

УТВЕРЖДАЮ

~~Метелица~~ директор

~~доктор химических наук~~

___ А.В. Метелица

23

___ 10 ___ 2025 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного автономного образовательного
учреждения высшего образования

«Южный федеральный университет» (ЮФУ)

на диссертационную работу

Ширяева Егора Михайловича

**«Математическая модель, методы и алгоритмы эффективной
реализации искусственных нейронных сетей, сохраняющих
конфиденциальность»,**

представленную на соискание учёной степени

кандидата физико-математических наук

по специальности 2.3.5. Математическое и программное обеспечение
вычислительных систем, комплексов и компьютерных сетей

Диссертационная работа Ширяева Е.М. посвящена исследованию и разработке методов и алгоритмов выполнения характерных для искусственных нейронных сетей операций над конфиденциальными данными. В работе стандартные методы и функции искусственных нейронных сетей адаптированы для обработки зашифрованных данных и реализованы на языке Python. Эффективность разработанных методов подтверждена сравнением с существующими подходами к конфиденциальной обработке данных, соответствующий функционал добавлен в разработанный программный комплекс, который предназначен и может быть использован для проектирования и тестирования искусственных нейронных сетей, сохраняющих конфиденциальность.

Актуальность темы диссертационной работы

Развитие классических методов машинного обучения и различных моделей искусственных нейронных сетей привело к тому, что методы искусственного интеллекта стали использоваться не только для решения

узконаправленных специализированных задач, но и для широкого круга задач различных сфер деятельности человека. С увеличением возможностей искусственного интеллекта возросла вычислительная сложность решаемых с его помощью задач, что привело к дефициту вычислительных мощностей, как у рядового пользователя, так и у малого и среднего бизнеса.

Наиболее рациональным способом снижения затрат на необходимые вычислительные ресурсы является применение облачных технологий, а именно услуг облачных провайдеров. Однако, в данном случае возникает проблема с удалённой обработкой конфиденциальных данных в облаке: с одной стороны, пользователь не может передать конфиденциальные данные в публичное облако для обработки, так как не желает (или не имеет права) их рассекретить, с другой стороны, провайдер не может передать веса модели пользователю, так как потратил немалые средства для ее обучения.

Выходом из сложившейся ситуации является удалённая обработка данных в зашифрованном виде. Данный механизм реализуется посредством гомоморфного шифрования, поддерживающего, как правило, операции умножения и сложения. Поскольку реализация функционала искусственных нейронных сетей выходит далеко за рамки указанного базиса операций, требуется её адаптация с учётом сохранения результатов операций над зашифрованными данными.

Отдельно стоит отметить, что в эпоху перехода к квантовым вычислениям, именно гомоморфное шифрование претендует на роль основного стандарта обеспечения безопасности, так как с высокой долей вероятности после окончания данного перехода современные протоколы утратят свою актуальность, что в свою очередь подчеркивает актуальность данного исследования.

Диссертационная работа Ширяева Е.М. посвящена решению актуальной задачи – исследованию и разработке математической модели, методов и алгоритмов для повышения эффективности реализаций искусственных нейронных сетей, сохраняющих конфиденциальность на основе схем полностью гомоморфного шифрования.

Структура и основное содержание диссертационной работы

Диссертация имеет логичную структуру, что даёт возможность последовательно и полно исследовать предложенные в работе методы и алгоритмы. Она состоит из введения, трёх глав, заключения, списка обозначений и сокращений, списка литературы, содержащего 186 наименований. Объем основного текста работы составляет 156 страниц, включая 39 рисунков и 6 таблиц.

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи работы, выбраны объект и предмет исследования, показаны научная новизна, практическая ценность полученных результатов, приведены основные положения, выносимые на защиту.

В первой главе рассмотрены распределённые вычислительные системы, а именно облачные и туманные вычисления. Проведён анализ их безопасности, выявлены проблемы конфиденциальности таких систем. Проанализировано применение методов искусственного интеллекта в публичных распределённых системах. Представлен обзор основных схем гомоморфного шифрования, как инструмента обеспечения конфиденциальности при удалённой обработке данных, а именно схем TFHE, CKKS и BFV.

Во второй главе определены язык программирования и основные библиотеки для проведения дальнейших исследований: Python и TenSEAL, Concrete-ML соответственно. Исследованы методы матричного умножения, сохраняющего конфиденциальность. Сформулированы и доказаны теоремы об умножении зашифрованной матрицы на открытую и об аппроксимации функции искусственной нейронной сетью. Предложена модификация гомоморфного умножения матрицы зашифрованных конфиденциальных входных данных на открытую матрицу параметров, использующая доказанные в теоремах положения и позволяющая сократить вычислительную сложность свёрточных нейронных сетей, сохраняющих конфиденциальность. Проведено исследование методов дистилляции и квантизации свёрточных нейронных сетей для различных схем гомоморфного шифрования.

В третьей главе представлено экспериментальное исследование различных моделей свёрточных нейронных сетей, сохраняющих конфиденциальность, с различными функциями активации, методами дистилляции и квантизации, схемами полностью гомоморфного шифрования, для различных входных данных. Показано, что в большинстве случаев схема TFHE обрабатывает данные быстрее в среднем на 50%, однако CKKS имеет более высокую точность распознавания, в среднем на 5%, притом что TFHE зачастую не может обеспечить точность выше 90%. Установлены оптимальные конфигурации в зависимости от размера входных данных. Разработан программный комплекс для проектирования свёрточных нейронных сетей, сохраняющих конфиденциальность, включающий разработанные методы и алгоритмы.

В заключении подведены итоги и обобщены результаты проведенных исследований. Предложенная математическая модель, методы и алгоритмы

позволяют не только расширить спектр задач, решаемых искусственными нейронными сетями на удаленных облачных сервисах, но и повысить эффективность решений с точки зрения вычислительной сложности и потребления памяти за счет оптимизации искусственных нейронных сетей и математического аппарата обработки конфиденциальных данных.

Основные результаты диссертационной работы

1. Разработан метод матричного умножения, который повышает быстродействие за счет уменьшения количества гомоморфных операций при сохранении конфиденциальности данных пользователя, уменьшая вычислительную сложность алгоритма с $O(n^4)$ до $O(n^2)$.

2. Модифицирован метод дистилляции, который использует коалицию учителей для уменьшения размеров целевой сети, что влечет за собой сокращение потребления памяти примерно в 1500 раз, уменьшение времени обработки данных в среднем в 30 раз, при уменьшении доли верных классификаций от 0.5% до 1%.

3. Выполнена адаптация методов квантизации, которая позволяет применять целочисленные и логические схемы полностью гомоморфного шифрования для построения нейронных сетей, сохраняющих конфиденциальность, с большей эффективностью с точки зрения потребления памяти более чем в 3.5 раза и уменьшения времени обработки данных на 20%.

4. Разработана функция активации с обучающимися коэффициентами, позволяющая повысить долю верных классификаций в среднем на 1.5% по сравнению с функциями, реализованными в библиотеках TenSEAL и Concrete-ML.

5. Разработан комплекс программ и алгоритмов для проектирования и исследования приближенных функций активации, позволяющий построить модель под конкретную задачу, повысить ее эффективность, а также расширить область применения для решения прикладных задач, требующих сохранения конфиденциальности.

Достоверность полученных результатов

Достоверность полученных в диссертации результатов подтверждается проведенным сравнительным анализом разработанных методов и алгоритмов с известными ранее с точки зрения потребляемой памяти и скорости обработки данных. Результаты диссертационного исследования прошли апробацию на конференциях и иных научных мероприятиях всероссийского и международного уровней, а также в 29 научных публикациях, среди

которых 4 в рецензируемых журналах, рекомендованных ВАК, 8 публикаций, индексируемых в базах научных работ Scopus и Web of Science, и 15 в тезисах докладов конференций. Кроме того, получены 3 свидетельства о государственной регистрации программ для ЭВМ.

Практическая значимость

Разработанные в диссертационном исследовании математические модели, методы и алгоритмы могут быть использованы в качестве основы для реализации искусственных нейронных сетей, сохраняющих конфиденциальность, т.е. обрабатывающих данные в зашифрованном виде. Полученные результаты и разработанный программный комплекс позволяют строить и анализировать модели для применения в прикладных областях с повышенными требованиями к конфиденциальности данных, как, например, здравоохранение, финансовый, банковский сектор и т.д.

Замечания

1. При описании операции умножения на зашифрованную матрицу (Параграф 2.2) опущены операции взятия индексов по модулю, о чем следовало бы дополнительно упомянуть в тексте. Кроме того, некоторые обозначения операций требуют пояснения, например, « Un^{-1} » (стр. 54-55).

2. Опечатка в формуле (2.12): « $p(x) = x^n \cdot \alpha_1 + x^{n-1} \cdot \alpha_2 + \dots + x^1 \cdot \alpha_n + \alpha_0$ ».

3. Ошибки и/или опечатки в Алгоритме 3.18. и Алгоритме 3.19 (стр. 105) – вход: не указано количество каналов, для «*input_tensor*», для «*weights_{conv}*» перепутано количество каналов на входе и выходе, вместо одного параметра α должно быть два α_{conv} и α_{layer} , для свёрточного и полносвязного слоев соответственно.

4. Алгоритм 3.24 представлен не полностью (стр. 108).

5. Перепутаны цвета колонок на Рисунке 3.18.

6. В работе нет сценариев атак на нейронные сети, сохраняющие конфиденциальность и методов противодействия им.

Заключение

Указанные замечания не снижают научную и практическую ценность диссертационной работы. Диссертация является законченным научным исследованием, написанным на высоком уровне. Результаты диссертационного исследования представлены в статьях автора, а также докладывались на всероссийских и международных конференциях. Автореферат диссертации корректно и полно отражает содержание работы.

Диссертационная работа соответствует требованиям ВАК РФ, предъявляемым к диссертациям по специальности 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а её автор, Егор Михайлович Ширяев, заслуживает присуждения учёной степени кандидата физико-математических наук по этой специальности.

Отзыв подготовлен профессором кафедры прикладной математики и программирования, доктором технических наук (05.13.18. Математическое моделирование, численные методы и комплексы программ) Анатолием Борисовичем Усовым (344090, г. Ростов-на-Дону, ул. Мильчакова, 8А, тел. раб.: +7(863)2975411, эл. почта: abusov@sfedu.ru).

Отзыв обсуждён и утверждён на заседании кафедры прикладной математики и программирования Института математики, механики и компьютерных наук им. И.И. Воровича Южного федерального университета от 28 октября 2025 г., протокол №4. Присутствовало на заседании 8 чел.

Результаты голосования: «за» – 8 чел., «против» – нет, «воздержались» – нет.

Заведующий кафедрой прикладной математики и программирования
Института математики, механики и компьютерных наук им. И.И. Воровича
ФГАОУ ВО «Южный федеральный университет»,

д.ф.-м.н., профессор

Г.А. Угольников

344090, г.Ростов-на-Дону, ул. Мильчакова, 8А
тел. раб. +7(863)297-54-11, e-mail: gaugolnickiy@sfedu.ru

Сведения об организации:

Федеральное государственное автономное образовательное учреждение
высшего образования «Южный федеральный университет»

Адрес: 344006 г. Ростов-на-Дону, ул. Б. Садовая, 105/42

Телефон: +7 (863) 218 40 00

E-mail: info@sfedu.ru

Веб-сайт: <https://www.sfedu.ru>