УДК [512.541.5:004.056.55]+512.624.95]:004.738.5

Т.Г. Білова

Харківська державна академія культури, Харків

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕТОДІВ ГОМОМОРФНОГО ШИФРУВАННЯ В ХМАРНИХ ОБЧИСЛЕННЯХ

Розглянуто основні поняття гомоморфного шифрування. Проаналізовано існуючи алгоритми побудови повністю гомоморфних систем. Визначено підходи до оцінки криптостійкості гомоморфного шифрування. Сформульовані проблеми та перспективи використання гомоморфного шифрування для організації безпеки даних в хмарних обчисленнях.

Ключові слова: *хмарні технології, безпека даних, криптографічні системи, гомоморфне шифрування, криптостійкість, матричний поліном.*

Вступ

Постановка задачі та аналіз досліджень. Хмарні технології – це зручне середовище для зберігання і обробки інформації, яке об'єднує в собі апаратні засоби, ліцензійне програмне забезпечення, канали зв'язку, а також технічну підтримку користувачів. Використання «хмар» дозволяє значно знизити витрати на інфраструктуру та підвищити ефективність роботи підприємств.

До безумовних переваг хмарних технологій відносять незалежність від апаратної платформи і географічної території, масштабованість, еластичність, мобільність, необмежений обсяг даних, що обробляються, та можливість нарощувати ресурси [1; 2]. Але невирішеним залишається питання збереження контролю над конфіденційною інформацією, що зберігається в «хмарі», і це значно обмежує використання цієї технології для побудови інформаційних систем, особливо потребуючих високого рівню захисту даних, що обробляються.

Усі поширені в даний час криптографічні алгоритми не дозволяють виробляти довільні обчислення над зашифрованими даними, істотно обмежуючи можливості використання хмарних ресурсів. Перспективним напрямком підвищення безпеки хмарних обчислень може стати створення ефективних алгоритмів повністю гомоморфного шифрування, які дозволять виробляти довільні обчислення без попередньої розшифровки даних.

Тому актуальним є аналіз існуючих підходів до побудови систем гомоморфного шифрування та визначення перспектив їх використання для підвищення інформаційної безпеки хмарних обчислень.

Мета та завдання дослідження. Метою даного дослідження є оцінка можливостей використання гомоморфних методів шифрування для підвищення надійності захисту конфіденційних даних в хмарі.

У відповідності з поставленою метою слід вирішити наступні завдання: визначити основні поняття гомоморфного шифрування; проаналізувати існуючи алгоритми повністю гомоморфного шифрування; визначити поняття криптостійкості, коректності та компактності для гомоморфних систем; оцінити криптостійкість повних гомоморфних систем; визначити перспективи використання гомоморфного шифрування в хмарних обчисленнях.

Основна частина

Поняття гомоморфного шифрування. Під гомоморфним шифруванням розуміється криптографічний примітив, що представляє собою функцію шифрування, яка задовольняє додатковій вимозі гомоморфності щодо будь-яких алгебраїчних операцій над відкритим текстом.

Реалізація повністю гомоморфного шифрування має задовольняти наступним вимогам [3]:

1. Спектр підтримуваних математичних функцій покриває повсякденні потреби програмістів.

2. Діапазони значень чисел покривають принаймні стандартні типи даних, а обчислення, вироблені над зашифрованими даними, мають прийнятну продуктивність.

3. Точність і швидкість зберігаються протягом усіх обчислень.

4. Складність обчислення примітивних операцій над зашифрованими даними – O(n log(n)) або O(n) від потужності допустимого діапазону значень.

5. Криптостійкість повинна бути досить велика, щоб виключити атаку повним перебором.

Гомоморфне шифрування довгий час було лише теоретичним напрямком досліджень, і лише в 2009 році в роботі Крейга Джентрі [4] була розглянута можливість практичного застосування таких методів.

Запропонована Джентрі схема є алгоритмом повністю гомоморфного шифрування [5]. Нехай p – секретний параметр, будь-яке непарне число. Тоді його можна представити у вигляді $p=2k+1$. Якщо $m\in\{0,1\}$, то число $z\in Z$ можна побудувати за правилом $z=2r+m$, де r – будь-яке ціле, тобто $z= m \bmod 2$. Алгоритм шифрування полягає у тому, щоб будь-

якому m ставиться у відповідність c=z+pq, де q – будь-яке ціле. Тобто c=2r+m+(2k+1)·q.

С отриманим таким чином числом c відбуваються обчислення. Причому (c mod 2)=(m+q) mod 2, тобто на цьому етапі можна визначити лише парність виходу з шифрування.

Сам процес шифрування складається з наступних кроків. Якщо c – число, що зашифроване, а p – таємний ключ, то за допомогою p проводиться дешифрування:

$$r=c \bmod p=(z+pq) \bmod p=z \bmod p+(pq) \bmod p.$$

Число r=c mod p є шумом, його можливі значення належать інтервалу (-p/2, p/2). Далі отримується початковий зашифрований біт m=r mod 2.

Для перевірки, чи є таке шифрування гомоморфним, співставимо $m_1, m_2 \in Z_2$ пару чисел

$$z_1=2r+m_1,\ z_2=2r+m_2.$$

Якщо взяти зашифроване число рівним p=2k+1, то зашифровані за допомогою нього значення будуть дорівнювати

$$c_1=z_1+p\cdot q_1,\ c_2=z_2+p\cdot q_2.$$

Додаток та добуток чисел c_1 та c_2 дорівнюють відповідно

$$c_1+c_2=z_1+z_2+ p(q_1+q_2)= 2r_1+m_1+2r_1+m_2+p(q_1+q_2)= =2(r_1+r_2)+m_1+m_2+(2k+1)\cdot(q_1+q_2); \quad (1)$$

$$c_1c_2=z_1z_2+ p(z_1q_2+ z_2q_1)+p^2 q_1q_2= =(2r_1+m_1)(2r_2+m_2)+2k(z_1q_2+ z_2q_1)+z_1q_1+ z_2q_2= =4r_1r_2+2(r_1m_2+ r_2m_1)+m_1m_2 +2k(z_1q_2+z_2q_1)+ +2r_1q_2+2r_2q_1+m_1q_1+m_2q_2. \quad (2)$$

При дешифруванні результату рівняння (1) виходить сума похідних біт m_1 та m_2:

$$[(c_1+c_2) \bmod p] \bmod 2=[2(r_1+r_2)+ m_1+ m_2] \bmod 2= =m_1+ m_2.$$

Якщо число p невідомо, дешифрувати результат неможливо:

$$(c_1+c_2) \bmod 2= m_1+ m_2+ q_1+ q_2.$$

Для операції добутку на основі рівняння (2) доказ є аналогічним.

Таким чином, запропонована Джентрі схема теоретично є повністю гоморфною. Але на практиці виконання обчислень призводить до накоплення похибки r, і коли вона перевищить p, дешифрування стане неможливим. Для запобігання накопичування похибки Джентрі запропонував технологію bootstrapping, але її використання при вирішенні прикладних задач призводить до значного зростання розмирів шифротексту.

З моменту опублікування роботи Джефрі основна задача вдосконалення алгоритмів гомоморфного шифрування – подолання росту ступеню поліномів та збільшення продуктивності алгоритмів у цілому. Наприклад, в [5] запропоновано кілька модифікацій повністю гомоморфного шифрування:

1. Алгоритм, заснований на поліномах від однієї змінної з коефіцієнтами з R. Використання в якості коефіцієнтів дійсних чисел дозволяє обчислювати практично довільні функції від дійсних аргументів (квадратний корінь, ступінь та ін.) Алгоритм також дає можливість порівнювати числа без розкриття їх точного значення, але швидке зростання ступенів поліномів при добутку та ріст коефіцієнтів при додаванні значно знижує точність та швидкість проведення обчислень.

2. Алгоритм гомоморфізмів кілець поліномів від однієї змінної над Z_n. На першому етапі поліном зіставляється похідному числу, на другому – безпосередньо шифрування. При дешифруванні використовується схема Горнера, результатом обчислень є молодший член поліному, що був отриманий. Недоліком схеми також є зростання ступеню поліномів при добутку, але його можна частково усунути використанням фактор-кілець поліномів.

3. Алгоритм гомоморфізмів кілець поліномів від багатьох змінних над Z_2. Виконує шифрування на рівні окремих бітів, для побудови «шифруючого» гомоморфізму використовується взаємно однозначна заміна змінних, що забезпечує побудову зворотної заміни та розшифрування даних. Перевага алгоритму – відсутність зростання ступеню поліномів за рахунок використання інтерполяційних поліномів Лангранжа або перетворення Кремони.

Властивості гомоморфних алгоритмів. В загальному випадку, гомоморфна система $\varepsilon=\left(\mathrm{KeyGen}_\varepsilon, \mathrm{Enc}_\varepsilon, \mathrm{Dec}_\varepsilon, \mathrm{Eval}_\varepsilon\right)$ – це четвірка ймовірнісних, поліноміальних по кількості кроків алгоритмів, що може бути сформульована наступним чином [6; 7]:

1. Генерація ключа. На цьому етапі алгоритм $(\mathrm{evk}, \mathrm{sk}) \leftarrow \mathrm{KeyGen}_\varepsilon(1^\lambda)$ приймає на вхід параметр криптостійкості λ та генерує відкритий ключ для обчислення evk та таємний ключ sk для шифрування та дешифрування.

2. Шифрування інформації на основі таємного ключа. Алгоритм $c \leftarrow \mathrm{Enc}_\varepsilon(\mathrm{sk}, m)$ приймає на вході таємний ключ sk та однобітове повідомлення відкритого тексту $m \in \{0,1\}$ та на їх основі генерує шифротекст c.

3. Дешифрування шифротексту. Алгоритм $m^* \leftarrow \mathrm{Dec}_\varepsilon(\mathrm{sk}, c)$ приймає на вхід таємний ключ sk і шифротекст c та генерує повідомлення відкритого текста $m^* \in \{0,1\}$.

4. Безпосередньо гомоморфне обчислення. Алгоритм $c_f \leftarrow \mathrm{Eval}_\varepsilon(f, c_1, ..., c_l)$ отримує на вході ключ для обчислення evk, функцію перетворення $f: \{0,1\}^l \rightarrow \{0,1\}$ та набір з l шифротекстів $c_1, \ldots, c_l$. На виході – підсумковий шифротекст c_f.

Функцію перетворення f можна представляти

за допомогою арифметичної схеми з функціональних елементів, еквівалентної булевій з елементів AND та XOR [6]. Ця функція може розглядатися як окремий об'єкт криптографічної системи, який відрізняється від відкритого ключа шифрування.

Семантичну кристостійкість такої системи (тобто криптостійкість у відношенні пасивних порушників) визначають наступним чином: ймовірність того, що алгоритм криптоаналітика вірно відлічить шифротекст нулю від шифротексту одиниці – функція, нескінченно мала від λ.

Коректність розшифрування після гомоморфного обчислення криптосхеми ε для булевої схеми з функціональних елементів F, що має t входів – якщо для будь-якої пари ключів (sk,evk), що були видані алгоритмом KeyGen(λ), та будь-яких t відкритих текстів m_i та відповідних їм шифротекстів $c_i \leftarrow \mathrm{Enc}(sk, m_i)$ виконується:

$$\mathrm{Dec}(sk, \mathrm{Eval}(rk, F, c)) = F(m_1, ..., m_t).$$

Компактність гомоморфної криптосистеми визначається наступним чином: система ε компактна, якщо існує поліном s=s(λ) такий, що довжина результату $\mathrm{Eval}_\varepsilon(f, c_1, ..., c_1)$ не перевищує s битів незалежно від f або числа входів. Тобто компактність розмірів шифротексту після гомоморфного обчислення повинна бути незалежна ні від числа входів t, ні від складності функції f, а тільки від розміру виходу f.

Ще однією важливою характеристикою гомоморфного шифрування є нетолерантність – вимога, щоб криптоаналітик не зміг перетворити шифротекст m в шифротекст будь-якого «залежного» повідомлення. Тобто повинна бути можливість обчислити будь-яку функцію з деякого зумовленого класу F_{HOM}, але вона не повинна бути в змозі перетворити шифротекст m в шифротекст f(m) для будь-якого $f \notin F_{HOM}$. Тобто нетолерантність є по суті вираженням функції контролю над обчисленнями, що виконує система гомоморфного шифрування.

Тобто для більшості практичних прикладань достатньо, щоб повністю гомоморфна схема ε була компактною та гомоморфною відносно усіх булевих схем функціональних елементів та зберігала контроль над своїми обчисленнями.

Кріптостійкість гомоморфних алгоритмів. Гомоморфне відображення можна представити через множину лінійних векторів X та Y [8], причому $|X| = 2^n, |Y| = 2^m$, $n \le m$. Якщо задати довільну функцію від i змінних $\lambda(x_1, x_2, ..., x_i)$, де $x_i \in X$, $\lambda(x_1, x_2, ..., x_i) \in X$, тоді гомоморфне шифрування задається парою відображень

$$f : X \xrightarrow{f} Y; \quad y = f(x); \tag{3}$$

$$f^{-1} : X \xrightarrow{f^{-1}} Y; \quad x = f^{-1}(y), \tag{4}$$

таких, що $\forall\lambda(x_1, x_2, ..., x_i)$ виконуються умови:

$$f^{-1}(f(\lambda(x_1, x_2, ..., x_i))) \equiv \lambda(x_1, x_2, ..., x_i), \tag{5}$$

$$\exists\lambda_f(y_1, y_2, ..., y_i) : \lambda(x_1, x_2, ..., x_i) \equiv \equiv f^{-1}(\lambda_f(y_1, y_2, ..., y_i)). \tag{6}$$

Рівняння (5) гарантує незмінність результату при шифруванні та дешифруванні довільної функції, а (6) дозволяє відображувати довільну операцію над множиною X в операцію над множиною Y.

Гомоморфне шифрування може відображати лише базисні операції, тобто такі операції, через які можна виразити всі функції. Умова відображення всіх можливих функцій і відображення базисних функцій є еквівалентними. Тобто, можливі такі відображення, як побітна сума по модулю 2, побітна кон'юнкція, побітне заперечення та бітовий зсув.

Розглянемо кріптостійкість гомоморфних систем. Проаналізуємо, як така система реагує на перехват шифротекста y:

$$f(0) = y \underset{f}{\oplus} y, \; f(2^n - 1) = y \underset{f}{\vee} \underset{f}{\neg} y;$$

$$f(2^0) = (f(2^n - 1) \underset{f}{>>} n - 1;$$

$$f(2^i) = (f(2^n - 1) \underset{f}{>>} n - i - 1) \underset{f}{\oplus}$$

$$\underset{f}{\oplus}(f(2^n - 1) \underset{f}{>>} n - i), \; i > 0.$$

Якщо $|X| \equiv |Y|$, тобто $|n| \equiv |m|$, i-й біт відкритого тексту знаходиться наступним чином:

$$f^{-1}(y) \wedge 2^i \equiv \begin{cases} 0, \text{ якщо } y \underset{f}{\wedge} f(2^i) \equiv f(0), \\ 1, \text{ в іншому випадку.} \end{cases}$$

Тобто без знання ключа шифрування можливо отримання відкритого тексту. Кількість гомоморфних операцій для отримання образів 2^i дорівнює

$$\omega_{\underset{f}{\oplus}} + \omega_{\underset{f}{\neg}} + \omega_{\underset{f}{\vee}} + \omega_{\underset{f}{>>}} =$$

$$= (1 + n - 1) + 1 + 1 + (n - 1) = 2n + 1.$$

Перевірка біт потребує n гомоморфних операцій та n звичайних операцій порівняння.

Якщо ймовірність отримання образу фіксованого прообразу розподілена рівномірно, то можна отримати повний перебір прообразів f(0) шляхом перехоплення k шифротекстів. Тоді спочатку розраховується k нових образів

$$f(0) = y_k \underset{f}{\oplus} y_k,$$

а потім усіма можливими додаваннями образи $C_k^2, C_k^3, ..., C_k^{k-1}, C_k^k$, тобто 2^k образів f(0).

Якщо Θ – множина усіх знайдених f(0), то i-й біт відкритого тексту

$$f^{-1}(y) \wedge 2^i \equiv \begin{cases} 0, \text{ якщо } y \underset{f}{\wedge} f(2^i) \in \Theta, \\ 1, \text{ в іншому випадку.} \end{cases}$$

У випадку, коли ймовірність розподілення образів фіксованого прообразу нерівномірна, то повний перебір може бути завершений за менший час, тому що існує такий образ f(0), ймовірність перейти до котрого після певної кількості операцій наближується до нуля.

Для аналізу кількості гомоморфізмів в випадку, коли n=m верхня оцінка складає

$$\left|X \xrightarrow{f} Y\right| \le 2^n \cdot 2^m = 2^{n+m}.$$

В випадку, коли n<m, верхня оцінка повних гомоморфних систем

$$\left|X \xrightarrow{f} Y\right| \le 2^{n+m} \cdot (n+1)^{2^m - 2^n}.$$

Слід зазначити, що при відсутності будь-якої базової операції загальний підхід до атаки стає неможливим.

Висновки

На основі приведеного аналізу існуючих гомоморфних алгоритмів шифрування можна зробити висновки, що на даний час за їх допомогою неможливо забезпечити потрібний рівень секретності в хмарних обчисленнях. Повністю гомоморфні системи можливі лише при достатній різниці розмірності просторів прообразів і образів. Проте ця умова вимагає великих обчислювальних ресурсів, що при поточному рівні технологічного розвитку є критичним. Тобто доцільно проводити побудови гомоморфних систем під конкретні завдання, які будуть вирішуватися над шифротекстом.

Перспективним напрямом удосконалення гомоморфних алгоритмів є підвищення ефективності шифрування, зокрема на основі матричних поліномів, розробка діючих методів оцінки рівня їх криптостійкості та пошук оптимального співвідношення між показниками гомоморфізму та нетолерантності. Подальші дослідження повинні охоплювати питання адаптації існуючих алгоритмів гомоморфного шифрування до особливостей застосування їх у хмарних обчисленнях.

Список літератури

1. Білова Т.Г. Перспективи використання хмарних технологій в системах електронного документообігу / Т.Г. Білова, В.О. Ярута [Текст] // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4 (120). – С. 86-89.

2. Білова Т.Г. Аналіз ризиків референтної структури хмарних обчислень / Т.Г. Білова, В.О. Ярута, І.О. Побіженко [Текст] // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – № 3 (16). – С. 144-147.

3. Білова Т.Г. Методи підвищення безпеки обробки даних в хмарних обчисленнях / Т.Г. Білова, В.О. Ярута, В.В. Побіженко // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2015. – Вип. 4 (45). – С. 71-73.

4. Gentry C. A fully homomorphic encryption scheme [Текст] / C. Gentry. – Ph.D. Thesis, 2009. – 199 p.

5. Жиров А.О. Безопасные облачные вычисления с помощью гомоморфной криптографии [Текст] / А.О. Жиров, О.В. Жирова, С.Ф. Кренделев // Безопасность информационных технологий. – М., 2013. – № 1. – С. 6-12.

6. Методы полностью гомоморфного шифрования на основе матричных полиномов / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 14-24.

7. Шевченко П.П. Шифрование как метод обеспечения безопасности конфиденциальной информации в "облачных вычислениях" / П.П. Шевченко, Н.В. Мельников [Текст] // Мат-лы XXI научн.-техн. конф. "Системы безопасности – 2012". – М.: Академия ГПС МЧС России, 2012. – С. 60-62.

8. Малинский А.Е. Оценка криптостойкости полностью гомоморфных систем [Електрон. ресурс] / А.Е. Малиновский // Инженерный журнал: наука и инновации. – 2013. – Вып. 11. – Режим доступа: http:// engjournal.ru/catalig/it/security/995.html.

Надійшла до редколегії 30.09.2016

Рецензент: д-р техн. наук, проф. Г.Г. Асєєв, Харківська державна академія культури, Харків.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ГОМОМОРФНОГО ШИФРОВАНИЯ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ

Т.Г. Белова

Рассмотрены основные понятия гомоморфного шифрования. Проанализированы существующие алгоритмы построения полностью гомоморфных систем. Определены подходы к оценке криптостойкости гомоморфного шифрования. Сформулированы проблемы и перспективы использования гомоморфного шифрования для организации безопасности обработки данных в облачных вычислениях.

Ключевые слова: *облачные технологии, безопасность данных, криптографические системы, гомоморфное шифрование, криптостойкость, матричный полином.*

PROBLEMS AND PROSPECTS FOR THE USE OF METHODS HOMOMORPHIC ENCRYPTION IN CLOUD TECHNOLOGIES

T.G. Bilova

The basic concept of homomorphic encryption. We analyzed the existing algorithms for constructing a fully homomorphic systems. Approaches to the evaluation of the reliability of the homomorphic encryption. Formulated the problems and prospects of using homomorphic encryption for data security in cloud computing.

Keywords: *cloud computing, data security, cryptographic systems, homomorphic encryption, cryptographic, matrix polynomial.*