УДК 004.056.5

ПРИМЕНЕНИЕ СХЕМ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

С. С. Скапцов, М. А. Кисель
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье исследуются вопросы обеспечения конфиденциальности при обработке данных в облачных средах с использованием технологии полностью гомоморфного шифрования. Данный метод позволяет выполнять математические операции над зашифрованными данными без их дешифрации на стороне сервера. Проведен анализ современных схем BFV и CKKS, рассмотрены механизмы накопления шума в шифротекстах и предложена модель защищенного взаимодействия, минимизирующая риски утечки информации на этапе вычислений.
Ключевые слова: криптография, гомоморфное шифрование, облачные вычисления, конфиденциальность данных, информационная безопасность, шифротекст, схема CKKS, вычислительная сложность, защита информации, алгоритм.

APPLICATION OF FULLY HOMOMORPHIC ENCRYPTION SCHEMES TO SECURE CLOUD COMPUTING

S.S. Skapcov, M.A. Kisel
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article investigates the issues of ensuring confidentiality during data processing in cloud environments using fully homomorphic encryption technology. This method allows performing mathematical operations on encrypted data without decryption on the server side. An analysis of modern BFV and CKKS schemes is carried out, mechanisms of noise accumulation in ciphertexts are considered, and a model of secure interaction that minimizes the risks of information leakage at the computation stage is proposed.
Keywords: cryptography, homomorphic encryption, cloud computing, data privacy, information security, ciphertext, CKKS scheme, computational complexity, information protection, algorithm.

Введение

Массовый переход к облачным вычислениям создает критическую уязвимость. Традиционные методы шифрования требуют расшифрования данных в оперативной памяти сервера для проведения операций. Это открывает доступ к конфиденциальной информации администраторам провайдера или вредоносному ПО. Полностью гомоморфное шифрование решает эту проблему, позволяя оперировать зашифрованными значениями. Актуальность темы обусловлена необходимостью внедрения концепции

«нулевого доверия» при обработке персональных и финансовых данных в распределенных сетях.

Основная часть

Математическая суть гомоморфного шифрования заключается в существовании гомоморфизма между кольцом открытых текстов и кольцом шифротекстов. Это означает, что результат операции над криптограммами после расшифрования будет идентичен результату аналогичной операции над исходными данными [3].

Современные эффективные схемы, таких как: BFV, CKKS, базируются на задаче обучения с ошибками в кольцах, что делает их устойчивыми к атакам квантовых компьютеров. При зашифровании в структуру данных вносится небольшой случайный параметр - «шум», обеспечивающий стойкость. Однако каждое гомоморфное умножение увеличивает уровень этого шума. При достижении критического порога корректное расшифрование становится невозможным, что требует применения процедуры "bootstrapping" (очистки шума), значительно замедляющей вычисления [1].

Для выбора оптимального решения при проектировании защищенных систем необходимо учитывать особенности различных криптографических схем. Основные характеристики наиболее востребованных алгоритмов представлены в таблице.

Сравнительный анализ схем гомоморфного шифрования
Comparative analysis of homomorphic encryption schemes

Схема	Тип данных	Особенности применения
BFV	Целые числа (Z)	Высокая точность, подходит для баз данных
BGV	Целые числа (Z)	Эффективна для глубоких вычислений (цепей)
CKKS	Числа с плавающей запятой (R/C)	Подходит для статистического анализа и машинного обучения, работает с приближенными значениями
TFHE	Логические значения (биты / Булевы цепи)	Самая быстрая процедура очистки шума (bootstrapping), идеальна для построения произвольной логики

В работе выделены два ключевых направления:

1. Схема BFV – ориентирована на точные вычисления с целыми числами, что необходимо для баз данных и финансового сектора.

2. Схема CKKS – поддерживает арифметику чисел с плавающей запятой. Она допускает контролируемую погрешность, что делает ее оптимальной для нейронных сетей и статистического анализа [2].

Защищенный цикл обработки включает генерацию ключей на стороне клиента, передачу шифротекстов в облако, выполнение сервером «слепых»

операций и возврат зашифрованного результата владельцу. Основным барьером остается вычислительная сложность, однако использование пакетной обработки данных (SIMD) и специализированных библиотек (Microsoft SEAL, OpenFHE) позволяет сократить временные затраты до приемлемых уровней в задачах Big Data

Заключение

Гомоморфная криптография – это фундамент приватных вычислений будущего. Несмотря на высокие требования к ресурсам, оптимизация алгоритмов и развитие аппаратных ускорителей делают практическое применение FHE реальным уже сегодня для медицины и финтеха. Дальнейшее развитие технологии позволит полностью устранить риск утечки данных на этапе их активной обработки.

Список использованных источников

1. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. - Санкт-Петербург : БХВ-Петербург, 2009. - 576 с.

2. Гентри, К. Полностью гомоморфное шифрование / К. Гентри // СТТ. - 2010. - № 3. - С. 50-55.

3. Мао, В. Современная криптография: теория и практика / В. Мао. - Москва : Вильямс, 2005. - 768 с.

References

1. Panasenko, S. P. Encryption Algorithms. Special Reference Book / S. P. Panasenko. - St. Petersburg: BHV-Petersburg, 2009. - 576 p.

2. Gentry, K. Fully Homomorphic Encryption / K. Gentry // STT. - 2010. - No. 3. - Pp. 50-55.

3. Mao, V. Modern Cryptography: Theory and Practice / V. Mao. - Moscow: Williams, 2005. - 768 p.

Сведения об авторах

Скапцов С.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Кисель М.А., курсанты курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Skapcov S.S., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics"

Kisel M.A., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics"