ОТЗЫВ

официального оппонента на диссертацию 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»

В настоящее время в области создания систем распределенной обработки конфиденциальных данных можно выделить две важнейшие взаимосвязанные фундаментальные научные проблемы:

1.разработка фундаментальных математических основ для проектирования эффективных систем распределенной обработки конфиденциальной информации в гетерогенных средах:

2.разработка методов анализа и обоснования уровней защиты целостности и конфиденциальности информации в системах распределенных вычислений, использующих криптографические средства защиты.

Одним из возможных подходов к обеспечению эффективности, конфиденциальности и целостности данных является использование алгоритмов, реализующих гомоморфное шифрование. Общая идея решения указанных выше проблем в контексте облачных вычислений состоит в том, чтобы делегировать обработку данных, не представляя к ним непосредственного доступа. Гомоморфные вычисления, используемые для реализации вполне гомоморфного шифрования (Fully Homomorphic Encryption), способны решать указанную проблему. Гомоморфные вычисления позволяют третьей (возможно ненадежной) стороне обрабатывать информацию без раскрытия исходных данных. Гомоморфизмы алгебраических систем позволяют применять арифметические операции к зашифрованной информации, сохраняя результаты операций для открытой информации. Другими словами, гомоморфные вычисления потенциально позволяют обеспечивать совместимость двух критических для систем распределенной обработки данных факторов: вычислений и конфиденциальности.

Одним из основных ограничивающих факторов для построения эффективных, безопасных и надежных систем обработки данных является высокая вычислительная сложность алгоритмов. Многочисленные попытки оптимизации существующих схем гомоморфных вычислений имели лишь незначительный успех. Требуется комплексный подход к уменьшению вычислительной сложности, включающий проработку всех этапов проектирования системы обработки данных.

Анализ современных систем распределенной обработки конфиденциальной информации, теоретических и экспериментальных исследований ведущих

российских и зарубежных ученых позволяют сделать вывод, что на данный момент проблема снижения вычислительной сложности алгоритмов обработки данных остается открытой. Таким образом, тема диссертационного исследования Бабенко М.Г., посвященная разработке математических моделей, методов и алгоритмов обработки зашифрованных данных в распределенных средах, является актуальной.
Диссертация состоит из введения, 6 глав, заключения, библиографии из 378 наименований и 2 приложений. Общий объем основного текста работы – 325 страниц, включая 35 таблиц и 43 рисунка.
Во введении обосновывается актуальность работы, формулируются цель и задачи работы, приводятся выносимые на защиту результаты, а также информация об их апробации и публикациях.
В первой главе представлен обзор угроз информационной безопасности в распределенных средах хранения и обработки данных. Сформулированы цели исследования и проведено построение структурной модели обработки данных. Выделены основные угрозы безопасности и подходы к уменьшению вероятности получения несанкционированного доступа к конфиденциальным данным.
Во второй главе произведено построение высокопроизводительной вычислительно стойкой структуры доступа (Теорема 2.5.1.) со свойствами гомоморфизма. Показано, что предложенная адаптивная служба хранения данных обладает более высокой степенью, чем схема, основанная на пороговой структуре доступа. Проведено сравнение разработанной схемы, которое дает существенное преимущество относительно известных взвешенных схем по производительности. Проведен анализ безопасности предложенной схемы, показано, что она позволяет уменьшить вероятность несанкционированного доступа к данным при облачном сговоре (Таблица 15).
В третьей главе представлен обзор существующих методов сравнения чисел для гомоморфных вычислений над кольцом классов вычетов с делителями нуля. Разработан метод сравнения чисел (основанный на Теореме 3.8.1.) и произведено сравнение его сложности со сложностями самых быстрых известных методов, которое показало уменьшение задержки на 75% и снижение аппаратных затрат на 41% и более. Разработаны новые алгоритмы определения знака числа для гомоморфных вычислений над кольцами вычетов с делителями нуля для четных диапазонов (Теорема 3.9.2 и Алгоритм 3).
В четвертой главе исследованы подходы к выполнению операций определения знака числа и сравнения чисел. Разработаны новые методы и алгоритмы реализации операций определения знака и сравнения чисел. Предложен модифицированный нейросетевой метод определения знака числа, позволяющий более, чем 15.1 раза, повысить точность указанной операции в окрестности проблемной точки $x=0$. Доказаны теоремы, в которых проводится уточнение оценки степени интерполяционного многочлена функции определения знака числа (Теорема 4.1.1) и функции сравнения чисел (Теорема 4.4.1) над простым полем. Доказано, что не существует многочленов наилучшего приближения функции знака числа степени

$n \geq 1$ над полем действительных чисел, являющихся четными функциями (Теорема 4.8.2.).

В пятой главе рассмотрены три формы ранга числа: классическая форма ранга, следующая из Китайской теоремы об остатках, нормализованный ранг числа и ранг числа, построенный с использованием функции ядра Акушского. Исследован вопрос об интерполяции функции ранга числа с помощью алгебраических многочленов (Теорема 5.2.1., Теорема 5.2.2. и Теорема 5.2.3). Предложен эффективный метод вычисления ранга числа, основанный на использовании функции ядра Акушского, не содержащей критических ядер. Доказана теорема, дающая оценку верхней и нижней границ разрядности констант при использовании приближенного метода для вычисления ранга (Теорема 5.4.1. и Следствие 5.4.1 (верхняя граница), Следствие 5.4.2 (нижняя граница)). Разработанный метод вычисления ранга числа позволяет сократить объем вычислений с одновременным увеличением скорости вычисления ранга числа. Показаны пути осуществления контроля результата обработки закодированных чисел, основанные на свойствах ранга (Теорема 5.3.1., Теорема 5.3.2. и Теорема 5.3.3.).

В шестой главе разработана конфигурируемая, масштабируемая. двухуровневая пороговая схема, позволяющая производить хранение и обработку данных в мультиоблаке с высокой степенью надежности. Получена верхняя граница для количества обнаруживаемых и исправляемых ошибок при использовании традиционных пороговых двухуровневых схем и предложенных пороговых двухуровневых схем с обратным распространением ошибки (Теорема 6.3.1.). Выполнен сравнительный анализ производительности схем 2Lbp-RRNS с учетом полного цикла хранения данных для восьми реальных облачных хранилищ. Отметим, что при кодировании/декодировании данных в 2Lbp-RRNS, для реализации обратного преобразования вариативно может быть использован один из алгоритмов: Mignotte (основанный на Китайской теореме об остатках), MRC8 или MRC16 (основанные на переходе к обобщенной позиционной системе счисления и отличающиеся лишь размером окна, 8 или 16 бит, при реализации нейронной сети конечного кольца). Показано, что производительность MRC16 при кодировании-загрузке колеблется в диапазоне 0.406-0.837 МБ/с, а при выгрузке-декодировании в диапазоне 0.54-1.093 МБ/с в зависимости от параметров хранилищ. Для сравнения, показатели наиболее близкого по производительности алгоритма Mignotte при кодировании-загрузке колеблются в диапазоне 0.13-0.257 МБ/с, а при выгрузке-декодировании в диапазоне 0.16-0.292 МБ/с.

В заключении диссертации содержится подробное описание теоретических и экспериментальных результатов исследований, выносимых на защиту.

В диссертационной работе получены следующие основные новые научные результаты:

1.Разработана теория построения многочленов наилучшего приближения функции определения знака числа, что улучшает и расширяет известные результаты.

2.Предложен метод вычисления многочленов наилучшего приближения и решена задача об их количестве.
3.Разработана теория сравнения зашифрованных чисел и определения их знака над кольцом с делителями нуля.
4.Выделен класс монотонных функций ядра Акушского. Решена проблема возникновения критических ядер.
5.Модифицированы методы контроля выполнения арифметических операций с зашифрованными данными с использованием ранга числа.
6.Разработан метод обнаружения и исправления ошибок в двухуровневом СОК с использованием расстояния Хэмминга.
7.Предложены оригинальные методы и алгоритмы повышения надежности и безопасности хранимых и обрабатываемых данных в распределенных средах.
8.Построены многочлены, использующие интерполяционные многочлены Лагранжа, позволяющие определять знак числа и сравнивать числа над простым полем, уточнены их степени.
9.Предложена 2Lbp-RRNS конфигурируемая масштабируемая двухуровневая структура доступа на основе избыточной системы остаточных классов (ИСОК), допускающая реализацию гомоморфных вычислений и позволяющая осуществлять параллельную обработку данных с сохранением их конфиденциальности.
10.Разработаны алгоритмы кодирования и декодирования данных в 2Lbp-RRNS для улучшения эффективности обработки данных в распределенных средах.
Диссертационная работа имеет теоретический характер. Достоверность полученных результатов обусловлена корректностью математических определений и доказательств, анализом эффективности разработанных моделей и алгоритмов, а также апробацией результатов на международных и всероссийских научных конференциях. Полученные в ходе диссертационного исследования результаты согласуются с приведенными численными экспериментами. По теме диссертации автором было опубликовано 89 статей, в том числе 36 статей в журналах из списка, рекомендованного ВАК РФ, или индексируемых в международных базах Scopus и/или Web of Science, 53 работы в сборниках трудов всероссийских и международных конференций.
Практическая значимость результатов работы подтверждается 26 свидетельствами о государственной регистрации программ для ЭВМ и 12 патентами на изобретения.
В диссертационной работе необходимо отметить следующие недостатки:
- При описании экспериментов в диссертационной работе не во всех случаях полностью описаны технические характеристики стенда для моделирования. Например, при описании программной реализации блочного шифра AES на графическом процессоре отсутствует описание характеристик системы.
- В рисунках диссертационной работы имеются неточности, несколько затрудняющие чтение материала. Например, в легенде рисунка 1 не указано пояснение к маркеру зеленого цвета.

- Представляется не совсем удобным использовать для конечных полей обозначение Z_m, являющееся стандартным для колец вычетов. В случае использования необходимо давать пояснение, что m=p-простое число.
- В диссертационной работе при значительном количестве рассматриваемых и используемых понятий и параметров отсутствует список обозначений.
- В тексте и формулах диссертационной работы имеется некоторое количество опечаток и неточностей.

Указанные недостатки не влияют на общую положительную оценку диссертации.

Диссертационная работа Бабенко М.Г. на соискание ученой степени доктора физико-математических наук является научно-квалификационной работой, в которой изложены новые научно обоснованные методы проектирования систем распределенной обработки данных с использованием гомоморфного шифрования, являющиеся существенным вкладом в решение фундаментальной проблемы обеспечения эффективности, целостности и конфиденциальности в системах распределенной обработки и хранения информации. Тема и основные результаты диссертации соответствуют паспорту специальности ВАК РФ 2.3.5 (05.13.11). Автореферат правильно и полно отражает содержание диссертации.

Диссертационная работа «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах» отвечает всем 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 специальности 2.3.5. (05.13.11).

Официальный оппонент, член-корреспондент
Академии криптографии РФ, д.ф.-м.н., доцент
кафедры информационной безопасности
факультета ВМК МГУ имени М.В.Ломоносова О.А.Логачев

«18» ноября 2022г.