УДК 004.056.5

Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ

Владислав Владиславович ГУДІЛІН,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

ГОМОМОРФНЕ ШИФРУВАННЯ ЯК ЗАСІБ УБЕЗПЕЧЕННЯ БАЗ ДАНИХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ НА ХМАРНИХ ПЛАТФОРМАХ

Одним із стратегічних напрямків подальшого розвитку інформаційного забезпечення Національної поліції України є створення центрів обробки даних – ЦОД на основі хмарних технологій. Використання зовнішніх хмарних платформ дозволить суттєво підвищити в техніко-економічному плані ефективність функціонування в цілому системи інформаційного забезпечення Національної поліції України. Але зберігання і обробка конфіденційних даних на носіях зовнішніх структур містить небезпеку з огляду на можливості неконтрольованого доступу до цих даних з боку провайдера хмарної інфраструктури, а також ризику несанкціонованих вторгнень в хмару. Звичайно, для захисту інформації провайдери надають певні криптографічні механізми. Однак майже відразу виявляється один недолік таких систем. Для модифікації віддалених даних необхідна передача по мережі приватного ключа, що ставить під загрозу збереження конфіденційності інформації через можливість прослуховування незахищеного каналу зв'язку.

Збереження конфіденційності інформації можна досягнути, якщо обробка даних буде здійснюватись на віддалених серверах у зашифрованому вигляді без можливості їх розшифрування на стороні серверів хмарного середовища. Тобто, при передачі інформації в хмару вона повинна бути зашифрована на стороні клієнта, оброблена в зашиф-

рованому вигляді на сервері, і розшифрована на стороні клієнта. Цю модель покликано реалізувати гомоморфне шифрування.

Поняття гомоморфності шифрування вперше сформовано в 1978 році Рівестом, Адлеманом і Дертузосом, але автори алгоритму RSA не змогли обґрунтувати необхідність та можливість застосування гомоморфного шифрування. Вони тільки припустили можливість виконання довільних операцій над зашифрованими даними без їх розшифрування [1]. Розроблені в наступні роки криптосистеми Ель-Гамаля, Гольдвассер-Мікалі, Пайє та Бенало були лише частково гомоморфні. У 2009 році аспірант Стенфордського університету і спеціаліст фірми «IBM» Крейг Джентрі теоретично обґрунтував принципову можливість створення повністю гомоморфної криптосистеми шифрування і запропонував одну таку систему. Запропонована система може використовуватися для забезпечення конфіденційності даних при будь-яких видах їх обробки в недовірених середовищах, наприклад, при хмарних або розподілених обчисленнях.

Математично поняття гомоморфності виражається наступним чином. Нехай K та L – це алгебраїчні кільця, множина, в якій визначені операції додавання та множення, подібні до додавання і множення цілих чисел. Відображення $f : K \to L$ називається гомоморфізмом цих множин, що задовільняє такі властивості:

$$f(h1 + h2) = f(h1) + f(h2)$$

$$f(h1 * h2) = f(h1) * f(h2)$$

де $h1, h2 \in K$.

Функцію f розглядаючи гомоморфність в аспекті шифрування, можна представити як функцію шифрування вихідних числових значень h1 та h2. Якщо алгоритм щифрування зодовільняє обидві властивості, він вважається повністю гомоморфним, якщо лише одну – частково гомоморфним алгоритмом шифрування, тобто гомоморфним лише для одної арифметичної операції: або операції додавання, або ж операції множення.

Алгоритм асиметричного шифрування RSA, один з найбільш відомих та ефективних алгоритмів шифрування даних, є частково гомоморфним, бо володіє властивістю гомоморфності відносно операції множення. Асиметричний алгоритми шифрування Ель-Гамаля, заснований на складності обчислення дискретних логарифмів в кінцевому полі, є також частково гомоморфним для операції множення. Схема шифрування Пайє дозволяє отримати суму двох незашифрованих чисел, перемноживши їх шифротексти, тобто є частково гомоморфною відносно операції додавання.

Розглянемо схему повністю гомоморфного шифрування Джентрі:

1. Генерація ключів. Обирається довільне непарне число $p = 2k + 1$. Дане число p слугує секретним ключем.

2. Шифрування. Нехай треба зашифрувати біт $m \in (0,1)$. Для цього генерується число $z = 2r + m$, де r – довільне ціле число. Це означає, що

$$z = m(\text{mod } 2).$$

Шифрування полягає в тому, що всякому числу m ставиться у відповідність число $c = pq + z$, де q – довільне ціле число. Отже,

$$E(m) = c = 2r + m + (2k + 1)q = 2(r + kq) + m + q.$$

4. Розшифрування. Для розшифрування достатньо чисел p та q. Тоді розшифрування за допомогою секретного ключа p:

$$c(\text{mod } p) = (z + pq)(\text{mod } p) = z(\text{mod } p) + pq(\text{mod } p) = z(\text{mod } p) =$$
$$= (2r + m)(\text{mod } p) = 2(r(\text{mod } p)) + m(\text{mod } p)$$
$$(c(\text{mod } p))(\text{mod } 2) = (2(r(\text{mod } p))(\text{mod } 2) = m(\text{mod } 2) = m.$$

Підтвердження повної гомоморфності схеми Джентрі:

Розглянемо два біти $m_1, m_2 \in (0,1)$.

Зіставимо їм $z_1 = 2r_1 + m_1$, $z_2 = 2r_2 + m_2$.

Вибір приватного ключа: $p = 2k + 1$.

Тоді шифротексти для m_1 та m_2:

$$E(m_1) = c_1 = z_1 + pq_1, E(m_2) = c_2 = z_2 + pq_2.$$

Тоді операція додавання над зашифрованими даними буде мати вигляд:

$$E(m_1) + E(m_2) = c_1 + c_2 + z_1 + z_2 + p(q_1 + q_2) =$$
$$= 2(r_1 + r_2) + m_1 + m_2 + p(q_1 + q_2).$$

Операція множення над зашифрованими даними:

$$E(m_1)E(m_2) = c_1c_2 = z_1 z_2 + p(z_1 q_2 + z_2 q_1) = p^2q_1q_2 =$$
$$= (2r_1 + m_1)(2r_2 + m_2) + p(z_1 q_2 + z_2 q_1) + p^2 q_1 q_2 =$$
$$= 4r_1 r_2 + 2(r_1 m_2 + r_2 m_1) + m_1 m_2 + p(z_1q_2 + z_2 q_1) + p^2q_1q_2.$$

При розшифровці даних відповідних операцій отримуємо:

$$D(E(m_1) + E(m_2)) = ((c_1 + c_2)(\text{mod } p))(\text{mod } 2) = m_1 + m_2;$$
$$D(E(m_1)E(m_2)) = ((c_1c_2)(\text{mod } p))(\text{mod } 2) = m_1m_2.$$

Істотним недоліком даної схеми є те, що виконання обчислень призводить до накопичення помилки, і після того як вона перевищує приватний

ключ, розшифрувати повідомлення становиться неможливим. Одним з варіантів вирішення даної проблеми є перешифрування даних після деякої кількості операцій, однак такий варіант знижує продуктивність обчислень і вимагає постійного доступу до секретного ключа. Інший недолік схеми Джентрі пов'язаний із зростанням розміру шифротексту [2]. З'явилося чимало робіт, спрямованих на розвиток запропонованої схеми Джентрі і усунення недоліків. Зокрема, була запропонована схема BGV (абревіатура від прізвищ творців – Brakerski, Gentry, Vaikuntanathan), а також шифрування на підставі LWE (Learning With Errors), яке дозволило зменшити складність побудови криптосистеми [3].

Повністю гомоморфне шифрування вже використовується для зберігання даних у базі даних «DynamoDB», публічної хмари американської компанії Amazon Web Service.

Таким чином, для подолання потреби в новітньому технічному та програмному забезпеченні органам внутрішніх справ слід експортувати свої бази даних в хмарне середовище, для захисту цілісності і конфіденційності, яких будуть застосовуватись алгоритми шифрування даних з гомоморфними властивостями.

Список бібліографічних посилань

1. Rivest R. L., Adleman L., Dertouzos M. L. Data clustering. Algorithms and Applications. Cham: Springer Ltd. Publ., Switzerland, 2015. 734 p.
2. Gentry C. A Fully homomorphic encryption using ideal lattices: The 41st Symposium on the Theory of Computing (STOC), Bethesda, USA, 2009. Pp. 169–178.
3. Gentry C. Homomorphic Encryption from Learning With Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based: 33rd Annual Cryptology Conf., Santa Barbara, USA, 2013. Pp. 73–93.

Одержано 02.04.2020