АДАПТИВНИЙ ВИБІР ПАРАМЕТРІВ ПАКЕТНОГО ГОМОМОРФНОГО ШИФРУВАННЯ ДЛЯ ОБРОБКИ ЗАШИФРОВАНИХ ДАНИХ

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

Застосування повністю гомоморфного шифрування (ПГШ) дає змогу делегувати обробку конфіденційних даних без їх розшифрування на стороні виконавця. Однак практична продуктивність таких обчислень визначається не лише вибором криптосхеми, а й способом розміщення даних у слотах шифротексту, кількістю ротацій та допустимою мультиплікативною глибиною. У попередніх працях розглянуто можливості пакетного SIMD-кодування, матричних поліномів і скорочення питомих витрат обробки [1, 2]. Подальшим етапом є розроблення обґрунтованого способу добору параметрів для конкретної структури обчислень.

Метою доповіді є формування підходу до адаптивного вибору параметрів пакетного гомоморфного шифрування з урахуванням структури вхідних даних, вартості перестановок слотів, точності результату та вимог до криптографічної стійкості.

Запропоновано розглядати параметризацію пакетної схеми як задачу вибору конфігурації, що складається з типу шифрування, ступеня поліноміального модуля, ланцюга модулів коефіцієнтів, масштабу кодування, числа зайнятих слотів і способу їх розміщення. Для точних цілочисельних обчислень доцільно використовувати схеми класу BFV/BGV, тоді як для наближених операцій над дійсними числами - CKKS. При цьому збільшення числа доступних слотів саме по собі не гарантує прискорення, оскільки залежні між слотами обчислення потребують ротацій і додаткових ключів перемикання.

У межах запропонованого підходу спочатку визначається обчислювальний граф задачі: кількість додавань і множень, мультиплікативна глибина, операції агрегації, характер доступу до елементів та допустима похибка. Далі формуються допустимі криптографічні конфігурації, для яких оцінка стійкості відповідає заданому рівню безпеки за чинними рекомендаціями [3].

Конфігурації, що не забезпечують достатнього запасу рівнів або точності, виключаються з подальшого розгляду.

Для решти конфігурацій оцінюється сукупна вартість виконання: час кодування й шифрування, гомоморфних множень, ротацій, рескейлінгу або перемикання модулів, а також обсяг пам’яті для шифротекстів і службових ключів.

Доцільно порівнювати не лише абсолютний час виконання, а й питомі витрати на один корисний елемент пакета. Вибір конфігурації здійснюється за мінімальною оціненою вартістю за умови дотримання обмежень безпеки, точності та доступної пам’яті.

Особливу увагу приділено матрично-векторним операціям, поширеним у конфіденційній аналітиці. Для них пряме слотне розміщення може вимагати значної кількості циклічних зсувів. Тому пропонується порівнювати діагональне представлення матриць, блочне компонування й схеми групування ротацій. Зменшення їх кількості потенційно скорочує затримку, проте потребує врахування додаткових множень на відкриті маски та витрат пам'яті. Відтак перевага певного варіанта визначається конкретною формою матриці та цільовою апаратною платформою.

На відміну від фіксованої конфігурації пакетного шифрування, адаптивний вибір передбачає окреме планування структури слотів для різних класів навантажень. Для незалежних поелементних операцій пріоритетом є максимальне використання слотів, для агрегувань - зменшення кількості ротацій, для довгих ланцюгів множення - достатній запас рівнів і контроль похибки. Така постановка дозволяє уникнути некоректного припущення, що саме матричне подання автоматично зменшує криптографічний шум, його зростання визначається параметрами схеми та послідовністю виконуваних операцій.

Для перевірки підходу доцільно реалізувати серію відтворюваних експериментів у Microsoft SEAL або OpenFHE на задачах покомпонентного обчислення, підсумовування слотів і множення матриці на вектор. Порівняння з фіксованими конфігураціями необхідно проводити за часом обробки одного елемента, кількістю ротацій, споживанням пам'яті, розміром шифротекстів і точністю дешифрованого результату. Окремо має бути перевірена відповідність наборів параметрів вимогам безпеки [3, 4].

Отже, обґрунтовано підхід до адаптивного вибору параметрів пакетного ПГШ, що пов'язує алгебраїчну організацію слотів із властивостями обчислювального графа та обмеженнями криптосистеми. Наукова спрямованість подальшого дослідження полягає у формалізації критерію вибору конфігурації й експериментальному визначенні умов, за яких оптимізація слотного розміщення забезпечує виграш у продуктивності без зниження заданого рівня захисту. Числові характеристики такого виграшу потребують окремого експериментального підтвердження.

Список літератури

1. Гущин Б.-Д. І. Аналіз ефективності повністю гомоморфного шифрування шляхом використання матричних поліномів. Проблеми інформатизації: тези XIII міжнар. наук.-техн. конф., 27–28 листопада 2025 р. Харків, 2025. Т. 2. С. 86–87.

2. Гущин Б.-Д. І. Проблемні питання застосування гомоморфного шифрування. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези XV міжнар. наук.-техн. конф. 2025. Т. 3. С. 114–115.

3. Bossuat J.-P. et al. Security Guidelines for Implementing Homomorphic Encryption. IACR Communications in Cryptology. 2025. Vol. 1, No. 4. DOI: 10.62056/anxra69p1.

4. Chen Y., Huang R., Yang B. Efficient Batch Fully Homomorphic Encryption with a Shorter Key from Ring-LWE. Applied Sciences. 2022. Vol. 12, No. 17. Art. 8420.