кибербезопасности индустриальных систем управления / Гончар С. Ф. // Тези доповідей міжнародної науково-практичної конференції "Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК", Київ, – 2013. – С. 36-37. ***3.*** *Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В. В. Мохор, А. М Богданов, А. С. Килевой – К.: ООО «ТриК», 2013. – 129 с.* ***4.*** *Грицай Г., Тиморин А., Гольцев Ю., Ильин Р. Безопасность промышленных систем в цифрах. – М.: Positive Technologies, 2012.* ***5.*** *Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури / Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. // Вісник Національного університету "Львівська політехніка": "Комп'ютерні системи та мережі". №806. – 2014. – 34 с.* ***6.*** *Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models.* ***7.*** *Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.*

Анна Ільєнко
Національний авіаційний університет

УДК 004.056.53(045)

СУЧАСНІ МЕТОДИ ГОМОМОРФНОГО ШИФРУВАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анотація: **Проведено порівняльний аналіз гомоморфних методів шифрування інформаційних ресурсів на основі забезпечення цілісності. В результаті складена порівняльна таблиця оцінки ефективності використання даних алгоритмів.**
Summary:. **Conduct comparative analysis homomorphic encryption methods of information sources based on integrity As a result, compiled a comparative table of assessing the efficiency of these algorithms.**
Ключові слова: **Інформаційна безпека, гомоморфне шифрування, криптографічна система, цілісність, електронно-цифровий підпис**

I Вступ

Наразі з метою захисту інформаційних ресурсів, що передаються, обробляються та зберігаються в сучасних інформаційно-комунікаційних системах та мережах (далі – ІКСМ), зазвичай використовують різноманітні криптографічні методи шифрування. Методи шифрування дозволяють досить надійно та ефективно захищати інформацію від несанкціонованого доступу та ознайомлення з нею. Застосування криптографічного захисту, тобто використання процедури шифрування тексту за допомогою складних математичних алгоритмів завойовує все більшу популярність. Одним з таких методів є алгоритм гомоморфного шифрування інформації.

Вперше поняття «гомоморфне шифрування» було використане в 1978 році після розробки відомого асиметричного алгоритму RSA його авторами Рональдом Рівестом, Леонардо Адлеманом та Майклом Дертузосом, але їх перші спроби обґрунтувати необхідність та можливість практичного застосування гомоморфного шифрування були невдалими. В 2009 році співробітником IBM Крейгом Джентрі була запропонована модель повністю гомоморфної криптографічної системи, за допомогою якої стало можливим реалізувати операції додавання та множення над зашифрованими даними без їх попереднього розшифрування [1 – 3].

II Постановка задачі

Наразі криптографічні гомоморфні алгоритми шифрування інформації широко використовуються в автоматизованих системах, хмарних обчисленнях і реалізуються у вигляді апаратних, програмних та/або програмно-апаратних методів. Використовуючи новітні методи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна досягнути високого рівня захищеності інформаційного обміну.

Метою даної статті є аналіз та порівняльна характеристика сучасних алгоритмів гомоморфного шифрування, визначення їх переваг та недоліків, принципів та специфіки використання, перспективи застосування в сучасних інформаційно-комунікаційних системах та мережах на основі забезпечення цілісності та конфіденційності.

III Основна частина

Характеристика сучасних гомоморфних алгоритмів шифрування та їх порівняльний аналіз

Під поняттям гомоморфного шифрування будемо розуміти модель шифрування, яка дозволяє виконувати певні математичні дії з зашифрованим текстом і отримувати зашифрований результат, який відповідає результату аналогічної операції, що проводиться з відкритим текстом.

Сучасні гомоморфні системи шифрування поділяються на 2 класи: частково гомоморфні системи та повністю гомоморфні системи.

Під поняттям ***частково гомоморфні*** системи будемо розуміти такі криптосистеми, які гомоморфні відносно тільки одної математичної функції (додавання або множення). Найбільш поширені та ефективні частково гомоморфні алгоритми описуються нижче [1 – 4].

Криптосистема RSA. Алгоритм асиметричного шифрування є одним з найбільш відомих та ефективних алгоритмів шифрування інформаційного потоку даних. Алгоритм є частково гомоморфним, бо володіє властивістю гомоморфності відносно операції множення відкритих текстів.

Нехай N – модуль алгоритму, $N = p \cdot q$, де p і q – взаємно прості числа, e – відкрита експонента, взаємно проста з $\varphi(n)$, m_1 – відкритий текст, k – відкритий ключ, функція шифрування:

$$E\left[(N,e),m_1\right] = m^e \bmod N. \tag{1}$$

При цьому для будь-яких значень m_1 і m_2 виконується умова гомоморфності відносно операції множення:

$$E(k,m1)\cdot E(k,m2) = m1^e \cdot m2^e \cdot \bmod N = E(k,m1\cdot m2). \tag{2}$$

Криптосистема Ель-Гамаля – найпростіший алгоритм шифрування, що ґрунтується на дискретному логарифмуванні. На відміну від RSA в алгоритмі Ель-Гамаля існують деякі відкриті параметри, які можуть бути у більшості користувачів інформаційного обміну. Вони називаються параметрами домена (ключа). В Криптосистемі Ель-Гамаля в циклічній групі G, якщо відкритий ключ є (G,q,p,h), де $h = g^x$, x – закритий ключ, функція шифрування виглядає наступним чином:

$$E(m) = \left(g^r, m\cdot h^r\right), r \in (0....,q-1). \tag{3}$$

При цьому для будь-яких значень m_1 і m_2 виконується умова гомоморфності відносно операції множення:

$$E(m1)\cdot E(m2) = \left(g^{r1}, m1\cdot h^{r1}\right)\cdot\left(g^{r2}, m2\cdot h^{r2}\right) = \left(g^{r1+r2}, (m1\cdot m2)\cdot h^{r1+r2}\right) = E(m1\cdot m2). \tag{4}$$

Таким чином, можна стверджувати, що криптосистема Ель-Гамаля є гомоморфною відносно операції множення.

Криптосистема Пейє. Даний криптографічний алгоритм заснований на принципі факторизації великого числа, що є добутком двох простих чисел.

Система є гомоморфною відносно операції додавання, бо знаючи відкритий ключ та шифротексти, що відповідають відкритим текстам m_1 і m_2, можна обчислити шифротекст відкритого тексту $(m_1 + m_2)$.

Це можна довести наступним чином. Нехай p і q – взаємно прості числа, $N = p \cdot q$, $L = \text{НСК}(p-1, q-1)$.

Далі обчислюємо M :

$$M = \left(L\cdot(g^L \bmod n^2)\right)^{-1} \bmod n. \tag{5}$$

Обираються числа g та r з множини Z, відкритим ключем є пара чисел (n,g), закритим ключем – пара чисел (L,M). Для здійснення операції шифрування відкритого тексту m проводиться наступне обчислення:

$$C = g^m \cdot r^n \bmod n^2. \tag{6}$$

При цьому для будь-яких значень m_1 і m_2, виконується умова гомоморфності:

$$E(m1)\cdot E(m2) = \left(g^{m1}\cdot r1^n\right)\cdot\left(g^{m2}\cdot r2^n\right) = \left(g^{m1+m2}\cdot r1\cdot r2^n\right) = E\left(m1+m2\right)\bmod n^2. \tag{7}$$

В даному випадку властивість гомоморфності описується не так, як в вище вказаних алгоритмах, бо добутком двох зашифрованих чисел буде їх сума, тобто при $E(k,m1)\cdot E(k,m2)\bmod n^2$ буде отримано при дешифруванні $(m1+m2)\bmod n^2$.

Під поняттям ***повністю гомоморфні*** системи будемо розуміти такі криптосистеми, які дозволяють здійснювати операції «+» та «х» над зашифрованими даними таким чином, що результат розшифрування збігається з результатом виконання тієї ж операції над незашифрованими даними. Найбільш поширена – криптосистема Гентрі [4 – 6].

Криптосистема Гентрі. Розглянемо запропонованому ним схему на прикладі обчислень в просторі *Z*. Нехай *p* – непарне число, $p=(2\cdot k+1)$. Це число *p* є секретним параметром. Припустимо, що проводиться шифрування двійкових бітів, тому *m* – відкритий текст, приймає значення 0 або 1. Тоді виберемо число $z=2\cdot r+m$, звідси – $z=m \bmod 2$.

Процедура шифрування полягає в наступному:

Для кожного значення M обчислюється функція:

$$C=z+p\cdot q, \tag{8}$$

де *q* – довільне число.

Відповідно функція шифрування має наступний вигляд:

$$C=2\cdot r+m+(2\cdot k+1)\cdot q. \tag{9}$$

Тоді процедура дешифрування складається з наступних математичних процедур.

Нехай нам відомі числа *c* та *p*, де *c* – зашифроване число, *p* – секретний параметр. Процедура дешифрування включає наступні дії:

$$r=c \bmod p=(z+p\cdot q) \bmod p=z \bmod + p\cdot q \bmod p. \tag{10}$$

Параметр $r=c \bmod p$ називається шумом, його можливі значення лежать в інтервалі від (–*p*/2;*p*/2). Далі отримуємо відкритий текст:

$$m=r \bmod 2. \tag{11}$$

Даний алгоритм є повністю гомоморфним, що можливо довести наступним чином. Припустимо, що є 2 числа m_1 і m_2. Зіставимо для них пару чисел Z_1 і Z_2:

$$Z_1=2r+m_1, \tag{12}$$

$$Z_2=2r+m_2. \tag{13}$$

Секретний параметр $p=(2\cdot k+1)$ – непарне число.

Функції шифрування виглядають наступним чином:

$$c_1=z+pq_1, \tag{14}$$

$$c_2=z+pq_2. \tag{15}$$

Тоді їх сума та добуток будуть дорівнювати відповідно:

$$\begin{aligned} &c_1+c_2=z_1+z_2+p(q_1+q_2)=2r_1+m_1+2r_2+m_2+p(q_1+q_2)= \\ &=2(r_1+r_2)+m1+m2+(2k+1)(q_1+q_2); \end{aligned} \tag{16}$$

$$\begin{aligned} &c_1c_2=z_1z_2+p(z_1q_2+z_2q_1)+p^2q_1q_2= \\ &=(2r_1+m_1)(2r_2+m_2)+2k(z_1q_2+z_2q_1)+z_1q_2+z_2q_1= \\ &=4r_1r_2+2(r_1m_2+r_2m_1)+m_1m_2+2k(z_1q_2+z_2q_1)+ \\ &+2r_1q_2+2r_2q_1+m_1q_2+m_2q_1. \end{aligned} \tag{17}$$

Застосування процедури дешифрування дасть наступний результат:

$$(c_1+c_2) \bmod 2=\left[2(r_1+r_2)+m_1+m_2\right] \bmod 2=(m_1+m_2). \tag{18}$$

Не знаючи секретний параметр *p*, розшифрувати результат неможливо:

$$(c_1+c_2) \bmod 2=\left[m_1+m_2+q_1+q_2\right]. \tag{19}$$

Використовуючи формулу (10) для дешифрування, отримаємо аналогічний результат:

$$(c_1c_2) \bmod 2=\left[2(r_1+r_2)+m_1m_2\right] \bmod 2=(m_1m_2). \tag{20}$$

Таким чином, доведено, що алгоритм Гентрі являє собою повністю гомоморфне шифрування.

Проте, незважаючи на те, що криптосистему Гентрі можна реалізувати програмно і використовувати в хмарних обчисленнях, вона має певні недоліки. Вони обумовлені тим, що існуючий шум (параметр *r*) при послідовному виконанні операцій швидко накопичується, і після того, як він перевищує параметр *p*, алгоритм працює неправильно і правильно розшифрувати криптограму стає неможливо. Тому насправді на

практиці алгоритм реалізувати дуже важко, бо в реальних обчисленнях помилка r дуже швидко накопичується, і для того, щоб цього уникнути, необхідно використовувати дуже складні алгоритми, що в свою чергу вимагають значних обчислювальних ресурсів.

Для вирішення недоліків в схемі Гентрі розробниками був запропонований механізм *bootstrapping*. Проте повністю ліквідувати недоліки схеми не вдалося, бо використання даного методу приводить до значного збільшення об'єму шифрованого тексту в схемі і значної кількості обчислювальних ресурсів. Тому для використання даного методу на практиці необхідно використовувати складні алгоритми, або обмежувати кількість операцій, які можуть виконуватися над даними.

Порівняльна характеристика алгоритмів гомоморфного шифрування наведена в таблиці 1.

Таблиця 1 – Порівняльна характеристика алгоритмів гомоморфного шифрування

Алгоритм	Ключ (біт)	Переваги	Недоліки	Гомо-морф-ність	Практичне застосування
1	2	3	4	5	6
RSA	1024	Є одним з найбільш криптостійких алгоритмів, при довжині ключа в 2048 біт практично унеможливлює крипто аналіз за рахунок задачі факторизації складних чисел, відсутність необхідності передачі секретного ключа каналами зв'язку.	Велика довжина ключа, порівняно з іншими алгоритмами (наприклад, симетричними), велика обчислювальна складність, значні обчислювальні ресурси, тому на практиці поєднується з іншими алгоритмами	Часткова	Практично не застосувався в зв'язку з великими обчислювальними ресурсами та затратами, що необхідні для практичної реалізації, теоретично можливо використовувати для забезпечення цілісності та конфіденційності інформації. Використовується для шифрування та формування ЕЦП.
Ель-Гамаля	1024	Є одним з найбільш криптостійких алгоритмів; криптостійкість заснована на вирішенні задачі дискретного логарифмування в кінечному полі, відсутність необхідності передачі секретного ключа каналами зв'язку.	Велика довжина ключа, велика обчислювальна складність, збільшення довжини шифру порівняно з початковим текстом.	Часткова	Теоретично використання можливе, але в поєднанні з іншими алгоритмами. Використовується для шифрування та формування ЕЦП.
Пейє	256	Криптосистема з відкритим ключем, заснована на задачі факторизації та складності обчислення квадратного кореня залишку від ділення, за рахунок введення випадкових параметрів (ймовірнісних величин) збільшується криптостійкість, відсутність передачі секретного ключа.	Криптостійкість менша, ніж в алгоритмах RSA та Ель-Гамаля, велика обчислювальна складність, вразливість до криптоаналізу при малій довжині ключа, вразливість до атаки по підібраному шифротексту.	Часткова	Теоретично використання можливе, але в поєднанні з іншими алгоритмами. Використовується для шифрування, формування ЕЦП та електронного голосування.
Гентрі	512	Є єдиною на даний час криптосистемою, заснованою на принципі повного гомоморфного шифрування, забезпечує	Велика обчислювальна складність, труднощі практичної реалізації алгоритмів, великий	Повна	Можливе використання з метою забезпечення конфіденційності інформації при її передачі та зберіганні на серверах

		конфіденційність інформації, що зберігається на серверах провайдерів хмарних обчислень, дає змогу виконувати операції над зашифрованим текстом, попередньо їх не розшифровуючи.	розмір шифротексту, вразливість до атаки на шифрований текст та повний перебір можливих ключів.		провайдера, можливість здійснення будь яких математичних дій з зашифрованим текстом. Використовується для шифрування, формування ЕЦП, електронного голосування та в електронній комерції.

Провівши порівняльний аналіз та характеристику сучасних алгоритмів гомоморфного шифрування, можна зробити наступні висновки:

1) визначити, який алгоритм є найбільш ефективним та потужним практично неможливо, бо вони мають свої недоліки та переваги, тому їх пріоритет в оцінці залежить від задачі, яка має бути вирішена;

2) для забезпечення криптостійкості конфіденційної інформації можливе використання асиметричних алгоритмів з відкритим ключем з метою шифрування/дешифрування інформації, генерації / перевірки ЕЦП, та надійного їх зберігання в зашифрованому вигляді;

3) у випадку, коли важливішим є питання швидкості обчислень, зменшення їх складності з метою економії програмно-апаратних ресурсів, пріоритетним є використання симетричних алгоритмів або використання комбінованих алгоритмів в поєднанні з функціями хешування; при цьому створюються різноманітні гібридні криптосистеми;

4) у випадку, коли необхідно зберегти конфіденційність інформації, що зберігається на сервері, ця інформація потребує обробки і її дешифрування при обробці несе загрозу для конфіденційності, тоді пріоритетним є використання моделі повного гомоморфного шифрування, що дає можливість виконання математичних операцій над зашифрованим текстом, при цьому не розшифровуючи його. Відповідно до цього, використовуючи алгоритм повного гомоморфного шифрування на сервері, конфіденційна інформація в відкритому вигляді зберігатися не буде на всіх етапах шифрування/дешифрування.

Практичні схеми реалізації алгоритмів гомоморфного шифрування

Повністю гомоморфна криптографічна система захисту інформації з достатньою швидкістю роботи – необхідна умова для забезпечення працездатності багатьох сучасних програмних додатків. Дана система дозволяє проводити статистичні та математичні обчислення, пошук даних, електронне голосування, схеми зобов'язань, багатосторонні секретні обчислення та будь-які інші операції над зашифрованими даними і при цьому гарантувати як високу швидкість обробки даних, так і їх конфіденційність [5, 8, 9].

Окрім досліджень в області гомоморфного шифрування також ведуться розробки на основі інших схем та в інших напрямках. Наприклад, одним із останніх досягнень в сфері захисту інформації в хмарних обчисленнях є розробка програмного комплексу ***CryptDB***, що використовує механізми гомоморфного шифрування. В CryptDB забезпечена підтримка шифрування, при якій дані на стороні СУБД ніколи не фігурують у відкритому вигляді, а всі передані в СУБД запити містять тільки зашифровані дані, у тому числі в умовних блоках. При використанні CryptDB в процесі виконання SQL-запитів всі дії проводяться тільки з зашифрованими даними, тобто користувач може відправити SQL-запит до СУБД і отримати результат без розшифровки інформації на стороні сервера (дані будуть розшифровані на обладнанні клієнта). Для забезпечення збереження конфіденційності інформації використовується багаторівнева система шифрування, при якій різні дані розміщуються на різних вкладених криптографічних рівнях, кожен з рівнів має свій ключ і підтримує обмежений набір простих операцій над зашифрованими даними. Для приховування даних на кожному рівні використовуються свої методи гомоморфного шифрування. Тим не менше, тільки повністю гомоморфне шифрування здатне зняти необхідність навіть частинного розшифрування даних для проведення обчислень над ними. Вирішивши дану проблему, гомоморфне шифрування також не можна назвати найбільш оптимальною схемою шифрування, бо воно принципово вразливе до атак по підібраному шифротексту. Нажаль, на даний момент не існує насправді якісної системи захисту інформації, заснованої на схемі гомоморфного шифрування, яка б вирішувала проблеми як конфіденційності, так і зручності використання, швидкості обчислень та продуктивності.

Тому в перспективі для ефективного використання такої системи захисту необхідна реалізація, яка б задовольняла наступні умови:

- можливість використання при проведенні процедури шифрування та дешифрування повного набору математичних функцій;
- точність і швидкість обчислень повинні бути сталими на всіх стадіях шифрування та дешифрування;

- кортеж ключів має бути настільки великим, щоб унеможливити можливість атаки повним перебором всіх можливих ключів;
- розмір зашифрованих даних та довжина ключа не має значно впливати на продуктивність системи.

IV Висновки

В результаті проведених досліджень було визначено особливості застосування гомоморфних криптосистем та алгоритмів при забезпеченні конфіденційності інформаційних ресурсів, їх класифікація, властивості та здійснений їх порівняльний аналіз. Для кожного з алгоритмів визначені недоліки, переваги, сфера застосування, можливість практичної реалізації. Серед розглянутих алгоритмів основна увага була приділена алгоритму Гентрі, що являє собою схему повністю гомоморфного шифрування і дозволяє виконувати обробку зашифрованого тексту. В даному алгоритмі існують певні недоліки, які стосуються складності його практичної реалізації. Враховуючи особливості розглянутих криптографічних алгоритмів, можна стверджувати, що саме алгоритм Гентрі є повністю гомоморфним, саме він є тим алгоритмом, на основі якого можливо виконувати практично всі операції з зашифрованим текстом задля забезпечення конфіденційності інформації при її передачі та зберіганні. Також розглянуті основні напрями удосконалення алгоритму повного гомоморфного шифрування, а також перспективи його використання.

Список використаної літератури: ***1.*** *Чунарьова А. В. Аналіз сучасних алгоритмів гомоморфного шифрування / А. В. Чунарьова, Д. М. Миколишин // Naukpwa przestrzen europy – 2014: X miedzynarodowej naukowi-praktycznej konferencji, 07-15 kwietnia 2014 r.: abstracts. – Przemysl (Polska), 2014. – V.33. – P. 98-101.* ***2.*** *Ільєнко А. В. Забезпечення конфіденційності інформаційних ресурсів на основі методів гомоморфного шифрування / А. В. Ільєнко, Р. В. Зюбіна // Авіа-2015: XII міжнародна науково-технічна конференції, 28-29 квітня 2015 р.: тези доп. – К., 2015. – С. 5.25-5.29.* ***3.*** *«Основы криптографии» / [Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.]. – Москва: Гелиос – АРВ, 2002. – 471 с.* ***4.*** *Н. П. Варновский. Гомоморфное шифрование. [Електронний ресурс] / Варновский Н. П. , Шокуров А. В // РФФИ. – 2011. – №6. – С. 27 – 36.* ***5.*** *C. Gentry , S. Halevi. Implementing gentry's fully-homomorphic encryption scheme // Gentry C., Halevi S./ Springer . – 2011. – С. 129–148.* ***6.*** *Грицик В. В. RSA та його оптимізація / В.В Грицик, Н.І. Пелих, Д.А. Януш // Наукові праці. – 2009. – Т.106. – С. 81 – 86.* ***7.*** *Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. –Москва: Кудиц – Образ, 2007. – 368 с.* ***8.*** *Акбаров Д. Е. Криптография, стандарты алгоритмов криптографической защиты информации и их приложения. – Ташкент, 2007. – 188 с.* ***9.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Москва: ТРИУМФ, 2002. – 816 с.*