АНАЛІЗ ЕФЕКТИВНОСТІ ПОВНІСТЮ ГОМОМОРФНОГО ШИФРУВАННЯ ШЛЯХОМ ВИКОРИСТАННЯ МАТРИЧНИХ ПОЛІНОМІВ

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

Зі зростанням обсягів хмарних обчислень актуальним стає питання забезпечення конфіденційності даних, що зберігаються та обробляються на зовнішніх серверах. Незважаючи на розвиток засобів доступу та безпеки, провайдери хмарних сервісів не гарантують повної відсутності ризику несанкціонованого доступу [1]. Тому виникає потреба в таких криптосистемах, які дозволяють здійснювати обчислення над інформацією, не розшифровуючи її.

Інструментом, що забезпечує таку властивість, є повністю гомоморфне шифрування, однак більшість відомих реалізацій страждають на надмірну обчислювальну складність. Одним із перспективних шляхів підвищення продуктивності є використання матричних поліномів та пакетного SIMD-кодування, що дозволяє одночасно виконувати операції над групами даних.

Метою доповіді є аналіз підходу до підвищення ефективності повністю гомоморфного шифрування (ПГШ) шляхом використання матричних поліномів і пакетного кодування, що дозволяє об’єднувати кілька відкритих текстів в один шифротекст для їх комплексної обробки у зашифрованому вигляді.

Гомоморфне шифрування є криптографічним примітивом, що викликає значний інтерес як у прикладному, так і в теоретико-математичному аспектах. Попри тривалу історію досліджень, низка ключових проблем цієї галузі досі лишається невирішеною. Гомоморфне шифрування має великий потенціал для застосування в сучасній криптографії та, ширше, у розробці математичних моделей і методів захисту інформації. Особливу практичну цінність становить можливість виконання обчислень безпосередньо над зашифрованими даними. У традиційних підходах конфіденційні дані шифруються перед зберіганням, а для виконання обчислень їх необхідно тимчасово розшифрувати, що створює потребу у використанні захищеного апаратного середовища та надійної інфраструктури керування секретними ключами. Натомість гомоморфне шифрування, за умови підтримки відповідних операцій, дозволяє здійснювати обчислення без розкриття даних, повністю усуваючи ризики, пов’язані з процесом їх розшифрування.

Основною сферою застосування повністю гомоморфних криптосистем є хмарні обчислення та інфраструктури аутсорсингу. Застосування ПГШ дозволяє зберігати дані на віддалених серверах виключно у зашифрованому вигляді та отримувати результати запитів також у зашифрованій формі, без потреби у проміжному розшифруванні інформації на стороні сервера.

Існує значна кількість протоколів взаємодії з базами даних, які забезпечують не лише конфіденційне отримання записів, а й приховане

отримання індексів елементів, що відповідають певним критеріям вибірки. Поряд із протоколами, що покладаються на повністю гомоморфне шифрування для виконання довільних операцій над зашифрованими даними, розробляються й інші схеми, у яких ПГШ використовується як інструмент для розв'язання специфічних криптографічних задач. До таких задач належать, перевірка делегованих обчислень та побудова стислих неінтерактивних доказів із нульовим розголошенням.

Можливість переставляти окремі слоти всередині одного шифротексту без його розшифрування суттєво розширює функціональні можливості гомоморфних систем [2]. Це уможливлює реалізацію стандартних машинних операцій у бітовому поданні, включаючи додавання, множення та логічний оператор XOR.

Практична значущість пакетного шифрування стала підґрунтям для включення його процедур до бібліотеки HElib, розробленої компанією IBM, яка є однією з найпоширеніших платформ для гомоморфних обчислень. У розглянутій криптосхемі відкриті тексти подаються у вигляді елементів кільця, тоді як шифротексти представляються матричними поліномами над цим самим кільцем. Шифрування передбачає кодування повідомлення у матрицю та формування матричного полінома із додаванням випадкової компоненти, що забезпечує семантичну криптостійкість.

Реалізація SIMD-шифрування може здійснюватися різними методами: на основі китайської теореми про залишки, [3] через використання множини різних власних значень або за допомогою інтерполяції матричних поліномів. Такий підхід є одним із найбільш гнучких, оскільки дає змогу контролювати ефективні SIMD-структури для гомоморфної обробки даних, зберігаючи можливість паралельного виконання операцій над векторами відкритих текстів.

Підходи до побудови пакетних повністю гомоморфних схем на основі матричних поліномів є перспективними для створення ефективних криптографічних механізмів.

Гомоморфне шифрування підтверджує свою актуальність як один із найбільш перспективних інструментів захисту інформації в умовах хмарних обчислень.

Список літератури

1. Рудий, С.В., Сєвєрінов, О.В. Дослідження моделі безпеки при використанні хмарних сервісів // ЧДТУ, ВА ЗС АР, УТіГН, НТУ "ХПІ", ХНУРЕ, "ПД ПКНДІ АП", 2022.

2. 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.

3. Xun Yi, Russell Paulet, and Elisa Bertino, "Homomorphic Encryption and Applications", Springer, 2014, pp. 1-213.