УДК 004.056.55

РОЗВИТОК ТА ЗАСТОСУВАННЯ ГОМОМОРФНИХ ШИФРІВ ДЛЯ БЕЗПЕЧНОГО ОБЧИСЛЕННЯ В ХМАРНИХ ТЕХНОЛОГІЯХ

Латанська Л.О., к.ф.-м.н., доцент[1]; Давидов Д.В.[2]
[1,2] Національний університет кораблебудування імені адмірала Макарова
[1,2] Миколаїв, Україна
[1]llatanskaya@gmail.com; [2]den0802200203@gmail.com

Анотація. *Проведено дослідження технологій гомоморфного шифрування в області обчислень в хмарних технологіях та здійснено порівняння гомоморфного шифрування з іншими методами безпечного обчислення.*
Ключові слова: *криптографія; шифрування; безпека; шифрування в хмарах; приватне обчислення; гомоморфні шифри; захист приватності; повністю гомоморфне шифрування.*

Вступна частина. У вік розвинутих інформаційних технологій, коли збереження та обробка великих обсягів даних стали ключовими аспектами сучасного суспільства, зростає важливість питань безпеки та конфіденційності. Особливо актуальними ці питання стають в контексті хмарних технологій, де десятки та сотні терабайтів даних зберігаються та обробляються на віддалених серверах із великою кількістю користувачів.

Захист даних та забезпечення конфіденційності стають критичними завданнями у такому середовищі, і одним із потужних інструментів для досягнення цих цілей є гомоморфні шифри. Гомоморфні шифри – це криптографічні технології, які дозволяють виконувати обчислення над зашифрованими даними без їх розшифрування.

Ця концепція стала пунктом перелому у безпеці даних та відкрила нові можливості для застосування хмарних обчислень у різних сферах, від медицини та фінансів до різних досліджень [1].

Метою роботи є дослідження розвитку та застосування гомоморфних шифрів для безпечного обчислення у хмарних технологіях.

Основна частина. Однією зі складностей концепції гомоморфного шифрування є коректне розуміння самого процесу проведення обчислень. Існують частково гомоморфні системи та повністю гомоморфні. У даній роботі будуть розглядатись повністю гомоморфні системи, які використовують повністю гомоморфне шифрування (Fully Homomorphic Encryption) [2].

Гомоморфне шифрування – форма шифрування, яка дозволяє виконувати певні математичні операції над зашифрованими даними та отримувати зашифрований результат, який відповідає результату операцій, виконаних над відкритими даними [3]. Інакше кажучи, у нас є задача – провести певні операції над нашими даними за допомогою хмарних сервісів. Ми не хочемо, щоб наші дані були відкриті та доступні, тому перед відправкою на хмару ми їх шифруємо. Далі йде відправка зашифрованих даних на сервер та їх обробка у зашифрованому вигляді. Після цього сервер повертає дані клієнту (нам) і тоді ми отримаємо результат необхідних нам операцій у зашифрованому вигляді, який зможемо розшифрувати, так як у нас є ключ. Як результат – ми задіяли хмарні технології для проведення обчислень над нашою інформацією без її публічного розкриття.

Історія гомоморфного шифрування починається з пропозиції такої ідеї у 1978 році винахідниками криптографічного алгоритму з відкритим ключем RSA Рональдом Рівестом

та Аді Шаміром разом з Майклом Дертузосом. Над даною концепцією працювали багато видатних криптографів, таких як Шафі Голдвассер, Сільвіо Мікаллі, Паскаль Пейє, проте усі дослідження стосувалися створення частково гомоморфної системи. Справжнім проривом у розвитку повністю гомоморфного шифрування стало запропоноване у 2009 році науковцем Крейгом Джентрі використання системи, яка основана на криптографії на решітках [3]. У наш час дані системи досягли великого рівня розвитку, багатьма компаніями створено бібліотеки для роботи з повністю гомоморфним шифруванням. Як приклад можна привести бібліотеку SEAL від Microsoft, HElib від IBM, OpenFHE та PALISADE від Intel, Samsung та MIT [4].

Коли дані передаються на хмару, зазвичай використовуються стандартні методи шифрування для захисту операцій і зберігання даних. Основна ідея полягала в тому, щоб зашифрувати дані перед надсиланням їх у хмару. Але провайдеру хмарного сервісу необхідно розшифровувати дані при кожній операції. Клієнт повинен буде надати приватний ключ до сервера для розшифровки даних перед виконанням необхідних обчислень, що може вплинути на конфіденційність і приватність даних, що зберігаються в хмарі. Натомість, системи гомоморфного шифрування використовуються для виконання операцій із зашифрованими даними без доступу до приватного ключа, єдиним власником якого є клієнт.

Шифрування є гомоморфним, якщо з Enc(a) та Enc(b) можна обчислити Enc(f(a, b)), де f може бути: +, ×, $\oplus$, без використання приватного ключа. Серед гомоморфного шифрування розрізняються системи в залежності від операцій, які дозволено виконувати над вихідними даними: криптосистеми Пейлера та Голдвассера-Мікаллі – адитивне гомоморфне шифрування (тільки додавання вихідних даних); системи RSA та Ель-Гамаля – мультиплікативне гомоморфне шифрування. Нижче подано дві властивості, від яких залежить ступінь гомоморфності системи [5]:

$$Dec\big(Enc(m_1) \otimes Enc(m_1)\big) = m_1 m_2,$$

$$Dec\big(Enc(m_1) \oplus Enc(m_2)\big) = m_1 + m_2,$$

де $\oplus$ та $\otimes$ – операції над зашифрованими даними, які відповідають операціям + та × над розшифрованими [6].

Перша властивість називається мультиплікативним гомоморфним шифруванням, а друга – адитивним. Алгоритм є повністю гомоморфним, якщо обидві властивості задовольняються одночасно. Достатність умови гомоморфізму за властивостями додавання та множення, випливає з того, що над бітами операції формується повний за Тюрінгом базис. Звідси слідує, що, якщо така криптосистема зможе надійно шифрувати два біта, то можливим стане і обчислення будь-якої булевої, а отже і будь-якої обчислювальної функції [6].

Проводячи аналіз існуючих популярних гомоморфних систем, які використовуються в хмарних обчисленнях, можна помітити притаманні усім наступні характеристики:

- забезпечення приватності даних на етапах з’єднання та в процесі зберігання даних;
- забезпечення безпеки провайдером хмарного сервісу;
- використання ключів шифрування тільки клієнтом.

Відмінність простежується у типах шифрування, що використовують криптосистеми. У таблиці 1 наведено порівняння систем за типом шифрування.

Таблиця 1

Порівняння гомоморфних криптографічних систем за типом шифрування [5]

	Криптографічна система				
	RSA	Пейлера	Ель-Гамаля	Голдвассера-Мікаллі	Джентрі
Тип гомоморфного шифрування	Мультиплікативне	Адитивне	Мультиплікативне	Адитивне, але може зашифрувати тільки 1 біт	Повністю гомоморфне

У контексті інших шифрувальних методів, повністю гомоморфний має як свої переваги так і недоліки. Кажучи про повністю гомоморфні алгоритми, можна звернути увагу на їх високий рівень захищеності даних та конфіденційності інформації. З іншої сторони, слід зазначити й велику кількість часу та ресурсу сервера, які необхідні на виконання операцій над даними клієнта. На цьому етапі постає питання оптимізації алгоритмів. Збільшити продуктивність, забезпечити конфіденційність інформації та стійкість алгоритму можливо, якщо задіяти такі способи, як:

- використання оптимальної схеми шифрування залежно від задачі;
- виконання пакетних обчислення, замість виконання обчислень над кожним бітом;
- використання апаратних акселераторів;
- використання оптимізованих бібліотек та платформ, створених для гомоморфного шифрування.

Висновки. Безпека хмарних обчислень на основі повного гомоморфного шифрування є новою концепцією безпеки, важливим напрямком для вдосконалення та винаходу нових криптографічних алгоритмів. Ця галузь викликає великий інтерес серед дослідників. Великі компанії, які забезпечують хмарні сервіси, активно розвивають напрямок гомоморфного шифрування, тим самим роблячи внесок у зростання безпеки та забезпечення якомога більшої довіри серед клієнтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Sellers, A. (2021, April 14). *Everything you wanted to know about homomorphic encryption (but we are afraid to ask)*. https://www.forbes.com/sites/forbestechcouncil/2021/04/14/everything-you-wanted-to-know-about-homomorphic-encryption-but-were-afraid-to-ask/?sh=2761b2501407

[2] Gentry, C. (2009). *A fully homomorphic encryption scheme*. A dissertation for the degree of doctor of philosophy. Stanford university.

[3] Wikipedia. (n.d.). *Homomorphic encryption*. Retrieved October 22, 2023, from https://en.wikipedia.org/wiki/Homomorphic_encryption

[4] Quah, I. (2022, July 7). *How to choose a homomiorphic encryption library*. https://dualitytech.com/blog/how-to-choose-a-homomorphic-encryption-library/

[5] Maha, TEBAA., & Said, EL HAJII. (2014). *Secure Cloud Computing through Homomorphic Encryption.* Mohammed V University.

[6] Аракелов, Г.Г. (2019). Вопросы применения прикладной гомоморфной криптографии. *Вопросы кибербезопасности, 5 (33)*, 70-74.

Latanska L.O., Davydov D.V.

Development and application of homomorphic ciphers for secure computing in cloud technologies

Abstract. *A study of homomorphic encryption technologies in the field of computing in cloud technologies was carried out and a comparison of homomorphic encryption with other methods of secure computing was carried out.*

Keywords: *cryptography; encryption; security; cloud encryption; private computing; homomorphic ciphers; privacy protection; fully homomorphic encryption.*