УДК 004.056.55

М. Т. Мовчанюк[1]
О. В. Салієва[2]

АНАЛІЗ СУЧАСНИХ ГОМОМОРФНИХ СИСТЕМ ШИФРУВАННЯ

Вінницький національний технічний університет;

Анотація

У доповіді здійснюється аналіз сучасних систем гомоморфного шифрування. Досліджено питання використання повністю гомоморфних та частково гомоморфних систем. Розглянуто їх основні відмінності, обмеження та переваги.

Ключові слова: система шифрування, гомоморфне шифрування, типи гомоморфного шифрування, обмеження, параметр безпеки, конфіденційність.

Abstract

The report analyzes modern homomorphic encryption systems. The issue of using completely homomorphic and partially homomorphic systems has been studied. Their main differences, limitations and advantages are considered.

Keywords: encryption system, homomorphic encryption, types of homomorphic encryption, restrictions, security parameter, confidentiality.

Вступ

У сучасному інформаційному суспільстві теми безпеки та захисту даних стали майже нероздільними. З метою забезпечення надійного захисту інформації компанії намагаються здійснювати конфіденційні обчислення, які дозволяють даним залишатися зашифрованими під час їх обробки.

Розробники все частіше звертаються до гомоморфного шифрування, оскільки воно забезпечує достатньо високий рівень безпеки. Гомоморфне шифрування – це доволі нова технологія, яка може допомогти компаніям забезпечити конфіденційність своїх клієнтів в роботі із зашифрованою інформацією.

Результати дослідження

Гомоморфне шифрування – це тип методу шифрування, який дозволяє виконувати обчислення для зашифрованих даних без попереднього їх розшифрування за допомогою секретного ключа. Результати обчислень також залишаються зашифрованими і можуть бути розшифровані лише власником приватного ключа.

Існує три основних типи гомоморфного шифрування [1]:

– частково гомоморфне шифрування (PHE): дозволяє виконувати лише вибрані математичні функції над зашифрованими даними;

– дещо гомоморфне шифрування (SHE): надає можливість виконувати обмежену кількість математичних операцій певної складності протягом обмеженої кількості разів;

– повне гомоморфне шифрування (FHE): дозволяє виконувати будь-які математичні операції необмежену кількість разів.

Обмін приватними даними з третіми сторонами, такими як хмарні сервіси або інші компанії, є проблемою через правила конфіденційності даних, такі як GDPR і CCPA. Недотримання цих правил може призвести до серйозних штрафів і заподіяти шкоду діловій репутації [2].

Традиційні методи шифрування забезпечують ефективний і безпечний спосіб зберігання приватних даних у хмарі в зашифрованому вигляді. Однак для виконання обчислень з даними, зашифрованими за допомогою цих методів, підприємствам потрібно або розшифрувати дані в хмарі, що може призвести до проблем із безпекою, або завантажити дані, розшифрувати їх і виконати обчислення, які можуть бути дорогими та тривалими.

Гомоморфне шифрування може дозволити компаніям безпечно використовувати хмарні обчислення та послуги зберігання даних. Це усуває компроміс між безпекою даних і зручністю використання. Під-

приємствам не потрібно покладатися на хмарні послуги щодо безпеки своїх особистих даних, зберігаючи при цьому можливість виконувати на них обчислення.

Гомоморфне шифрування дозволяє організаціям ділитися конфіденційними бізнес-даними з третіми сторонами, не розкриваючи їм дані чи результати обчислень. Це може прискорити співпрацю та інновації без ризику порушити безпеку конфіденційної інформації. Ці служби потім повертають зашифрований результат власнику, який може розшифрувати його за допомогою приватного ключа [3].

Використання системи гомоморфного шифрування забезпечує відповідність нормативним вимогам.

Гомоморфне шифрування усуває компроміс між зручністю використання даних та їх конфіденційністю: немає потреби маскувати або відкидати будь-які функції, щоб зберегти конфіденційність даних. Усі функції можна використовувати в аналізі без шкоди для конфіденційності.

Сучасні системи гомоморфного шифрування є квантово безпечні: повністю гомоморфні схеми шифрування стійкі до квантових атак.

Часткові та дещо гомоморфні системи шифрування існували з кінця 70-х років, але повністю гомоморфна система, яка дозволяє виконувати всі математичні операції над зашифрованими даними, була вперше створена в 2009 році. У своїй нинішній формі повністю гомоморфне шифрування є все ще є новою розробкою для забезпечення безпеки даних [4].

До недоліків повністю гомоморфного шифрування можна віднести низьку продуктивність: між повільною швидкістю обчислень або проблемами точності, повністю гомоморфне шифрування залишається комерційно неможливим для додатків із складними обчисленнями. Загальний консенсус у науковій спільноті полягає в тому, що дослідження та розробка алгоритмів повністю гомоморфного шифрування активно проводиться на даному етапі, тому сьогодні воно корисне в поєднанні з іншими технологіями, що підвищують конфіденційність, такими як безпечні багатосторонні обчислення.

Висновки

Оскільки більшість крадіжок даних відбувається під час їхнього тимчасового розшифрування або ж використання в незахищеному вигляді, то гомоморфне шифрування дозволяє будь-кому виконувати операції з даними без необхідності їх попереднього розшифрування, що робить всю систему захищеною від порушення конфіденційності.

Ризик витоку конфіденційної інформації в складних ІТ-системах не можна ігнорувати, і тому зростає інтерес до застосування гомоморфної технології для забезпечення конфіденційності даних і децентралізованого доступу до організаційних даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке гомоморфне шифрування? [Електронний ресурс] // Keyfactor. – 2021. – Режим доступу до ресурсу: https://www.keyfactor.com/blog/what-is-homomorphic-encryption/.

2. Ділмегані Д. Що таке гомоморфне шифрування? Переваги та проблеми [Електронний ресурс] / Д. Ділмегані. – 2021. – Режим доступу до ресурсу: https://research.Що таке гомоморфне шифрування? Переваги та проблеми.com/homomorphic-encryption/.

3. Ефективне повністю гомоморфне шифрування від (стандартного) LWE [Електронний ресурс] // Cryptology ePrint. – 2011. – Режим доступу до ресурсу: http://eprint.iacr.org/2011/344.

4. Кастро Л. Чи потребує повністю гомоморфне шифрування прискорення обчислень? [Електронний ресурс] / Л. Кастро, Р. Агравал, А. Джоші // Корнельський університет. – 2021. – Режим доступу до ресурсу: https://arxiv.org/abs/2112.06396.

Мовчанюк Мар'яна Тимофіївна – студентка групи КІТС-18б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: aelil.mary@gmail.com

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

***Movchanyuk Mariana T.* –** department of Management and Information Security, Vinnitsa National Technical University, Vinnytsia**, e-mail:** aelil.mary@gmail.com

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