ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертационную работу Русаловского Ильи Дмитриевича «Разработка методов и средств реализации алгоритмов гомоморфного шифрования», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Русаловский Илья Дмитриевич с отличием окончил очное обучение в Южном федеральном университете в 2018 году по специальности 10.05.03 «Информационная безопасность автоматизированных систем», затем аспирантуру Южного федерального университета по специальности: 05.13.19 (2.3.6) «Методы и системы защиты информации, информационная безопасность». При выполнении диссертационного исследования как теоретической, так и экспериментальной части, Русаловский И.Д. проявил себя как высококвалифицированный и инициативный специалист, способный самостоятельно ставить и решать задачи научно-технического характера. Также следует отметить способности соискателя к творческому мышлению и владение современными методами исследования. В процессе работы Русаловский И.Д. продемонстрировал целеустремленность, педантичность, ответственность при решении поставленных научно-технических задач.

Диссертационная работа посвящена разработке методов и алгоритмов выполнения гомоморфных операций, позволяющих расширить список поддерживаемых операций в существующих схемах и библиотеках гомоморфной криптографии.

Актуальность темы. В современном мире информационные технологии активно применяются во всех сферах жизни. В результате процесса информатизации вырос объем информации, возросли информационные потоки. В условиях бурного роста информационных технологий как никогда ранее стала актуальна проблема обеспечения информационной безопасности. Одна из основных задач информационной безопасности – это обеспечение

конфиденциальности информации. Актуальность необходимости обеспечения конфиденциальности информации обострилась с появлением и широким распространением облачных технологий. Классические криптографические средства обеспечивают необходимый уровень защиты данных при их передаче от клиента на облачный сервис по незащищенному каналу связи, такому как интернет. Однако после передачи сервис получает неограниченный доступ к данным клиента, так как эти данные необходимо обработать и вернуть результат клиенту. В этом кроется потенциальная уязвимость, так как сервис может быть оказаться недобросовестным, либо может быть подменен или скомпрометирован. Для решения этой проблемы может быть применено одно из молодых направлений в криптографии – гомоморфная криптография.

Однако существующие программные комплексы (HElib, Microsoft SEAL, TFHE) реализуют только основные операции над гомоморфно зашифрованными данными – сложение и умножение в алгоритмах над целыми данными, конъюнкцию и исключающее ИЛИ в алгоритмах над битами. В то время как для решения прикладных задач необходима поддержка полного перечня операций над гомоморфно зашифрованными данными: суммы, разности, умножения, деления, а также сравнения чисел. Поэтому разработка методов и алгоритмов, позволяющих реализовать полный перечень арифметических и логических операций над гомоморфно зашифрованными данными, является актуальной задачей, чему и посвящена данная диссертационная работа. Благодаря разработанным методам и алгоритмам возможно выполнить гомоморфную реализацию практически любого алгоритма обработки данных и использовать их для защищенных облачных вычислений.

Научная новизна работы Русаловского Ильи Дмитриевича:

1. Разработан новый метод, позволяющий выполнять гомоморфное деление на базе любого полностью гомоморфного алгоритма над целыми числами.
2. Разработаны новые методы гомоморфного сравнения чисел. Первый метод позволяет выполнить сравнение гомоморфно зашифрованных чисел при их побитном гомоморфном шифровании. Второй метод позволяет выполнить гомоморфное сравнение чисел в гомоморфных схемах шифрования, основанных на

модулярной арифметике.

3. Разработана гомоморфная реализация алгоритмов побитовых целочисленных операций сложения, разности, умножения и деления, которые могут быть выполнены на основе любого полностью гомоморфного алгоритма шифрования над битами. Разработанные алгоритмы позволяют выполнять арифметические и логические операции в рамках одного гомоморфного алгоритма шифрования, благодаря чему возможно выполнить гомоморфную реализацию практически любого прикладного алгоритма обработки данных.

4. Разработана гомоморфная реализация алгоритмов побитовых операций сложения, разности, умножения и деления над числами в формате с плавающей точкой, которые могут быть выполнены на основе любого полностью гомоморфного алгоритма шифрования над битами. Разработанные алгоритмы позволяют выполнять арифметические и логические операции в рамках одного гомоморфного алгоритма шифрования, а также повышают точность вычислений по сравнению с алгоритмами над числами в формате с фиксированной точкой.

Достоверность научных результатов, представленных в работе, подтверждается непротиворечивостью и согласованностью с известными подходами, фактами и исследованиями в рассматриваемой области.

Практическая ценность и реализация результатов. Практическая значимость диссертационной работы заключается в расширении возможностей практического применения гомоморфного шифрования для решения прикладных задач. Разработанные методы и алгоритмы выполнения гомоморфной математики могут быть использованы в разработке программных продуктов, которые могут быть использованы для разработки сервисов безопасных облачных вычислений на основе гомоморфной криптографии, а также могут быть внедрены в существующие программные комплексы.

Русаловский Илья Дмитриевич по теме диссертационного исследования опубликовал 12 печатных работ: из них: 1 индексирована SCOPUS, 6 работ опубликованы в журналах, входящих в Перечень ВАК РФ; 5 статей опубликованы в материалах конференций, входящих в реферативную базу РИНЦ. По теме исследования автором получено 1 свидетельство о государственной регистрации

программ для ЭВМ.

Основные теоретические и практические результаты диссертационной работы использованы в научно-исследовательских работах и учебном процессе на кафедре безопасности информационных технологий ИКТИБ ЮФУ. Использованы в гранте РФФИ № 20-37-90140/20 на тему: “Разработка методов и средств гомоморфного шифрования для облачных сервисов”.

Считаю, что диссертация Русаловского Илья Дмитриевича «Разработка методов и средств реализации алгоритмов гомоморфного шифрования» соответствует требованиям, установленным положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет», и рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», технические науки.

Научный руководитель, профессор кафедры
«Безопасности информационных технологий»
Южного федерального университета
доктор технических наук, профессор
Бабенко Людмила Климентьевна
347928 г. Таганрог, ул. Чехова, д. 2
Тел. +7(863)436-15-18, e-mail: lkbabenko@sfedu.ru
Персональная страница: https://sfedu.ru/en/person/lkbabenko
Специальности:
05.13.18 – Математическое моделирование, численные методы и комплексы программ
05.13.15 – Вычислительные машины, комплексы и компьютерные сети

Я, Бабенко Людмила Климентьевна, даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«12» февраля 2024 г. Л. К. Бабенко

Подпись Бабенко Л.К. заверяю

Директор ИКТИБ ЮФУ

доктор технических наук, доцент Г. Е. Веселов