ГОМОМОРФНЕ ШИФРУВАННЯ В ХМАРНИХ ОБЧИСЛЕННЯХ

Азаренко А.П., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Хмарні обчислення стали невід'ємною складовою сучасного світу і дозволяють користувачам зберігати та обробляти великі обсяги даних без необхідності у власних комп'ютерах [1]. **Метою доповіді** є дослідження можливостей використання гомоморфних методів шифрування з метою покращення надійності захисту конфіденційних даних у хмарному середовищі, а саме: аналіз існуючих алгоритмів повністю гомоморфного шифрування; визначення поняття криптостійкості, коректності та компактності для гомоморфних систем; оцінка криптостійкості повних гомоморфних систем; визначення перспектив використання гомоморфного шифрування в хмарних обчисленнях.

Гомоморфне шифрування є методом шифрування даних, який дозволяє проводити операції з зашифрованими даними не розшифровуючи їх. Це дозволяє зберігати конфіденційні дані в безпеці, навіть коли вони перебувають в публічному хмарному середовищі [2]. В доповіді наведені результати дослідження різних методів гомоморфного шифрування, таких як повне гомоморфне шифрування та часткове гомоморфне шифрування, результати порівняльного аналізу ефективності застосування цих методів в хмарних обчисленнях.

Повні гомоморфні системи в хмарних обчисленнях повинні забезпечувати високий рівень криптографічної стійкості за допомогою криптографічних методів та протоколів, які забезпечують захист від різних видів атак, таких як: атаки типу залежність від контексту, атаки на основі розкриття ключів, атаки на основі перехоплення інформації та інших. Гомоморфне шифрування має кілька переваг для хмарних обчислень, зокрема, збереження конфіденційності, зменшення ризику витоку даних, менша потреба в пропускній здатності та забезпечення безпеки даних [3]. Попри потенційні переваги, гомоморфне шифрування все ще є відносно новою технологією і має обмеження. Також воно може бути повільним і вимогливим до ресурсів, що може бути проблемою обробки великих обсягів даних.

Список літератури

1. Carlin, S., Curran, K. Cloud Computing Security. International Journal of Ambient Computing and Intelligence. 2011. Vol. 3, No. 1. P. 14-19. DOI: https://doi.org/10.4018/jaci.2011010102.

2. Gentry C. A fully homomorphic encryption scheme. Ph.D. Thesis. 2009. 199 p.

3. Lauter, K., Naehrig, M., Vaikuntanathan, V. Can Homomorphic Encryption be Practical? CCSW'11, Chicago, USA. 2011. P. 113-124. Available at: https://eprint.iacr.org/2011/405.pdf (accessed 23.03.2023).