Басістий В.П., аспірант,
Логош В.Д., магістрант
Західноукраїнський національний університет

АЛГОРИТМИ ГОМОМОРФНОГО ШИФРУВАННЯ

Алгоритми гомоморфного шифрування дозволяють виконувати обчислення над зашифрованими даними без їх розшифрування, отримуючи результат, який після розшифрування відповідає результату обчислень над відкритими даними. Ця технологія набуває дедалі більшої актуальності завдяки зростанню обсягів даних, потребі в конфіденційності та розвитку хмарних обчислень.

Алгоритм гомоморфного шифрування на основі "навчання з помилками" (Learning With Errors, LWE) є одним із широко досліджуваних підходів у сучасній криптографії, зокрема в контексті постквантової безпеки та гомоморфного шифрування. Він базується на математичній задачі, яка вважається стійкою навіть до атак квантових комп'ютерів.

LWE був запропонований Одедом Регевом у 2005 році і став основою для багатьох гомоморфних схем, включаючи частково гомоморфні (Partially Homomorphic Encryption, PHE) і повністю гомоморфні (Fully Homomorphic Encryption, FHE) системи [1, 2].

Основна ідея підходу "навчання з помилками" полягає в тому, щоб відрізнити випадкові лінійні рівняння від рівнянь, які мають невеликий "шум" (помилку), доданий до них. Ця складність використовується для створення криптосистем, які дозволяють шифрувати дані таким чином, що обчислення над ними (наприклад, додавання чи множення) можливі без розшифрування.

Алгоритми гомоморфного шифрування на основі LWE використовують математичні проблеми LWE для забезпечення безпеки і можливості виконання операцій над зашифрованими даними. Основні принципи роботи таких алгоритмів включають:

1) генерація ключів. Секретний ключ є випадковим вектором s. Відкритий ключ складається з множини пар (a, b), де $b = \langle a, s \rangle + e \bmod q$;

2) шифрування. Для шифрування повідомлення m, вибирається підмножина пар з відкритого ключа і комбінується їх з повідомленням. Результатом є зашифрований текст, який містить приховане повідомлення плюс невелику помилку;

3) розшифрування. Для розшифрування використовується секретний ключ для обчислення скалярного добутку, від якого потім віднімається зашифрований текст, щоб отримати повідомлення плюс помилку. Якщо помилка достатньо мала, її можна видалити, щоб отримати оригінальне повідомлення;

4) гомоморфні операції. Алгебраїчна структура зашифрованого тексту дозволяє виконувати операції додавання та множення над зашифрованими даними, які перетворюються на відповідні операції над відкритими даними після розшифрування.

Математично, схеми гомоморфного шифрування на основі LWE зазвичай працюють над кільцями поліномів, що дозволяє ефективно представляти та маніпулювати зашифрованими даними. Популярний підхід полягає у використанні кільцевої версії LWE (Ring-LWE або RLWE), яка забезпечує кращу ефективність порівняно з оригінальною проблемою LWE.

Одним з ключових викликів у гомоморфному шифруванні є управління шумом. Кожна гомоморфна операція, особливо множення, збільшує рівень шуму у зашифрованому тексті. Якщо шум стає занадто великим, правильне розшифрування стає неможливим. На основі LWE розроблено ряд алгоритмів гомоморфного шифрування, зокрема [2]:

BGV (Brakerski-Gentry-Vaikuntanathan). Алгоритм підтримує довільну кількість додавань та обмежену кількість множень, з ефективними методами контролю шуму.

BFV (Brakerski/Fan-Vercauteren). Алгоритм оптимізований для ефективного множення, що широко використовується в практичних реалізаціях.

CKKS (Cheon-Kim-Kim-Song). Алгоритм призначений для обчислень з наближеними числами, що дозволяє ефективно виконувати обчислення з наближеними результатами.

GSW (Gentry-Sahai-Waters). Алгоритм використовує матричну версію LWE для досягнення компактності гомоморфного множення.

Базуючись на математичній проблемі LWE, алгоритми гомоморфного шифрування забезпечують безпеку навіть проти квантових обчислень.

Список використаних джерел:

1. Doan, T. V. T., Messai, M. L., Gavin, G., Darmont, J. A survey on implementations of homomorphic encryption schemes. The Journal of Supercomputing. 2023. Vol.79(13). P.15098-15139.

2. Mahato, G. K., Chakraborty, S. K. A comparative review on homomorphic encryption for cloud security. IETE Journal of Research. 2023. Vol. 69(8). P.5124-5133.