовского комплекса НБИКС-природоподобных технологий Федерального государственного бюджетного учреждения «Национальный исследовательский центр «Курчатовский институт»,
3. Шабанов Борис Михайлович, доктор технических наук, член-корр. РАН, директор Межведомственного Суперкомпьютерного Центра РАН, заместитель директора по научной работе Федерального государственного учреждения «Федеральный научный центр Научно-

исследовательский институт системных исследований Российской академии наук»

дали положительные отзывы на диссертацию.

Ведущая организация Объединенный институт ядерных исследований, г. Дубна, в своем положительном заключении, подписанном Кореньковым Владимиром Васильевичем, доктором технических наук, директором Лаборатории информационных технологий им. М.Г. Мещерякова, указала, что диссертационная работа содержит математически обоснованные положения и практические результаты, которые могут быть в целом квалифицированы как решение крупной научной проблемы, направленной на повышение качества разрабатываемого программного обеспечения.

Соискатель имеет более 160 опубликованных работ, в том числе по теме диссертации опубликовано 89 работ, из них в рецензируемых научных изданиях опубликовано 36 работ, включая 11 публикаций в изданиях с квартилем Q1, 12 – с квартилем Q2, 3 – с квартилем Q3. В трудах российских и международных конференций опубликованы 53 работы.

Получено 26 свидетельств о государственной регистрации программ для ЭВМ и 12 патентов на изобретения.

Наиболее значимые работы соискателя:

1. Tchernykh A., Schwiegelsohnc U., Talbi E.G., Babenko M. Towards Understanding Uncertainty in Cloud Computing with Risks of Confidentiality, Integrity, and Availability // Journal of Computational Science. — 2019. — Vol. 36. — P. 100581.
2. Babenko M., Tchernykh A., PulidoGaytan B., et al. Towards the Sign Function Best Approximation for Secure Outsourced Computations and Control // Mathematics. — 2022. — Vol. 10. — No 12. — P. 2006.
3. Babenko M., Piestrak S.J., Chervyakov N., Deryabin M. The Study of Monotonic Core Functions and Their Use to Build RNS Number Comparators // Electronics. — 2021. — Vol. 10. — No 9. — P. 1041

4. Tchernykh A., Babenko M., Chervyakov N. et al. Scalable Data Storage Design for Nonstationary IoT Environment with Adaptive Security and Reliability // IEEE Internet of Things Journal. — 2020. — Vol. 7. — No 10. — P. 10171–10188.
5. Babenko M., Deryabin M., Piestrak S.J. et al. RNS Number Comparator Based on a Modified Diagonal Function // Electronics. — 2020. — Vol. 9. —No 11. — P. 1784.
6. Babenko M.G., Golimblevskaia E.I., Shiriaev E.M. Comparative Analysis of Homomorphic Encryption Algorithms Based on Learning with Errors // Proceedings of the Institute for System Programming of the RAS. — 2020. — Vol.32.—No2.— P.37–52.
7. Chervyakov N., Babenko M., Tchernykh A. et al. AR-RRNS: Configurable Reliable Distributed Data Storage Systems for Internet of Things to Ensure Security // Future Generation Computer Systems. — 2019. — Vol. 92. — P. 1080–1092.
8. Tchernykh A., Babenko M., Chervyakov N. et al. AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage // International Journal of Approximate Reasoning. — 2018. — Vol. 102. — P. 60–73.
9. Miranda-Lopez V., Tchernykh A., Babenko M. et al. 2Lbp-RRNS: Two-Levels RRNS with Backpropagation for Increased Reliability and Privacy-Preserving of Secure Multi-Clouds Data Storage // IEEE Access. — 2020. — Vol. 8. — P. 199424–199439.
10. Бабенко М.Г., Черных А.Н., Червяков Н.И. и др. Эффективное сравнение чисел в системе остаточных классов на основе позиционной характеристики // Труды Института системного программирования РАН. — 2019. — Т. 31. — No 2. — С. 187–201.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- предложен метод вычисления многочленов наилучшего приближения и решена задача об их количестве;
- модифицированы методы контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа;
- разработан метод обнаружения и исправления ошибок в двухуровневой системе остаточных классов с использованием расстояния Хемминга;
- предложены оригинальные методы и алгоритмы повышения надежности и безопасности хранимых и обрабатываемых данных в распределенных средах;
- предложена 2Lbp-RRNS конфигурируемая масштабируемая двухуровневая структура доступа на основе избыточной системы остаточных классов, допускающая реализацию гомоморфных вычислений и позволяющая осуществлять параллельную обработку данных с сохранением их конфиденциальности;
- разработаны алгоритмы кодирования и декодирования данных в 2Lbp-RRNS для улучшения эффективности обработки данных в распределенных средах.

Теоретическая значимость исследования обоснована тем, что:

- разработана теория построения многочленов наилучшего приближения функции определения знака числа;
- разработана теория сравнения зашифрованных чисел и определения их знака над кольцом с делителями нуля;
- выделен класс монотонных функций ядра Акушского, решена проблема возникновения критических ядер;
- построены многочлены, использующие интерполяционные многочлены Лагранжа, позволяющие определять знак числа и сравнивать числа над полем Z_m, уточнены их степени.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что их применение позволяет проектировать распределенные системы обработки конфиденциальных данных, использующие гомоморфные вычисления. Предложенные модели построения подобных систем, а также эффективные реализации вычислительно сложных операций и алгоритмов кодирования, декодирования обеспечивают повышение эффективности систем распределенной обработки конфиденциальных данных в современных распределенных вычислительных системах.

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

Оценка достоверности результатов исследования выявила:

- в работе корректно применяются классические методы исследования;
- приводятся строгие доказательства;
- проводится анализ эффективности разработанных моделей и алгоритмов;
- полученные результаты исследования подтверждаются численными экспериментами.

Личный вклад соискателя состоит в личном участии на всех этапах процесса разработки, реализации предложенных методов и алгоритмов и их анализа. Все выносимые на защиту результаты получены лично автором. Из совместных работ в диссертацию включены только те результаты, которые принадлежат непосредственно автору. В опубликованных совместных работах постановка и решение задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя.

В ходе защиты диссертации были высказаны следующие критические замечания:

- Недостаточное внимание уделено проблеме неопределенности времени выполнения задач при проектировании надежных систем длительного хранения больших данных.
- Не уточнены классы задач, для которых предложенные методы позволяют получить эффективное решение.

Соискатель Бабенко Михаил Григорьевич согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 08 декабря 2022 года диссертационный совет принял решение за разработку теоретических положений, совокупность которых можно квалифицировать как научное достижение, и решение научной проблемы, имеющей важное научное и практическое значение присудить Бабенко М.Г. ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 18 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 22 человек, входящих в состав совета, проголосовали: за – 17, против – 1.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Петренко А. К.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

08 декабря 2022 года