ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ ГОМОМОРФНОГО ШИФРУВАННЯ

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

Гомоморфне шифрування (Homomorphic Encryption, HE) - технологія, що дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування [1-3]. Застосування гомоморфного шифрування відкриває великі можливості для обробки зашифрованих даних без їх розшифрування в багатьох сферах, де критично важливо зберігати конфіденційність інформації.. Однак, попри потенціал, існує низка проблемних питань, які стримують широке впровадження цієї технології в практичні системи безпеки та обробки даних.

Метою доповіді є аналіз проблемних питань при практичному застосуванні гомоморфного шифрування.

В роботі розглянуті ключові сучасні сфери застосування HE [1-3].

1. Хмарні обчислення (Cloud Computing), обробка зашифрованих даних на стороні постачальника хмарних послуг без розкриття вмісту.

2. В медицині та біоінформатиці захищене зберігання та аналіз медичних записів пацієнтів, генетичної інформації (DHK). Використання HE у дослідженнях із багатьма організаціями без обміну розшифрованими даними.

3. В фінансових сервісах конфіденційна аналітика для банків, страхових компаній, бірж. Обчислення кредитного рейтингу, оцінка ризиків без доступу до відкритих даних клієнта.

4. Електронне голосування (E-voting). Забезпечення анонімності та перевірності результатів голосування, так як дані не розкриваються, але можуть бути агреговані без розшифрування.

5. В Інтернеті речей (IoT) для обробки конфіденційних даних, зібраних з розумних пристроїв, безпосередньо на сервері або у хмарі. Використання в промисловому IoT (IIoT), медичних пристроях, Smart City.

6. Захист персональних даних у Big Data, аналітика зашифрованих великих масивів даних з соціальних мереж, телекомів, сервісів для обчислення трендів, поведінкових моделей, не розкриваючи особистості.

7. Машинне навчання над зашифрованими даними (Privacy-Preserving ML). Навчання або інференс моделей на даних, які ніколи не розшифровуються. Використання в конфіденційній медичній діагностиці, рекомендаційних системах, фінансах. Працює разом з Federated Learning, Secure Multi-Party Computation (SMPC).

8. В юридичних сервісах та державному управлінні для безпечної взаємодії між державними структурами при обробці реєстрів, митних даних, податкових баз, де важлива повна конфіденційність.

9. В системах кібербезпеки та цифрової ідентичності. Застосовується в антифрод-системах, аналізі поведінки користувачів без втрати їхньої конфіденційності. Підтримка Zero Knowledge Proofs та протоколів автентифікації.

В процесі проведеного аналізу виявлені проблемні питання, які стримують широке впровадження гомоморфного шифрування в практичні системи безпеки та обробки даних.

1. Обчислювальна складність та продуктивність. Базові арифметичні операції (додавання, множення) в HE можуть займати в сотні або тисячі разів більше часу, ніж у звичайних обчисленнях, тому гомоморфне шифрування є надзвичайно ресурсомістким.

2. Розмір зашифрованих даних в HE системах мають величезний розмір. Це створює проблему при збереженні, передаванні та обробці таких даних, особливо в хмарних середовищах та IoT-системах.

3. Обмежена функціональність у деяких реалізаціях. Частково гомоморфне шифрування (PHE) підтримує лише одну операцію (додавання або множення), складно реалізувати умовні оператори (if/else), порівняння або логічні операції, діє обмеження на глибину обчислень (multiplicative depth) у схемах FHE.

4. Інтеграція з існуючими системами. Потрібна адаптація програмного забезпечення, баз даних, аналітичних інструментів до роботи з HE.

5. Складність реалізації. Розробка систем із підтримкою HE вимагає висококваліфікованих спеціалістів. Висока вірогідність помилок внаслідок складної математичної бази (решітки, модулярна арифметика, шумові моделі).

6. Відсутність єдиного загальноприйнятого стандарту HE. Утруднене сумісне використання різних криптобібліотек (SEAL, HElib, TenSEAL). Складнощі з юридичними аспектами, якщо система повинна відповідати, наприклад, GDPR.

7. Обмежена підтримка в апаратному забезпеченні. Переважна більшість CPU/GPU не оптимізована для обчислень у HE. Високопродуктивні реалізації можливі лише з використанням спеціалізованого апаратного прискорення (FPGA, ASIC), що ще не є масовим.

8. Проблеми масштабування. Обробка великих обсягів зашифрованих даних вимагає величезних обчислювальних ресурсів, унеможливлюючи застосування в реальному часі для Big Data, IoT, Smart Grid.

10. Обмежене практичне використання. Реальних продуктів із повною підтримкою HE одиниці: proof-of-concept, обмежені демонстраційні системи.

Таким чином гомоморфне шифрування – це потужний інструмент для захисту конфіденційності, але висока обчислювальна складність, великі розміри даних, складність реалізації та відсутність стандартів гальмують широке впровадження цієї технології.

Список літератури

1. Halevi, S., & Shoup, V. (A Full Introduction to Homomorphic Encryption). 2013. IBM Research. 92 ps.

2. Yi, X., Paulet, R., Bertino, E., Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption (pp. 27-46). Springer International Publishing

3. Coron, J.-S., Naccache, D., & Tibouchi, M. (Homomorphic Encryption). 2011. Springer. 142 p.