ОПТИМІЗАЦІЯ ПАКЕТНИХ ГОМОМОРФНИХ СХЕМ ДЛЯ ОБРОБКИ ВЕЛИКИХ МАСИВІВ ДАНИХ

Гущин Б.-Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи працюють з великими обсягами конфіденційних даних, і традиційне шифрування вимагає розшифрування перед обчисленнями, що підвищує ризик компрометації інформації. Повністю гомоморфне шифрування дозволяє виконувати обчислення над зашифрованими даними, зберігаючи їх конфіденційність. Попри це, практичне застосування таких схем обмежене високою обчислювальною складністю та великим розміром шифротекстів. Використання пакетних схем, де один шифротекст містить кілька повідомлень і операції виконуються одночасно, дозволяє значно підвищити ефективність гомоморфних обчислень.

Метою доповіді є дослідження способів оптимізації пакетних гомоморфних схем для роботи з великими масивами даних, зменшення обчислювальних витрат та підвищення ефективності криптографічних операцій.

Пакетні гомоморфні схеми забезпечують одночасну обробку декількох повідомлень у межах одного шифротексту. Кожен шифротекст представляється у вигляді матриці, елементами якої є поліноми над кільцем. Таке подання дозволяє виконувати арифметичні та логічні операції одночасно над усіма елементами матриці, значно зменшуючи кількість обчислень і витрати обчислювальних ресурсів.

Важливою особливістю є можливість перестановки слотів у матриці без розшифрування, що надає гнучкість у побудові складних обчислювальних алгоритмів та дозволяє ефективно реалізовувати паралельні операції.

Матричні поліноми також дозволяють більш рівномірно розподіляти шум, який накопичується під час послідовних гомоморфних операцій, що підвищує допустиму глибину обчислень без необхідності частого виконання bootstrap-перетворень [1]. Завдяки оптимальному розміщенню повідомлень у слотах матриці, можна забезпечити баланс між швидкістю обчислень та криптографічною стійкістю, що особливо важливо при роботі з великими масивами даних.

Сучасні дослідження показують, що вибір структурованих матричних поліномів і спеціальних алгоритмів кодування може ще більше підвищити ефективність пакетних схем. Оптимізація включає не тільки розмір пакетів, а й підбір параметрів кілець, поліноміальних базисів та стратегій розподілу повідомлень у слотах, що зменшує рівень шуму та дозволяє зберігати точність обчислень навіть при великій кількості операцій [2]. Важливим аспектом є вибір ступеня полінома та модуля, які безпосередньо впливають на рівень шуму і глибину допустимих обчислень.

Оптимізація пакетних гомоморфних схем включає вибір розміру пакетів, структури матриць і параметрів поліноміальних кілець. Великий розмір

пакетів дозволяє одночасно обробляти більше даних, проте підвищує рівень шуму, що потребує коректної балансування параметрів.

Застосування SIMD-підходу дає змогу ефективно використовувати сучасні багатоядерні процесори для паралельного виконання обчислень, що істотно прискорює обробку даних у реальному часі.

Варто також зазначити, що інтеграція адаптивного вибору параметрів матричних поліномів та автоматичне регулювання структури пакетів у реальному часі дозволяє динамічно балансувати між швидкістю обчислень і криптографічною стійкістю, підвищуючи загальну ефективність системи. [2-3].

Практична реалізація оптимізованих пакетних схем ефективна у хмарних обчисленнях та захищених базах даних, де необхідна обробка великих масивів конфіденційної інформації без розкриття даних. Прикладом може бути обчислення сум, середніх величин або простих статистичних характеристик на зашифрованих даних. Використання матричних поліномів дозволяє зменшити кількість шифротекстів та прискорити обчислення, що забезпечує ефективність і масштабованість криптографічних сервісів.

Проведений аналіз підтверджує, що оптимізація пакетних гомоморфних схем за допомогою матричних поліномів підвищує ефективність обробки великих обсягів даних.

Матричні структури дозволяють одночасно кодувати декілька повідомлень, рівномірно розподіляти шум та збільшувати глибину обчислень без частого bootstrap-перетворення [3, 4].

Оптимізація параметрів пакетів і структури матриць забезпечує баланс між продуктивністю та криптографічною стійкістю, що робить такі схеми перспективними для хмарних обчислень, захищених баз даних та систем делегованих обчислень.

Отримані результати підтверджують доцільність подальших досліджень щодо адаптивного вибору параметрів матричних поліномів і практичної реалізації пакетних схем у сучасних бібліотеках гомоморфного шифрування.

Список літератури

1. Гущин Б.-Д. І. Аналіз ефективності повністю гомоморфного шифрування шляхом використання матричних поліномів // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 4 т.]. Т. 2 : секції 3, 7. – Харків : НТУ "ХПІ", 2025. – С. 86-87.

2. Chen, Y., Huang, R., & Yang, B. (2022). Efficient batch fully homomorphic encryption with a shorter key from ring-lwe. *Applied Sciences*, *12*(17), 8420.

3. Hushchyn Bohdan-Danylo Analysis of Homomorphic Encryption Algorithms / Hushchyn Bohdan-Danylo // Computer and information systems and technologies : Seventh International Scientific and Techn. Confe., september 2024. – Kharkiv : NURE, 2024. – P. 56.

4. Белей, О. І. (2018) «Гомоморфне шифрування даних у хмарних сховищах методом матричних поліномів», Сучасний стан наукових досліджень та технологій в промисловості, (4 (6), с. 5–14. doi: 10.30837/2522-9818.2018.6.005.