УДК 004.056.5

Чернюк О.К.
Салієва О.В.

ПОРІВНЯЛЬНИЙ АНАЛІЗ РІЗНОВИДІВ ГОМОМОРФНОГО ШИФРУВАННЯ

Вінницький Національний Технічний Університет

Анотація

В даній роботі розглянуто основні види гомоморфного шифрування. Наведено їх особливості, приклади, переваги та недоліки. На основі отриманих даних здійснено порівняльний аналіз досліджуваних видів гомоморфного шифрування.

Ключові слова: Захист, конфіденційність, гомоморфне шифрування.

Abstract

This paper discusses the main types of homomorphic encryption. Their features, examples, advantages and disadvantages are presented. On the basis of the obtained data, a comparative analysis of the studied types of homomorphic encryption is carried out.

Key words: Protection, privacy, homomorphic encryption.

Вступ

Гомоморфне шифрування є одним із найбільш перспективних методів забезпечення конфіденційності даних, дозволяючи виконувати обчислення над зашифрованою інформацією без необхідності її розшифрування. У даній роботі проаналізовано основні види гомоморфного шифрування, їхні особливості, переваги та недоліки. Розглянуто частково гомоморфне, додатково гомоморфне, мультиплікативне та цілком гомоморфне шифрування.

Дослідження

Частково гомоморфне шифрування є одним із найпростіших видів гомоморфного шифрування, яке дозволяє виконувати лише одну математичну операцію над зашифрованими даними – або додавання, або множення. Цей вид шифрування використовується в задачах, де обчислення є вузькоспеціалізованими, наприклад, підрахунок сум або множення зашифрованих значень. Серед найвідоміших алгоритмів, що реалізують частково гомоморфне шифрування, можна виділити RSA і Paillier [1].

Однією з основних переваг частково гомоморфного шифрування є його низькі обчислювальні витрати порівняно з більш універсальними підходами. Завдяки обмеженості до однієї операції, ці алгоритми мають меншу складність обчислень, що дозволяє застосовувати їх у задачах, які вимагають швидкості та ефективності. Крім того, такі алгоритми часто мають простішу реалізацію, що робить їх привабливими для впровадження в системах із обмеженими ресурсами, таких як пристрої IoT.

Проте обмеженість цього виду шифрування до однієї математичної операції є його основним недоліком. Неможливість виконання комбінованих обчислень, таких як послідовне додавання та множення, значно знижує його універсальність. Це ускладнює застосування частково гомоморфного шифрування у складніших сценаріях, таких як обробка даних у системах машинного навчання чи виконання багатоступеневих обчислень у хмарних середовищах [1].

Таким чином, частково гомоморфне шифрування є корисним для вузькофокусованих задач, де важливими є швидкість і низькі обчислювальні витрати, однак його обмеження до однієї операції значно звужує область його застосування в умовах сучасних високонавантажених інформаційних систем.

Додатково гомоморфне шифрування є більш універсальним підходом, ніж частково гомоморфне, оскільки дозволяє виконувати як операції додавання, так і множення, хоча й у обмеженій кількості. Цей вид шифрування спрямований на подолання обмежень, притаманних частковому гомоморфному шифруванню, і знаходить застосування у задачах, де потрібне поєднання базових арифметичних операцій. Прикладами алгоритмів, що реалізують додатково гомоморфне шифрування, є ранні версії шифрування Гентрі та алгоритми, засновані на граткових структурах (lattice-based) [2].

Основною перевагою додатково гомоморфного шифрування є можливість виконання як додавання, так і множення над зашифрованими даними. Це дозволяє вирішувати більш складні задачі, порівняно

з частковим гомоморфним шифруванням, і відкриває ширші можливості для застосування, зокрема у фінансових системах, де одночасно потрібні обчислення суми платежів та обчислення комісійних зборів. Такий підхід забезпечує кращу функціональність, що є важливою умовою для більш універсальних інформаційних систем.

Однак додатково гомоморфне шифрування має свої обмеження. Найбільш суттєвим недоліком є накопичення шуму в зашифрованих даних після кожної операції. Це явище обмежує кількість допустимих операцій, оскільки надмірний шум робить розшифрування даних неможливим. Для подолання цього обмеження необхідно виконувати періодичне "очищення" шуму за допомогою технік повторного шифрування, що значно збільшує обчислювальні витрати. Крім того, обчислювальна складність цього методу все ще залишається високою порівняно з традиційними методами обробки даних.

Таким чином, додатково гомоморфне шифрування є проміжним рішенням між частково гомоморфним та цілком гомоморфним шифруванням. Воно забезпечує більшу функціональність і універсальність, але має обмеження, пов’язані з накопиченням шуму та обчислювальною складністю. Це робить його придатним для задач, де потрібна помірна кількість операцій над зашифрованими даними, але не вистачає ресурсів для реалізації цілком гомоморфного шифрування [2].

Мультиплікативне гомоморфне шифрування є одним із базових видів гомоморфного шифрування, який підтримує виконання лише однієї операції – множення над зашифрованими даними. Цей підхід знайшов застосування у задачах, де основні обчислення можна звести до множення, наприклад, при аналізі статистичних даних або виконанні спеціалізованих математичних операцій. Серед алгоритмів, що реалізують мультиплікативне шифрування, найбільш відомими є RSA та ElGamal.

Однією з основних переваг мультиплікативного шифрування є його обчислювальна ефективність у задачах, орієнтованих виключно на операції множення. Завдяки обмеженню до однієї математичної операції, алгоритми цього типу мають відносно низьку складність і можуть бути реалізовані з меншою кількістю ресурсів. Наприклад, алгоритм ElGamal часто використовується у криптографічних системах, що вимагають захисту конфіденційних даних під час множення числових значень, таких як ключі шифрування або хеші [3].

Проте, як і частково гомоморфне шифрування, мультиплікативне має значні обмеження. Найважливішим недоліком є те, що воно підтримує виключно одну операцію. Це означає, що у випадках, коли для виконання задачі потрібні додавання або комбінація арифметичних операцій, мультиплікативне шифрування стає непридатним. Така обмеженість значно звужує сферу його застосування, роблячи його підходящим лише для вузькоспеціалізованих сценаріїв.

З огляду на переваги і недоліки, мультиплікативне гомоморфне шифрування є ефективним рішенням для задач із чітко визначеними вимогами до обчислень, які зводяться до множення. Проте його функціональна обмеженість унеможливлює використання у більш універсальних системах обробки даних, таких як багатофункціональні фінансові або аналітичні платформи. Це визначає його роль як специфічного, але важливого інструмента в арсеналі криптографічних технологій [3].

Цілком гомоморфне шифрування є найбільш універсальним і потужним видом гомоморфного шифрування, яке дозволяє виконувати такі арифметичні операції як додавання та множення над зашифрованими даними без обмежень на їх кількість. Ця властивість робить його унікальним серед інших видів гомоморфного шифрування і відкриває широкий спектр можливостей для безпечної обробки даних у різних сферах, таких як фінансові сервіси, медицина, машинне навчання та інші конфіденційні обчислення. Перший практичний алгоритм цілком гомоморфного шифрування був запропонований Крейгом Гентрі у 2009 році, і з тих пір ця технологія активно розвивається. Сучасні алгоритми, такі як Gentry's scheme та TFHE (TenSEAL), демонструють значний прогрес у продуктивності [4].

Основною перевагою цілком гомоморфного шифрування є можливість виконання складних обчислень над зашифрованими даними без їх розшифрування. Це надає змогу розробляти системи, що гарантують повну конфіденційність навіть у середовищах із підвищеним рівнем недовіри, наприклад, у хмарних обчисленнях. За допомогою цілком гомоморфного шифрування можна тренувати моделі машинного навчання або проводити аналітику великих даних, не розкриваючи вихідну інформацію. Крім того, цей вид шифрування забезпечує найвищий рівень безпеки завдяки своїй стійкості до криптоаналітичних атак [4].

Однак цілком гомоморфне шифрування має суттєві недоліки, які ускладнюють його широке впровадження. Головною проблемою є високі обчислювальні витрати, які значно перевищують

ресурси, необхідні для частково або додатково гомоморфного шифрування. Обчислення із використанням цілком гомоморфного шифрування є надзвичайно ресурсоємними через складність алгоритмів, особливо для великих обсягів даних. Крім того, виконання операцій вимагає значного обсягу пам'яті та часу, що обмежує застосування у реальному часі або на пристроях із низькими ресурсами [4].

Таким чином, цілком гомоморфне шифрування є перспективною технологією для завдань, які потребують максимальної універсальності та конфіденційності. Незважаючи на обмеження, пов'язані з продуктивністю, ця технологія активно вдосконалюється, і очікується, що у майбутньому її застосування стане більш доступним завдяки оптимізації алгоритмів і зростанню обчислювальних можливостей сучасних систем.

У таблиці 1 здійснено порівняння розглянутих видів гомоморфного шифрування.

Таблиця 1 – Порівняння основних видів гомоморфного шифрування

Вид шифрування	Операції	Приклади	Переваги	Недоліки
Частково гомоморфне	Або додавання, або множення	RSA, Paillier	Менші обчислювальні витрати	Обмеження до однієї операції
Додатково гомоморфне	Обмежене додавання і множення	Ранні алгоритми Gentry, Lattice-based	Підтримка обох операцій у обмеженій кількості	Обмежена кількість операцій через накопичення шуму
Мультиплікативне	Множення	RSA, ElGamal	Підходить для додатків з множенням	Обмеженість до множення
Цілком гомоморфне	Додавання та множення без обмежень	Gentry, TFHE	Підтримка будь-яких обчислень, найвищий рівень безпеки	Високі обчислювальні витрати, потребує багато ресурсів

Таким чином, в таблиці 1 продемонстровано різноманітність видів гомоморфного шифрування, кожен з яких має свої переваги та обмеження. Частково гомоморфне шифрування забезпечує ефективність для вузьких задач, додатково гомоморфне – баланс між функціональністю і продуктивністю, мультиплікативне – оптимальне для задач множення, а цілком гомоморфне пропонує універсальність за рахунок високих обчислювальних витрат. Вибір виду залежить від вимог до безпеки, ресурсоємності та складності обчислень.

Висновок

У даній роботі проаналізовано основні види гомоморфного шифрування, їхні особливості, переваги та недоліки. Частково гомоморфне шифрування демонструє ефективність у вузькоспеціалізованих задачах завдяки низьким обчислювальним витратам, однак обмежується однією операцією. Додатково гомоморфне забезпечує підтримку як додавання, так і множення, але має обмеження через накопичення шуму. Мультиплікативне шифрування, орієнтоване на операції множення, залишається релевантним у специфічних додатках. Найбільш універсальним є цілком гомоморфне шифрування, яке дозволяє виконувати будь-які арифметичні операції, хоча й вимагає значних обчислювальних ресурсів.

Результати дослідження демонструють, що вибір виду гомоморфного шифрування залежить від специфіки завдань та доступних ресурсів. Частково гомоморфне і мультиплікативне підходять для простих операцій, тоді як додатково і цілком гомоморфне відкривають ширші можливості, але за рахунок зростання складності. Подальший розвиток технологій гомоморфного шифрування має потенціал зробити їх більш ефективними, що дозволить інтегрувати їх у широке коло інформаційних систем, орієнтованих на захист конфіденційності даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. GENTRY C. Fully Homomorphic Encryption using Ideal Lattices [Електронний ресурс] / CRAIG GENTRY. – 2009. – Режим доступу до ресурсу: https://crypto.stanford.edu/craig/FHE.pdf.
2. Homomorphic Encryption Standardization [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://homomorphicencryption.org/.
3. RSA Cryptosystem Overview [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.tutorialspoint.com/rsa-algorithm.
4. PAILLIER P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes [Електронний ресурс] / PASCAL PAILLIER. – 1999. – Режим доступу до ресурсу: https://www.di.ens.fr/~mvaudenay/crypto/Paillier99.pdf.

Чернюк Олександр Костянтинович– студент групи КІТС-23М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: chernukalex2b@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Cherniuk Oleksandr – student of KITS-23M group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: chernukalex2b@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com