Российский федеральный ядерный центр –
Всероссийский научно-исследовательский
институт экспериментальной физики

РФЯЦ-ВНИИЭФ

РОСАТОМ

Russian Federal Nuclear Center –
All-Russian Research Institute of
Experimental Physics



XX МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

СУПЕРВЫЧИСЛЕНИЯ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

Саров
5-9 октября 2026

ТЕЗИСЫ

XX INTERNATIONAL CONFERENCE

SUPERCOMPUTING AND MATHEMATICAL MODELING

Sarov
October 5-9, 2026

ABSTRACTS

Российский федеральный ядерный центр –
Всероссийский НИИ экспериментальной
физики

Russian Federal Nuclear Center –
All-Russian Research Institute
of Experimental Physics

ГОСКОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

STATE CORPORATION FOR ATOMIC ENERGY «ROSATOM»

XX Международная конференция

СУПЕРВЫЧИСЛЕНИЯ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

05 – 09 октября 2026

ТЕЗИСЫ

XX International Conference

SUPERCOMPUTING AND MATHEMATICAL MODELING

October 05 – 09, 2026

ABSTRACTS

Саров
2026

УДК 519.6; 519.7
ББК 22.18в6
С 89

С 89 **Супервычисления и математическое моделирование**. XX Международная конференция. Тезисы – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2026. – 272 с.: ил.

ISBN 978-5-9515-0639-9

Сборник содержит тезисы докладов, представленных на XX Международной конференции «Супервычисления и математическое моделирование»

УДК 519.6; 519.7
ББК 22.18в6

ISBN 978-5-9515-0639-9

© ФГУП «РФЯЦ-ВНИИЭФ», 2026

ОРГАНИЗАЦИИ–УЧАСТНИКИ

- Российский федеральный ядерный центр – Всероссийский НИИ экспериментальной физики», Саров
- АО «Атомэнергопроект», Санкт-Петербург
- Волгоградский государственный технический университет, Волгоград
- Воронежский институт высоких технологий, Воронеж
- Всероссийский научно-исследовательский институт автоматики им. Н. Л. Духова, Москва
- Всероссийский научно-исследовательский институт по эксплуатации атомных электростанций, Москва
- Институт автоматики и электрометрии СО РАН, Новосибирск
- Институт вычислительной математики им. Г. И. Марчука РАН, Москва
- Институт вычислительной математики и математической геофизики СО РАН, Новосибирск
- Институт математики им. С. Л. Соболева СО РАН, Новосибирск
- Институт математики и механики им. Н. Н. КрасовскогоУрО РАН, Екатеринбург
- Институт механики МГУ им. М. В. Ломоносова, Москва
- Институт проблем безопасного развития атомной энергетики РАН, Москва
- Институт проблем искусственного интеллекта, Донецк
- Институт проблем механики им. А. Ю. Ишлинского РАН, Москва
- Институт проблем управления им. В. А. Трапезникова РАН, Москва
- Институт системного программирования РАН, Москва
- Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ, Казань
- Казанский (Приволжский) федеральный университет, Казань
- Московский государственный университет им. М. В. Ломоносова, Москва
- Московский физико-технический институт (национальный исследовательский университет), Долгопрудный
- Научно-исследовательский и конструкторский институт энерготехники им. Н. А. Доллежаля, Москва
- Научно-технологический университет «Сириус», ФТ Сириус
- Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского, Нижний Новгород
- Национальный исследовательский технологический университет «МИСиС», Мос
- Национальный исследовательский ядерный университет «МИФИ», Москва
- Нижегородский государственный технический университет им. Р. Е. Алексеева, Нижний Новгород
- Нижегородский институт управления — филиал РАНХиГС, Нижний Новгород
- НИУ «Высшая школа экономики», Москва
- НИЦ супер-ЭВМ и нейрокомпьютеров, Таганрог
- Новосибирский национальный исследовательский государственный университе Новосибирск
- Новосибирский государственный технический университет, Новосибирск
- Новосибирский центр информационных технологий «Унипро», Новосибирск
- АО «НПО «Сплав» имени А. Н. Ганичева», Тула
- ОКБ «Гидропресс», Подольск

Каплина Д.А., Боков Д.Н., Мотор М.А.
ВЕСЛО. Сервисная система. Область применимости и архитектура……

Клепцова Л.А.
Модульный подход к решению уравнений математической физики с параметризованными граничными условиями на основе PINN……

Князьков В.С., Федюнин Р.Н., Исупов К.С.
Доверенные системы исскуственного интеллекта на основе нейронных сет с обработкой данных в системах остаточных классов: концепция и пра реализации……

Константинова Е.П.
Автоматический анализ микроструктуры WC-Co без ручной разм универсальная предобученная модель и теоретически обоснованный алг выделения зерен……

Коротков А.В., Крутякова О.Л., Козелков А.С., Курулин В.В.
Метод моделирования обтекаемых тел с вращающимися элементами в н несжимаемой жидкости на произвольных неструктурированных сетках……

Котмакова А.А., Авдеев Е.Э., Капица Д.В.
CFD анализ ветровой нагрузки на здания ядерного острова АЭС «Пакш-II»

Кравченко К.Н.
Расчет гидродинамических характеристик обтекания подводного аппарата в ПО Логос-Аэрогидро. Методика и использование в работах АО «СПМБМ «Малахит»……

Краснопольский Б.И.
Об оптимизации параметров методов решения систем линейных алгебраич уравнений для эволюционных задач……

Краюхин С.А., Володина Н.А., Воронков Р.А., Забусов П.В., Князев В.Н., Трунов Ширшова М.О.
Численное моделирование горения порохов в программном модуле Логос Прочность пакета программ Логос……

Криворотько О.И., Зятьков Н.Ю., Неверов А.В.
Физически-информированный алгоритм глубокого обучения для ре многопопуляционной задачи среднего поля в эпидемиологии……

Кругликов Ю.С., Кетлеров В.В., Ачаковский О.И., Авдеенков А.А.
Численное моделирование распространения водорода и горения натрия в помещениях АС при обосновании водородной взрывозащиты РУ БН……

ДОВЕРЕННЫЕ СИСТЕМЫ ИССКУСТВЕННОГО ИНТЕЛЛЕКТА НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ С ОБРАБОТКОЙ ДАННЫХ В СИСТЕМ ОСТАТОЧНЫХ КЛАССОВ: КОНЦЕПЦИЯ И ПРАКТИКА РЕАЛИЗАЦИИ

В. С. Князьков, Р. Н. Федюнин, К. С. Исупов

Пензенский государственный университет, Пенза

Классический инференс нейронных сетей предполагает использование крипто чески незащищенного пространства слоев, а также незащищенных данных, весов и с ний [1]. Это создает возможность для искажения промежуточного или конечного резу вычислений либо для перехвата информации третьей стороной [1]. Традиционным под к защите является применение средств криптографической защиты, что приводит к жанию модели и повышению сложности ее эксплуатации [1].

В последние годы активно развиваются схемы полностью гомоморфного шифр (FHE), такие как BFV и CKKS, позволяющие выполнять вычисления над зашифрова данными. Однако эти подходы требуют добавления управляемого криптографи шума и реализации сложных операций его контроля, что приводит к значительным лительным накладным расходам.

Предложенный авторами метод на основе формата FPRNS (Floating-Point Number System) и модифицированной архитектуры LeNet-5 использует систему оста классов (СОК) для гомоморфного представления данных, обеспечивая линейность оп В отличие от криптографических схем FHE, разработанный подход решает проблему данных и ускорения вычислений на уровне представления самих данных, а не чере ление управляемого криптографического шума. СОК в представленной работе явля новой метода, а не просто оптимизацией, как в «Full-RNS» версиях BFV/CKKS.

Формат данных FPRNS представляет собой оригинальную разработку ав коллектива [2]. Мантисса числа представлена в виде набора остатков по модулям вы системы, порядок хранится отдельно в двоичном виде. Ключевые операции: Round ление мантиссы с использованием интервально-позиционной характеристики; Adjus ректировка остатков мантиссы после немодульных операций.

Негомоморфная модель использует тип данных FP16/FP32 [3, 4, 5] и эталон дель LeNet-5 [4] с датасетом MNIST [5]. Гомоморфная модель – модифицированна с заменой операций сложения/умножения на гомоморфные аналоги FPRNS, вынос ций активации и пулинга на клиентскую сторону, адаптацией весов и смещений по

Клиент гомоморфной модели генерирует набор модулей СОК (ключ гомо вычислений), загружает MNIST и веса, передает их на сервер в гомоморфном ви просу сервера выполняет негомоморфные операции (Round, Adjust, пулинг, активац вер оперирует исключительно гомоморфными операциями и типом FPRNS. На этап ализации сервер настраивает слои CNN с использованием гомоморфных весов и с после чего приступает к обработке гомоморфных данных.

Современные схемы FHE (BFV, CKKS) основаны на RLWE с управл требуют релинеаризации и рескейлинга, имеют за

...ход основан на гомоморфном представлении данных в СОК, использует операции Round ...ighost, решает проблему предотвращения переполнения динамического диапазона и де...монстрирует замедление около 77x.

Экспериментальным стендом для проверки гипотиз и получения числовых результа...ов является сервер – Intel Core i7-1165G7 (2.8 GHz), 64 GB RAM, Ubuntu 22.04; клиент – ...el Core i7-1165G7 (2.8 GHz), 16 GB RAM, Ubuntu 22.04; сеть – Gigabit Ethernet; датасет – ...IST (60 000 обучающих, 10 000 тестовых изображений). Точность негомоморфной мо... – 98.7 %, гомоморфной – 98.1 % (падение на 0.6 %).

На стороне сервера реализуется 96 % операций. Оставшиеся 4 %: негомоморфные ...ерации реализуются на стороне клиента (4 %). Общее время гомоморфного инференса ...вышает негомоморфный примерно в 77 раз, что лучше опубликованных данных для клас...ических FHE-схем (100–200x и выше) [6, 7, 8].

Ограничением предложенной модели являются: негомоморфные операции, которые ...ебуют взаимодействия с клиентом (задержки); выбор набора модулей СОК, который явля... NP-трудной задачей; точность снижается на 0.6 %; модель безопасности уступает FHE ...ступна для сценариев с пассивным перехватом).

Перспективным направлением дальнейших исследований авторы видят вынос акти...ий на сервер через полиномиальную аппроксимацию, эвристический подбор модулей ...К, адаптация для LLM, гибридное сочетание FPRNS с классическими FHE-схемами.

В заключение отметим, что в статье представлена и экспериментально подтверждена ...ель гомоморфного инференса на основе FPRNS [9, 10, 11, 12] и модифицированной ...Net-5. Результаты (96% операций на сервере, замедление 77x) демонстрируют эффектив...ть подхода. В отличие от BFV/CKKS, метод использует СОК как основу гомоморфного ...ставления данных, избегая накладных расходов на управление шумом.

Список литературы

1. Pindado Z., Spendlhofer T., Allam M., et al. SoK of Private Deep Neural Network ...ference with Approximate Fully Homomorphic Encryption // Cryptology ePrint Archive. – 2026.
2. Isupov K., Knyazkov V. Interval estimation of relative values in residue number sys... // Journal of Circuits, Systems, and Computers. 2018. T. 27. № 1. C. 1850004.
3. Number Systems for Deep Neural Network Architectures [Электронный ресурс]. – ...ежим доступа: https://books.google.com (дата обращения: 10.06.2026).
4. LeCun Y., Bottou L., Bengio Y., Haffner P. Gradient-based learning applied to doc...ment recognition // Proceedings of the IEEE. – 1998. – T. 86, № 11. – C. 2278-2324.
5. Deng L. The MNIST database of handwritten digit images for machine learning ...search // IEEE Signal Processing Magazine. – 2012. – T. 29, № 6. – C. 141-142.
6. Roh H., Choi W.-S. Hyena: Optimizing Homomorphically Encrypted Convolution ...r Private CNN Inference // IEEE/ACM ICCAD 2025. – 2025.
7. Optimization of CNN inference for multi-image with fully homomorphic encryption ...Journal of King Saud University – Computer and Information Sciences. – 2025.
8. Yang Z., Niu C., Wei B., et al. RBOOT: Accelerating Homomorphic Neural Net...work Inference by Fusing ReLU within Bootstrapping // Cryptology ePrint Archive. – 2025.

РФЯЦ-ВНИИЭФ

РОСАТОМ

ISBN 978-5-9515-0639-9