На правах рукописи

РУСАЛОВСКИЙ ИЛЬЯ ДМИТРИЕВИЧ

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ РЕАЛИЗАЦИИ АЛГОРИТМОВ ГОМОМОРФНОГО ШИФРОВАНИЯ

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Таганрог 2024

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» на кафедре безопасности информационных технологий имени Олега Борисовича Макаревича Института компьютерных технологий и информационной безопасности.

Научный руководитель:	**Бабенко Людмила Климентьевна** доктор технических наук, профессор
Официальные оппоненты:	**Осипян Валерий Осипович** доктор физико-математических наук, доцент, ФГБОУ ВО «Кубанский государственный университет», г. Краснодар, профессор кафедры анализа данных и искусственного интеллекта **Тебуева Фариза Биляловна** доктор физико-математических наук, доцент, ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, заведующая кафедрой компьютерной безопасности

Защита состоится «06» июня 2024 г. в 14:00 часов на заседании диссертационного совета ЮФУ801.02.02 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в зональной научной библиотеке ЮФУ по адресу: г. Ростов-на Дону, ул. Зорге, 21-ж и на сайте ФГАОУ ВО «Южный федеральный университет» по адресу: https://hub.sfedu.ru/diss.

Отзывы на автореферат в двух экземплярах, заверенные печатью учреждения, просьба направлять по адресу: 347922, Ростовская обл., г. Таганрог, ГСП-17А, пер. Некрасовский, 44, к. 302, Диссертационный совет ЮФУ801.02.02.

Автореферат разослан «___» марта 2024 г.

Ученый секретарь
диссертационного совета ЮФУ801.02.02,
кандидат технических наук, доцент  Ельчанинова Н.Б.

Общая характеристика работы

Актуальность темы исследования. Актуальность облачных технологий и решений возрастает с каждым годом. По данным компании Reportlinker.com мировой рынок управления ИТ-услугами (ITSM) на основе облачных технологий вырос с 7,61 миллиарда долларов в 2022 году до 8,72 миллиарда долларов в 2023 году при совокупном годовом темпе роста (CAGR) в 14,6%. Облачные технологии активно применяются во всех сферах жизни – науке, образовании, медицине, бизнесе и так далее. В связи с высокой популярностью данных сервисов остро стоит вопрос обеспечения в них информационный безопасности, в частности, вопрос обеспечения конфиденциальности данных, так как число утечек информации в России и во всем мире растет с каждым годом.

Стандартные криптографические средства обеспечивают сохранность информации в процессе ее передачи по незащищенным каналам связи, однако на облачном сервисе данные расшифровываются для последующей обработки и в этом кроется потенциальная уязвимость. В случае подмены или компрометации сервера злоумышленник получит доступ к расшифрованным данным. Также, если поставщик услуг окажется неблагонадежным, он тоже сможет получить доступ к конфиденциальным данным пользователя. При этом уровень защиты информации определяется не только надежностью механизмов защиты, но также уровнем доверия к поставщику услуг. Использование гомоморфного шифрования (ГШ) вместо классического шифрования позволяет решить вышеприведенные проблемы, так как ГШ позволяет обрабатывать данные в зашифрованном виде. Наибольший интерес в прикладных задачах представляют схемы полностью гомоморфного шифрования (ПГШ), которые поддерживают две операции над гомоморфно зашифрованными данными и позволяют выполнять неограниченное число последовательных операций над зашифрованными данными. Однако существующие программные комплексы, реализующие ГШ, поддерживают

только основные гомоморфные операции, а для прикладного применения необходима разработка дополнительных гомоморфных операций.

Степень разработанности темы. Впервые вопрос о существовании схем ПГШ был рассмотрен в работе Ривеста, Эйдлмана и Дертузо. Однако долгое время этот вопрос оставался открытым и были известны только схемы ГШ, обладающие ограниченным функционалом.

Прорыв в этом направлении был достигнут в 2009 году, когда Крейг Джентри предложил новую концепцию построения схем ПГШ с открытым ключом. На основе его схемы сейчас построены многие другие, использующие различный математический аппарат. Криптографическая стойкость данных схем строится на сложности решения задач теории решеток.

Вопрос прикладного применения ГШ рассматривается в работах отечественных и зарубежных исследователей: А. А. Гаража, Е. А. Толоманенко, В. Д. Салман, А. М. Щелкунов, P. Martins, D. Archer, Г. Г. Аракелов, Ф. Б. Буртыка.

Обзор и сравнительный анализ существующих схем ГШ и программных комплексов, реализующих эти схемы, приводится в работах A. Kim, М. Г. Бабенко, P. V. Parmar, S.S. Sathya. В работе S.S. Sathya рассматриваются существующие криптографические библиотеки ПГШ (SEAL, HElib, TFHE) и делается вывод о нехватке в них гомоморфных операций деления и сравнения шифртекстов.

Таким образом, существующие программные комплексы 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.

Целью исследования является расширение круга выполняемых гомоморфных криптографических операций.

Научная задача состоит в разработке методов и алгоритмов реализации гомоморфных операций, позволяющих эффективно применять гомоморфную криптографию для защищенных облачных вычислений.

Достижение поставленной цели и научной задачи исследования требует решения следующих частных задач:

1. Проанализировать существующие методы и алгоритмы гомоморфного шифрования, а также существующие программные реализации алгоритмов гомоморфного шифрования.
2. Разработать методы и алгоритмы реализации гомоморфных операций.
3. Провести экспериментальные исследования по оценке достоверности и эффективности разработанных методов и алгоритмов.

Объектом исследования являются технологии защиты данных при обработке в облачных сервисах.

Предметом исследования являются методы и алгоритмы гомоморфного шифрования.

Методология и методы исследования. Методы исследования основаны на использовании теоретических основ математической логики, теории вероятностей, теории чисел, основ алгоритмизации, методов программирования, теории информационной безопасности, теории гомоморфного шифрования.

К основным **научным положениям, выносимым на защиту**, следует отнести:

1. Новый метод гомоморфного деления позволяет выполнять гомоморфное деления на основе любого полностью гомоморфного алгоритма над целыми числами.

2. Методы гомоморфного сравнения чисел позволяют сравнить гомоморфно зашифрованные числа и получить гомоморфно зашифрованный результат, соответствующий результату сравнения.

3. Алгоритмы реализации гомоморфных операций сложения, разности, умножения и деления над целыми числами через операции над битами с использованием любого полностью гомоморфного алгоритма шифрования над битами позволяют в рамках одной криптосистемы выполнять и арифметические, и логические операции, что позволяет выполнить реализацию практически любого прикладного алгоритма обработки данных.

4. Алгоритмы реализации гомоморфных операций сложения, разности, умножения и деления над рациональными числами в формате с плавающей точкой с использованием любого полностью гомоморфного алгоритма шифрования над битами позволяют в рамках одной криптосистемы выполнять и арифметические, и логические операции, а также позволяют повысить точность вычислений, что важно при выполнении операции деления.

5. Алгоритм гомоморфной реализации метода Гаусса позволяет выполнить решение СЛАУ методом Гаусса над гомоморфно зашифрованными данными и получить гомоморфно зашифрованный результат, соответствующий решению системы.

Теоретическая значимость результатов исследования заключается в разработке новых методов и алгоритмов для реализации гомоморфных вычислений при решении задач обработки данных в недоверенных средах.

Научная новизна. В диссертации получены следующие новые научные результаты.

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. Разработаны алгоритмы гомоморфной реализации 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. Разработаны алгоритмы гомоморфной реализации 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.

Практическая значимость 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 применяться для разработки сервисов безопасных облачных вычислений на основе гомоморфной криптографии, а также могут быть внедрены в существующие программные комплексы.

Степень достоверности полученных результатов подтверждается разработкой действующих методов и алгоритмов и их программной реализацией, экспериментами.

Внедрение результатов работы. Результаты диссертационных исследований, подтвержденные соответствующими актами, используются в:

1. научно-производственной деятельности ООО «Айвиаппс» (г. Таганрог), а именно: выполнена практическая апробация разработанных алгоритмов реализации гомоморфной математики на основе битовых операций;
2. гранте РФФИ № 20-37-90140/20 на тему: “Разработка методов и средств гомоморфного шифрования для облачных сервисов”;
3. учебном процессе на кафедре безопасности информационных технологий им. О. Б. Макаревича ИКТИБ ЮФУ.

Апробация результатов. Основные положения и выводы, полученные в представленной работе, докладывались и обсуждались на всероссийских научных конференциях: : IV Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» (г. Таганрог, 2017 г.), IV Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» (г. Таганрог, 2018 г.), Научно-методическая конференция «Современные компьютерные технологии» (г. Таганрог, 2020 г.), 15th International Conference On Security Of Information And Networks, SIN 2022 (Sousse, Tunisia, 2022 г.).

Публикации. Основные положения диссертации опубликованы в 12 научных печатных работах, в том числе: 6 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ, 1 – в научных рецензируемых изданиях, индексируемых в базе Scopus, 5 – в материалах конференций и других изданиях. Получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Вклад соавторов ограничивался постановкой задач исследования и обсуждением полученных результатов.

Связь работы с научными программами, темами, грантами. Исследования выполнялись при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90140/20 на тему: “Разработка методов и средств гомоморфного шифрования для облачных сервисов”.

Соответствие паспорту специальности. Диссертационная работа посвящена разработке методов и алгоритмов выполнения гомоморфной математики, что соответствует паспорту специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»: п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» и п. 19 «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов».

Объем и структура диссертационной работы. Диссертация написана на русском языке, состоит из введения, пяти глав, заключения, списка используемой литературы из 91 наименования и приложений. Полный объём диссертации составляет 143 страницы (в том числе приложения 20 стр.), включая 14 рисунков и 12 таблиц.

Содержание работы

Во введении дается краткая характеристика работы, сформулированы ее цели и задачи, обоснована актуальность исследований в данной предметной области, показана научная новизна и практическая ценность полученных результатов.

В первой главе рассмотрены текущие тенденции и исследования в области гомоморфной криптографии. Выполнен анализ существующих программных комплексов полностью гомоморфного шифрования, таких как SEAL, HElib, TFHE. В программных комплексах отсутствует поддержка операций гомоморфного деления и сравнения шифртекстов, а также нет возможности выполнять условные операции, а ведь поддержка этих операций

необходима во многих алгоритмах обработки данных. Шифрование выполняется либо над целыми числами с возможностью выполнять арифметические операции, либо над битами с возможностью выполнять побитовые операции, однако нет возможности выполнять и побитовые, и арифметические операции в рамках одного гомоморфного алгоритма шифрования. Возможность выполнять побитовые и арифметические операции в рамках одной гомоморфной криптосистемы позволило бы реализовать сложные алгоритмы обработки данных, содержащие в том числе условные операции и сравнение чисел.

Как видно из анализа, программные комплексы реализуют, как правило, только криптографические примитивы, а для полноценного применения в прикладных задачах требуется расширение круга поддерживаемых гомоморфных операций, что в свою очередь требует определенного уровня знаний и навыков, а также дополнительных временных затрат. На основании проведенного анализа можно сделать вывод о нехватке решений для прикладного применения гомоморфной криптографии. Формулируются следующие проблемы:

- отсутствие поддержки операции гомоморфного деления;
- отсутствие поддержки операций гомоморфного сравнения;
- отсутствие поддержки условных операций;
- отсутствие возможности выполнять и арифметические, и логические операции над шифртекстами в рамках одной криптосистемы.

Во второй главе подробно рассматривается проблема гомоморфного деления, анализируется возможность реализации данной операции в разных алгоритмах гомоморфного шифрования, предлагается метод гомоморфного деления на основе представления шифртекстов в виде простой дроби.

Данный метод позволяет реализовать гомоморфное деление на основе любого полностью гомоморфного алгоритма шифрования над целыми числами, поддерживающего гомоморфные операции суммы, разности и

умножения. Открытый текст (целое или рациональное число) представляется в виде простой дроби. Делимое и делитель шифруются по отдельности с помощью полностью гомоморфного алгоритма шифрования, полученная зашифрованная дробь является шифртекстом. Операции над шифртекстами реализуются как операции над простыми дробями, а при расшифровке делимое и делитель расшифровываются раздельно и делятся друг на друга. Метод можно представить следующим образом:

Пусть дан некоторый полностью гомоморфный алгоритм шифрования над целыми, для которого определены E(m) – алгоритм шифрования, D(c) – алгоритм расшифрования, обратный к E(m), $\otimes$,$\oplus$ – операторы гомоморфного умножения и сложения над зашифрованными данными соответственно, где m – открытый текст, c – шифртекст. Тогда схема шифрования целого числа m с поддержкой операции деления может быть построена следующим образом.

Алгоритм шифрования:

1. Представляем открытый текст m в виде простой дроби, где m_1 – делимое, m_2 – делитель.

2. Шифруем делимое и делитель с помощью полностью гомоморфного алгоритма шифрования над целыми числами: $a = E(m_1)$, $b = E(m_2)$

3. Шифртекст в предлагаемой схеме шифрования будет представлен в виде пары зашифрованных гомоморфно чисел: c = (a; b)

Алгоритм расшифрования:

1. Расшифруем гомоморфно зашифрованные делимое и делитель, в виде которых представлен шифртекст: $r_1 = D(a)$; $r_2 = D(b)$

2. Выполняем деление, чтобы получить результат в виде десятичной дроби: $r = r_1 / r_2$

Реализация математических операций:

- Сложение. $C_1 + C_2 = (a_1 \otimes b_2 \oplus a_2 \otimes b_1;\ b_1 \otimes b_2)$
- Умножение. $C_1 * C_2 = (a_1 \otimes a_2;\ b_1 \otimes b_2)$

- Деление. ${}^{C_1}/_{C_2} = (a_1 \otimes b_2;\ b_1 \otimes a_2)$

Данный метод прост в реализации, универсален, с его помощью можно добавить операцию деления в любой полностью гомоморфный алгоритм шифрования над целыми. Также метод может быть полезен в том случае, когда реализация гомоморфного деления другим способом требует больших вычислительных мощностей. К минусам можно отнести увеличение размерности шифртекста приблизительно в два раза, так как он представлен двумя гомоморфно зашифрованными числами. Также увеличивается сложность выполнения других операций: умножение усложняется примерно в два раза (из-за необходимости выполнять ее дважды - для делимого и делителя), а сложность операций сложения и разности увеличивается приблизительно в 4 раза (при условии того, что вычислительная сложность операций гомоморфного сложения и умножения эквивалентна) из-за необходимости приведения числа к общему знаменателю.

В третьей главе рассматривается возможность построения гомоморфных операций над целыми числами на основе гомоморфных операций над битами. Разработаны алгоритмы реализации гомоморфных побитовых операций сложения, разности, умножения и деления. Также разработан метод гомоморфного сравнения шифртекстов.

Алгоритм умножения. Для гомоморфной реализации данный алгоритм можно представить следующим образом:

- на каждом этапе рассчитываем частичное произведение и суммируем его с промежуточным результатом
- частичное произведение равно $A \wedge (b_i \otimes b_{i-1}) \ll i-1$, нумерацию битов начинаем с младших разрядов, b_0 разряд принимаем равным 0
- полученное частичное произведение подаем на универсальное суммирующее устройство, сигнал, управляющий режимом работы, рассчитываем по формуле $F = (b_i \otimes b_{i-1}) \wedge b_i$. Если биты различны и текущий бит равен 1, то результат выражения будет равен 1 и будет активен режим

разности, во всех иных случаях устройство будет работать в режиме суммирования.

Алгоритм деления. Пусть дан некоторый полностью гомоморфный алгоритм шифрования над битами, для которого определены E(m) – алгоритм шифрования, D(c) – алгоритм расшифрования, обратный к E(m), $\otimes$,$\oplus$ – гомоморфные логические операции, определённые в данном алгоритме шифрования, где m – открытый текст, c – шифртекст. В общем виде алгоритм шифрования можно представить следующим образом:

1. Целое число m раскладываем побитно: $m = m_1 m_2 \ldots m_n$
2. Каждый бит шифруется отдельно: $C = E(m_1)E(m_2)\ldots E(m_n)$

Для облегчения выполнения операции разности в данной криптосистемы числа представляются в дополнительном коде. Алгоритм гомоморфного деления целых чисел, представленных в виде массива гомоморфно зашифрованных битов, можно представить следующим образом:

1. Нормализация делимого и делителя. В случае, если делитель и делимое имеют разную разрядность, нормализуем их разрядность к одной величине – наибольшей разрядности среди них. В шифртекст с меньшей разрядностью для нормализации необходимо продублировать самый левый разряд (знаковый) необходимое число раз.
2. Определяем разрядность частного. Минимально допустимое значение модуля делителя равно 1, поэтому числитель по модулю не может быть больше делимого. Следовательно, разрядность частного будет равна разрядности делимого.
3. Формируем начальный остаток, заполняя его знаковым битом делителя.
4. Сдвигаем содержимое делимого влево, игнорируя знаковый бит. Выдвинутый бит вдвигаем справа в промежуточный остаток.
5. Прибавляем модуль делителя к остатку, взяв его с противоположным знаком. Фактически, это вычитание из старших разрядов делимого, которые мы постепенно перемещаем на место остатка. Если знак

полученного остатка совпадает со знаком делителя, то значение следующего бита частного устанавливаем равным 1, иначе 0. Если знак полученного остатка совпадает со знаком делимого, то используем этот остаток на следующей итерации, иначе выполняем операцию «восстановления» остатка – используем предыдущее значение остатка.

6. Если сформированы n+1 битов частного, где n – разрядность частного, то переходим к следующему шагу. Иначе возвращаемся к шагу 6.

7. Прибавляем к частному единицу округления. В случае, если мы получаем отрицательный результат, начальное заполнение частного будет в обратном коде. Поэтому прибавление единицы автоматически округляет результат и переводит его в дополнительный код, в случае отрицательного результата.

8. Отбрасываем (n+1)-й бит частного. Полученное частное является результатом деления.

Условный оператор. Также в предлагаемом побитовом представлении возможно реализовать условные операторы, которые в общем виде можно представить как:

$$f(x) = \begin{cases} a, & \text{условие 1} \\ b, & \text{условие 2} \end{cases}$$

Условия могут быть любыми, но, как правило, сравниваются некоторые значения. Для построения гомоморфной реализации условного алгоритма необходимо разработать гомоморфную реализацию для каждого оператора неравенства и оператора равенства в виде некоторого метода, который в качестве входных параметров будет принимать два шифртекста и будет возвращать в качестве результата гомоморфно зашифрованный бит, который при расшифровании равен 1, если условие верно и 0 в обратном случае. Рассмотрим реализацию данного метода в рамках побитной схемы шифрования (см. параграф 3.1 диссертации).

Пусть c – шифртекст, представленный в виде массива зашифрованных гомоморфно битов, $f(c_1;c_2)$ – некоторый гомоморфный алгоритм,

возвращающий шифртекст от 1 в случае, если сравнение чисел выполняется, $\wedge, \vee, \oplus$ – гомоморфные операции конъюнкции, дизъюнкции и исключающего «или» над шифртекстами. Тогда условие вида «если числа верны, результата равен первому числу, иначе результат равен второму числу» можно в общем виде выразить как:

$$c_3 = c_1 \oplus f(c_1; c_2) \vee c_2 \oplus \overline{f(c_1; c_2)} \quad (2)$$

Приведенное выше выражение можно адаптировать при необходимости под условия решаемой задачи.

Метод гомоморфного сравнения. Для реализации сравнения двух целых чисел, представленных в двоичном виде в дополнительном коде и зашифрованных побитно предлагается следующий алгоритм.

Пусть A, B – два шифртекста, представленных в дополнительном коде и зашифрованных побитно с помощью схемы ПГШ над битами, для которых определена функция разности, а для каждой пары битов (a_i, b_j) определены гомоморфные операторы исключающего «или», конъюнкции и дизъюнкции, тогда:

Для проверки равенства чисел сравниваем их побитно и суммируем результаты сравнений: $r = \overline{(a_0 \oplus b_0) \wedge (a_1 \oplus b_1) \wedge \ldots \wedge (a_n \oplus b_n)}$. Если все биты попарно равны, то числа равны и мы получим в результате 1, иначе 0.

Строгие сравнения чисел можно выполнить следующим образом:

- Вычисляем разность C = A – B
- Вычисляем r – результат проверки чисел на равенство

Результат сравнения определяется на основе комбинации знакового бита c_0 и результата сравнения r. Напомним, что знаковый бит равен 1, если число отрицательное, и 0, если положительное.

- $A < B$; c_0 – результат отрицательный, только если A строго меньше B
- $A \leq B$; $c_0 \vee r$ – результат отрицательный или числа равны
- $A > B$; $\overline{c_0 \vee r}$ – инверсия выражения $A \leq B$

- $A \geq B$; $\overline{c_0}$ – инверсия выражения A < B

На основе приведенных выше формул можно получить гомоморфно зашифрованный результат любого сравнения чисел, что можно использовать в разработке гомоморфной реализации алгоритмов. Например, при реализации алгоритма Гаусса на основе предложенного метода можно определять нулевые элементы на главной диагонали и выполнять перестановку строк при необходимости.

Оценка сложности разработанных алгоритмов. Для разработанных алгоритмов гомоморфного сложения, разности, умножения и деления дается оценка сложности, выраженная в числе побитовых гомоморфных операций. Оценка приведена в таблицах 1-3.

Таблица 1. Сложность выполнения операций сложения и вычитания

Число битов	Гомоморфное сложение	Гомоморфное умножение	Глубина по умножению
16	64	32	16
32	128	64	32
64	256	128	64

Таблица 2. Сложность выполнения операции умножения

Число битов	Гомоморфное сложение	Гомоморфное умножение	Глубина по умножению
16	1040	784	$\approx 16^{16}$
32	4128	3104	$\approx 32^{32}$
64	16448	12352	$\approx 64^{64}$

Таблица 3. Сложность выполнения операции деления

Число битов	Гомоморфное сложение	Гомоморфное умножение	Глубина по умножению
16	1802	1394	$\approx 64^{18}$
32	6666	5346	$\approx 128^{34}$
64	25610	20930	$\approx 256^{66}$

На основе результатов анализа можно сделать вывод, что для реализации побитовых гомоморфных операций суммы и разности при небольшой глубине можно использовать пороговые гомоморфные схемы шифрования, однако для реализации побитовых гомоморфных операций умножения и деления можно использовать только схемы ПГШ, потому что пороговые схемы не смогут обеспечить такую глубину по умножению.

В четвертой главе рассматривается возможность построения гомоморфных операций над рациональными числами на основе гомоморфных битовых операций над целыми и битами. Приводится алгоритм шифрования и рассматривается реализация арифметических операций сложения, разности, умножения и деления, а также логическая операция сравнения.

Все операции над числами в формате с плавающей точкой состоят из операций над целочисленными порядком и мантиссой, следовательно, легко могут быть реализованы через битовые операции. Однако при выполнении гомоморфной реализации возникают сложности с операциями нормализации и приведения чисел к одной степени, так как эти операции выполняются до достижения некоторого условия (число в нормальной форме, равные степени чисел). Однако управляющий алгоритм не может определить, когда это условие выполнится, так как обрабатывает зашифрованные данные. Поэтому при выполнении гомоморфной реализации необходимо предполагать худший исход, когда на выполнение данных операций требуется максимально возможное число итераций, а при выполнении каждой итерации над гомоморфно зашифрованными данными обрабатывать данные таким образом, чтобы при достижении условия число больше не изменялось.

В главе подробно рассматривается гомоморфная реализация каждой из проблемных операций (нормализации и приведения к одному порядку), а также реализация каждой арифметической операции. Из-за того, что операции нормализации и приведения к одному порядку всегда выполняются по худшему сценарию с максимальным числом итераций, сложность выполнения операций возрастает по сравнению с алгоритмами над числами с

фиксированной запятой. Однако представление чисел в формате с плавающей точкой позволяет повысить размерность шифруемых чисел при том же числе зашифрованных бит, а также многократно повышает точность вычислений, поэтому для решения задач, где требуется высокая точность, а также для задач, где выполняется большое число операций деления и ошибка от округления быстро накапливается, имеет смысл использовать числа в формате с плавающей точкой.

Оценка сложности разработанных алгоритмов. Для разработанных алгоритмов гомоморфного сложения, разности, умножения и деления дается оценка сложности, выраженная в числе побитовых гомоморфных операций. Оценка приведена в таблицах 4-6.

Таблица 4. Сложность выполнения операций сложения и разности

Число битов	Гомоморфное сложение	Гомоморфное умножение
16	1136	1048
32	4264	4500
64	16760	19744

Таблица 5. Сложность выполнения операции умножения

Число битов	Гомоморфное сложение	Гомоморфное умножение
16	565	431
32	2448	1860
64	11491	8687

Таблица 6. Сложность выполнения операции деления

Число битов	Гомоморфное сложение	Гомоморфное умножение
16	898	737
32	3970	3158
64	17914	15057

Оценка показала, что операции гомоморфного сложения и вычитания над числами в формате с плавающей точкой намного сложнее аналогичных

операций над числами в формате с фиксированной точкой. Однако операции умножения и деления, наоборот, имеют более низкую сложность. Следовательно, разработанные алгоритмы могут эффективней применяться в алгоритмах обработки данных, содержащих большое число операций суммы и умножения, и обеспечивать более высокую точность вычислений, по сравнению с алгоритмами над числами в формате с фиксированной точкой.

Пятая глава посвящена разработке гомоморфной реализации некоторых прикладных алгоритмов на основе разработанных в предыдущих главах методов и алгоритмов, а также практической апробации разработанных алгоритмов.

Одной из областей применения гомоморфной криптографии являются защищенные облачные вычисления, а также их частный случай – обработка цифровых изображений. Поэтому были рассмотрены возможности гомоморфной реализации алгоритмов обработки цифровых изображений, в частности алгоритмов масштабирования. Были проанализированы некоторые простейшие алгоритмы масштабирования (метод ближайшего соседа, алгоритм EPX) и была предложена гомоморфная реализация для алгоритма EPX, логика работы которого отображена на рисунке 1.

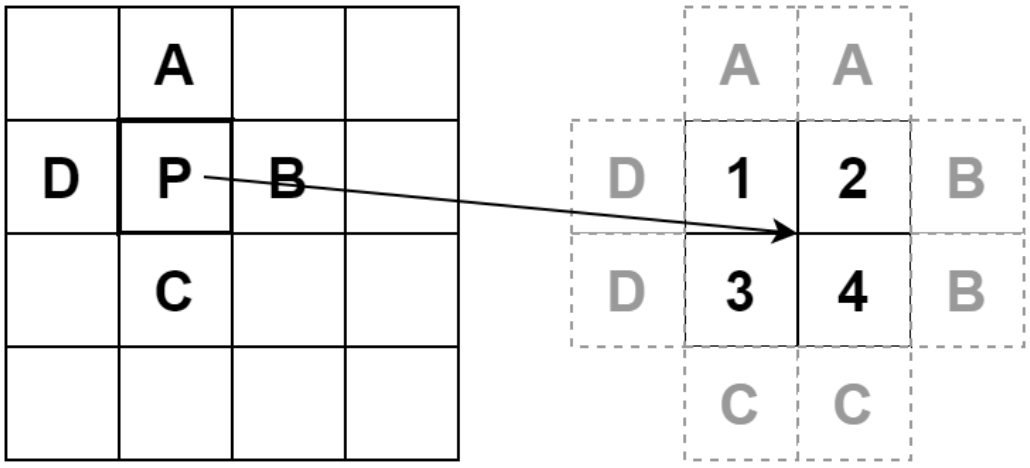

Рисунок 1 – Алгоритм EPX

Корректировка цвета результирующих пикселей в алгоритме EPX выполняется следующим образом:

- Если A = D, то 1 = A, иначе 1 = P
- Если A = B, то 2 = A, иначе 2 = P
- Если C = D, то 3 = C, иначе 3 = P
- Если C = B, то 4 = C, иначе 4 = P

Если значения пикселей A и D исходного изображения равны, то пиксель результирующего изображения 1 красится в цвет пикселя A, иначе цвет пикселя 1 остается равен P (начальному заполнению). Аналогичные операции выполняются для остальных пикселей результирующего изображения.

Алгоритмы масштабирования содержат методы коррекции цветов исходного изображения, позволяющие улучшить качество результирующего изображения и методы коррекции основываются на анализе соседних пикселей исходного изображения, для которого необходимо применение алгоритма гомоморфного сравнения. Для обработки изображения требуются огромные вычислительные ресурсы, так как каждый пиксель, представленный тремя целыми числами – цветовыми компонентами модели RGB, необходимо будет зашифровать побитно, и каждая операция сравнения будет выполняться на основе множества битовых гомоморфных операций.

Также была рассмотрена гомоморфная реализация алгоритма Гаусса. Решение систем линейных уравнений необходимо для решения многих задач, поэтому гомоморфная реализация алгоритма Гаусса, обеспечивающего решение СЛАУ, актуальна. Алгоритм Гаусса обладает следующими преимуществами:

- Нет необходимости исследовать систему на совместность
- Метод можно применять и к системам, в которых число уравнений не равно числу неизвестных, а основная матрица системы вырожденная

- Метод результативен при сравнительно небольшом числе операций

Всю работу алгоритма можно разбить на три основных действия:

- проверка системы перед итерацией обнуления элементов столбца и перестановка уравнений при необходимости во избежание появления нулевого элемента на главной диагонали (выполняется во время прямого хода)
- обнуление элементов столбца ниже главной диагонали (выполняется во время прямого хода)
- проверка системы перед следующей итерацией и перестановка уравнений при необходимости во избежание появления нулевого элемента на главной диагонали (выполняется во время прямого хода)
- получение значения неизвестных, начиная с нижней строки в матрице (обратный ход)

Все вышеприведенные операции возможно реализовать гомоморфно при условии, что система шифрования поддерживает все арифметические операции (сложение, разность, умножение и деление), а также логическую операцию сравнения числа с нулем. Самой сложной операцией в алгоритме будет перестановка уравнений, так как данные зашифрованы и управляющий алгоритм не знает, когда в главной диагонали появится ненулевой элемент. Из-за этого необходимо выполнять попытку перестановки уравнений максимальное число раз, перебирая все уравнения.

Также в главе приводятся детали практической реализации предложенных методов и алгоритмов, приводятся результаты экспериментальной проверки результатов исследования. В качестве основы для реализации гомоморфной криптографии была использована библиотека Helib для MacOS. Для шифрования была использована схема BGV в режиме шифрования битов (пространство открытого текста равно 2). На основе алгоритмов, рассмотренных в главе 3, с использованием битовых гомоморфных операций, были реализованы арифметические гомоморфные

операции суммы, разности, умножения и деления. Схема программной реализации приведена на рисунке 2.

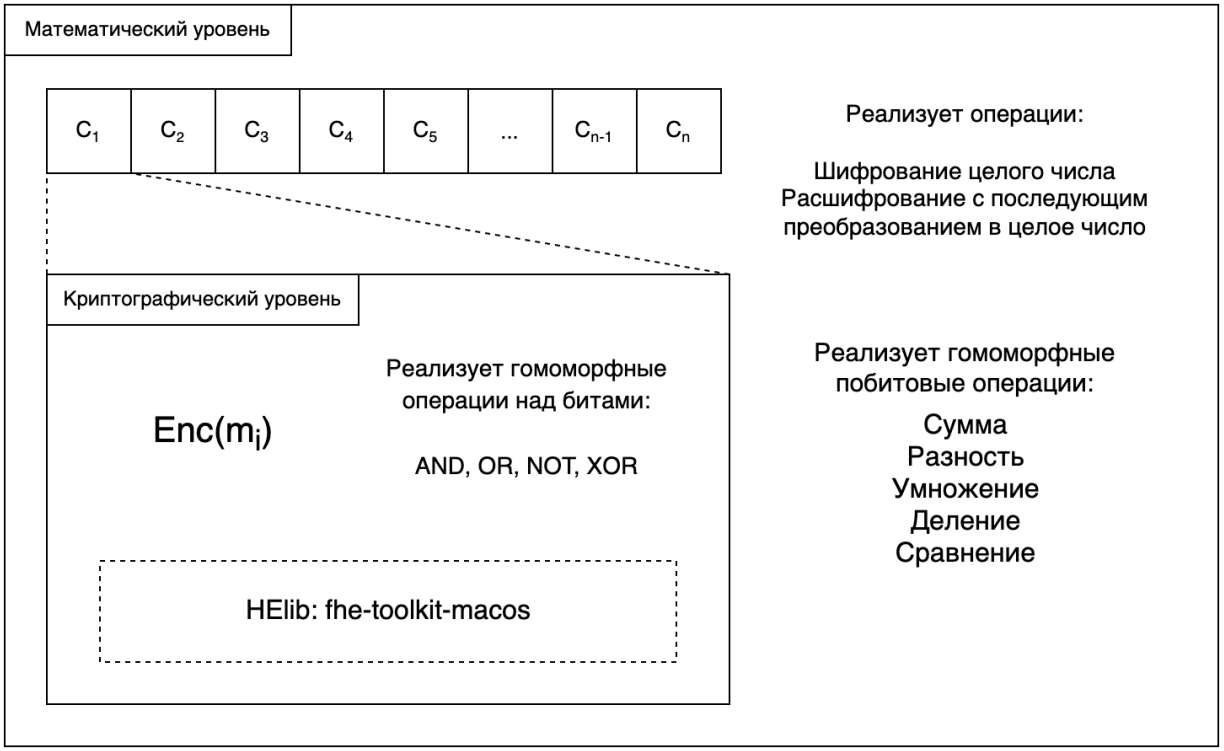

Рисунок 2 – Схема программной реализации побитовой арифметики

В качестве криптографического ядра (схемы ПГШ) используется криптографическая библиотека “HElib: fhe-toolkit-macos”. Программный код приведен в диссертации в приложении 2. Для проверки достоверности разработанных алгоритмов были подготовлены тесты, в рамках которых для каждой арифметической операции генерировались два случайных числа, шифровались побитно, над ними выполнялась гомоморфная арифметическая операция, результат которой расшифровывался и сравнивался с эталоном. Тесты были выполнены для разной размерности шифртекста (16 битов и 32 бита). Результаты тестирования приводятся в таблице 7.

Таблица 7. Результаты тестирования

Операция	16 битов		32 бита	
	Всего тестов	Успешно пройдено	Всего тестов	Успешно пройдено
Сложение	100	100	100	100
Разность	100	100	100	100
Умножение	100	100	100	100
Деление	100	100	100	100

Практическая апробация показала, что предложенные алгоритмы работают корректно.

Заключение

В результате диссертационного исследования было найдено решение актуальной научной задачи и достигнута поставленная цель, заключающаяся в расширении круга выполняемых гомоморфных криптографических операций посредством разработки новых методов и алгоритмов реализации гомоморфной математики над гомоморфно зашифрованными данными. Это подтверждается следующими полученными научными и практическими результатами:

1. Разработан новый метод, позволяющий выполнять гомоморфное деление на базе любого полностью гомоморфного алгоритма над целыми числами. Метод основан на представлении шифртекста в виде простой дроби, а всех гомоморфных операций – как операций над простыми дробями, для реализации которых достаточно гомоморфных операций суммы, разности и умножения. Для разработанного метода была выполнена программная реализация и получено свидетельство о государственной регистрации программы для ЭВМ № 2020611853.

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. Разработаны алгоритмы гомоморфной реализации 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. Выполнена программная реализация разработанных алгоритмов побитовых целочисленных операций сложения, разности, умножения и деления, а также разработанного метода гомоморфного сравнения чисел, представленных в виде массива гомоморфно зашифрованных битов. В качестве криптографического ядра программной реализации была использована библиотека полностью гомоморфного шифрования HElib для MacOS. Выполненное тестирование программной реализации подтвердило корректность работы разработанных алгоритмов.

5. Разработаны алгоритмы гомоморфной реализации 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. Выполнена оценка сложности вычислений для алгоритма над числами в формате с фиксированной точкой и в формате с плавающей точкой. Оценка приводится в числе гомоморфных операций над битами. Оценка показала, что операции гомоморфного сложения и вычитания над числами в формате с плавающей точкой намного сложнее аналогичных операций над числами в формате с фиксированной точкой. Однако операции умножения и деления, наоборот, имеют более низкую сложность. Следовательно, разработанные алгоритмы могут эффективней применяться в

алгоритмах обработки данных, содержащих большое число операций суммы и умножения, и обеспечивать более высокую точность вычислений, по сравнению с алгоритмами над числами в формате с фиксированной точкой.

6. Проанализированы возможности применения разработанных методов и алгоритмов и разработаны гомоморфные реализации алгоритмов масштабирования цифровой графики и алгоритма Гаусса. Для разработанного алгоритма гомоморфной реализации алгоритма Гаусса была выполнена программная реализация. Тестирование, выполненное на системах СЛАУ низших порядков (до степени 4 включительно), показало корректность разработанного алгоритма.

Материалы диссертационной работы были использованы в гранте РФФИ № 20-37-90140/20 на тему: “Разработка методов и средств гомоморфного шифрования для облачных сервисов”.

Публикации автора по теме диссертации

В рецензируемых журналах из перечня ВАК РФ

1. Бабенко, Л. К. Библиотека полностью гомоморфного шифрования целых чисел / Л. К. Бабенко, И. Д. Русаловский // Известия ЮФУ. Технические науки. – 2020. – № 2(212). – С. 218-227. – DOI 10.18522/2311-3103-2020-2-218-227.

2. Бабенко, Л. К. Метод реализации гомоморфного деления / Л. К. Бабенко, И. Д. Русаловский // Известия ЮФУ. Технические науки. – 2020. – № 4(214). – С. 212-221. – DOI 10.18522/2311-3103-2020-4-212-221.

3. Бабенко, Л. К. Масштабирование цифровых изображений с применением гомоморфного шифрования / Л. К. Бабенко, И. Д. Русаловский // Вопросы кибербезопасности. – 2021. – № 3(43). – С. 2-10. – DOI 10.21681/2311-3456-2021-3-2-10.

4. Русаловский, И. Д. Разработка методов гомоморфного деления / И. Д. Русаловский, Л. К. Бабенко, О. Б. Макаревич // Известия ЮФУ.

Технические науки. – 2022. – № 4(228). – С. 103-112. – DOI 10.18522/2311-3103-2022-4-103-112.

5. Бабенко, Л. К. Гомоморфная реализация метода Гаусса / Л. К. Бабенко, И. Д. Русаловский // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 33-40. – DOI 10.21681/2311-3456-2023-4-33-40.

6. Бабенко, Л. К. Побитовые гомоморфные операции над числами с плавающей точкой / Л. К. Бабенко, И. Д. Русаловский // Известия ЮФУ. Технические науки. – 2023. – № 4(234). – С. 26-34. – DOI 10.18522/2311-3103-2023-4-26-34.

В международных научных изданиях, индексируемых Scopus

7. Babenko, L. Homomorphic operations on integers via operations on bits / L. Babenko, I. Rusalovsky // Proceedings of the 2022 15th IEEE International Conference on Security of Information and Networks, SIN 2022. – 2022. – P. 01-04. – DOI 10.1109/SIN56466.2022.9970502.

В прочих изданиях

8. Русаловский, И. Д. Библиотека гомоморфного шифрования Helib / И. Д. Русаловский // III Всероссийская научно-техническая конференция "Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности" : материалы Всероссийской научно-технической конференции, Таганрог, 03-09 апреля 2017 г. : [в 2 ч.]. Ч. 1. – Ростов-на-Дону : Издательство Южного федерального университета, 2017. – С. 73-76.

9. Русаловский, И. Д. Проблема гомоморфного деления / И. Д. Русаловский // Студенческая наука для развития информационного общества : сборник материалов VII Всероссийской научно-технической конференции (г. Ставрополь, 26-28 декабря 2017 года) : [в 2 ч.]. Ч. 1. – Ставрополь : СКФУ, 2018. – С. 434-437.

10. Русаловский, И. Д. Гомоморфная реализация алгоритма Гаусса / И. Д. Русаловский // IV Всероссийская научно-техническая конференция "Фундаментальные и прикладные аспекты компьютерных технологий и

информационной безопасности" : материалы Всероссийской научно-практической конференции. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – С. 364-367.

11. Русаловский, И. Проблема полностью гомоморфной обработки целых чисел / И. Русаловский, Л. Бабенко // Безопасность информации и компьютерных сетей : материалы 12-й Международной научной конференции (SIN 2019), 12-15 сентября 2019 г., Сочи, Россия. – Сочи : РИЦ ФГБОУ ВО "СГУ", 2019. – С. 41-43.

12. Бабенко, Л. К. Гомоморфное шифрование. Теоретические основы. Области применения / Л. К. Бабенко, И. Д. Русаловский // Современные компьютерные технологии : сборник статей Научно-методической конференции, Таганрог, 25-29 февраля 2020 г. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – С. 58-65. – DOI 10.18522/mod.comp.tech.2020.1.9.

Свидетельства о государственной регистрации программ для ЭВМ

13. Свидетельство о государственной регистрации программы для ЭВМ № 2020611853 Российская Федерация. Реализация программы полностью гомоморфной обработки целых чисел : № 2020610864 : заявл. 31.01.2020 : опубл. 11.02.2020 / Л. К. Бабенко, И. Д. Русаловский ; заявитель федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (Южный федеральный университет).