УДК 004.056.53(045)

А. В. Ільєнко — канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0001-8565-1117
e-mail: chunariova@gmail.com

ОЦІНКА ЕФЕКТИВНОСТІ ОПТИМІЗОВАНОЇ КРИПТОСИСТЕМИ ГЕНТРІ З УМОВИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Вступ

Стрімке збільшення обсягів інформаційних потоків в сучасних інформаційно-комунікаційних системах та мережах, ставить підвищені вимоги до технічних характеристик мереж зв'язку та до впровадження нових сучасних методів криптографічного захисту з метою забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів та інформаційної системи в цілому. Застосування криптографічного захисту, тобто використання процедури шифрування та дешифрування з умови забезпечення конфіденційності інформації завойовує все більшу популярність. Одним з таких методів являються алгоритми гомоморфного шифрування інформації.

Постановка завдання дослідження

На сьогодні криптографічні гомоморфні алгоритми шифрування інформації широко використовуються в автоматизованих системах, хмарних обчисленнях і реалізуються у вигляді апаратних, програмних та/або програмно-апаратних методів.

Метою даних досліджень є аналіз існуючих криптосистем гомоморфного шифрування інформації, визначення критеріїв та вимог щодо формування сучасних гомоморфних систем шифрування. На базі зазначених вимог проводиться оптимізація криптосистеми Гентрі, що забезпечує мінімізацію часу на проведення програмних операцій шифрування/дешифрування та підвищення криптостійкості за рахунок додаткового шифрування сеансового ключа.

Аналіз існуючих методів гомоморфних систем шифрування інформації

Сучасні гомоморфні системи шифрування поділяються на два класи: частково гомоморфні системи (Криптосистема RSA, Ель-Гамаля, Пейє) та повністю гомоморфні системи шифрування [1, 2 с. 1–2]. Криптосистема Гентрі є алгоритмом повного гомоморфного шифрування, що дозволяє виконувати математичні операції з зашифрованим текстом і отримувати зашифрований результат, який відповідає результату аналогічної операції, що проводиться з відкритим текстом. Безперечно, сам факт можливості здійснення таких операцій є основною перевагою алгоритму і вирізняє його серед інших [3, с. 3].

Проте сама математична реалізація алгоритму має певні недоліки, які можуть дозволити зловмисникам на основі відомого ключа та зашифрованого тексту, використовуючи відомі атаки на алгоритми та засоби криптоаналізу, отримати відкритий текст. Звичайно якщо не враховувати можливість здійснення криптоаналізу зловмисниками, алгоритм ідеально би підходив для забезпечення конфіденційності інформації під час використання «хмарних» обчислень, проте в наш час, коли захист інформації від несанкціонованого доступу являється однією з найбільш актуальних проблем, важливим завданням є виявлення «слабких» місць у самому алгоритмі та їх можливе усунення за рахунок введення додаткових параметрів та функцій в алгоритм.

Одним з слабких місць алгоритму є те, що для шифрування та дешифрування використовується один і той самий сеансовий ключ. Тому необхідно звернути увагу на можливість оптимізації алгоритму з метою підвищення надійності захисту згенерованого ключа.

Математичні основи оптимізованого криптографічного алгоритму Гентрі

Спробуємо оптимізувати алгоритм Гентрі таким чином, щоб його криптостійкість та надійність була збільшена, при цьому швидкодія зменшилася би в незначному обсягу [4, 5, с. 1–2].

Криптосистема Гентрі. Розглянемо запропоновану схему для на прикладі обчислень у просторі Z. Нехай p — непарне число, $p = (2k+1)$. Число p являється секретним параметром. Припустимо, що проводиться шифрування двійкових бітів, тому m — відкритий текст, приймає значення 0 або 1. Тоді оберемо число $z = 2r + m$, звідси — $z = m \bmod 2$.

Процедура шифрування полягає в такому:

Для кожного значення M обчислюється функція:

$$C = z + pq, \qquad (1)$$

де q — довільне число.

Відповідно функція шифрування має такий вигляд:

$$C = 2r + m + (2k+1)q. \qquad (2)$$

Тоді процедура дешифрування складається з таких математичних процедур [6, с. 4].

Нехай нам відомі числа c та p, де c — зашифроване число, p — секретний параметр.

Процедура дешифрування включає такі дії:

$$r = c \bmod p = (z + pq) \bmod p = \\ = z \bmod + pq \bmod p. \quad (3)$$

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

$$m = r \bmod 2 \quad (4)$$

Даний алгоритм є повністю гомоморфним, що можливо довести так:

Припустимо, що є 2 числа m_1 і m_2. Зіставимо для них пару чисел Z_1 і Z_2:

$$Z_1 = 2r + m_1 \quad (5)$$

$$Z_2 = 2r + m_2 \quad (6)$$

Секретний параметр $p = (2 \cdot k + 1)$ — непарне число. Функції шифрування виглядають так:

$$c_1 = z + pq_1 \quad (7)$$

$$c_2 = z + pq_2 \quad (8)$$

Тоді їх сума та добуток будуть дорівнювати відповідно:

$$c_1 + c_2 = z_1 + z_2 + p(q_1 + q_2) = \\ = 2r_1 + m_1 + 2r_2 + m_2 + p(q_1 + q_2) = \\ = 2(r_1 + r_2) + m1 + m2 + (2k + 1)(q_1 + q_2); \quad (9)$$

$$c_1 c_2 = z_1 z_2 + p(z_1 q_2 + z_2 q_1) + p^2 q_1 q_2 = \\ = (2r_1 + m_1)(2r_2 + m_2) + 2k(z_1 q_2 + z_2 q_1) + \\ + z_1 q_2 + z_2 q_1 = 4r_1 r_2 + 2(r_1 m_2 + r_2 m_1) + m_1 m_2 \\ + 2k(z_1 q_2 + z_2 q_1) + 2r_1 q_2 + 2r_2 q_1 + m_1 q_2 + m_2 q_1. \quad (10)$$

Застосування процедури дешифрування дає такий результат:

$$(c_1 + c_2) \bmod 2 = \left[2(r_1 + r_2) + m_1 + m_2\right] \bmod 2 \\ = (m_1 + m_2). \quad (11)$$

Якщо секретний параметр p невідомий, розшифрувати результат неможливо:

$$(c_1 + c_2) \bmod 2 = [m_1 + m_2 + q_1 + q_2] \quad (12)$$

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

$$(c_1 c_2) \bmod 2 = [2(r_1 + r_2) + m_1 m_2] \bmod 2 = (m_1 m_2). \quad (13)$$

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

Як було зазначено вище, одним з слабких місць алгоритму є те, що для шифрування та дешифрування використовується один і той самий сеансовий ключ. Тому необхідно звернути увагу на можливість оптимізації алгоритму для підвищення надійності згенерованого ключа.

Для підвищення криптостійкості заданого алгоритму пропонується використання такої схеми шифрування, за якої сеансовий ключ додатково буде шифруватися за допомогою асиметричного алгоритму RSA і передаватися в канал зв'язку в зашифрованому вигляді. Це забезпечить криптостійкість та надійність алгоритму, оскільки для криптоаналізу та розшифрування ключа зловмиснику необхідно буде вирішити завдання розкладу параметра n на прості співмножники p та q, а за вдалого підбору цих параметрів (не менш ніж 1024 біт) таке завдання вирішити практично неможливо за сучасних умов.

Для цього в алгоритмі пропонується використовувати пару ключів (відкритий та закритий) для шифрування секретного сеансового ключа.

Використаємо додаткові параметри n, p, q при цьому $n = pq$, де p, q — взаємно прості числа, які будуть генеруватися за допомогою генератора взаємно простих чисел. Далі буде обчислюватися функція Ейлера $\varphi(n)$, що дорівнює добутку чисел $p-1$ та $q-1$. Після обчислення цього параметра буде підібране таке число e, що $1 < e < \varphi(n)$ і за допомогою алгоритму Евкліда буде обчислено число d таким чином, що $ed \equiv 1\left(\bmod\left(\varphi(n)\right)\right)$.

Отже, модернізований алгоритм Гентрі буде виглядати так. Для початку проведемо процедуру знаходження відкритого та секретного асиметричного алгоритму RSA: за допомогою криптостійкого генератора простих чисел p, q. Далі проведемо процедуру знаходження числа $n = pq$ та обчислення функції Ейлера $n = \varphi(n)$.

Далі проведемо вибір та обчислення відкритого ключа e, де $3 \le e < \varphi(n)$, а також секретного ключа d за алгоритмом Евкліда, при цьому $ed \equiv 1\left(\bmod\left(\varphi(n)\right)\right)$.

Наступним кроком буде знаходження секретного параметру. Нехай x — непарне число, $x = (2 \cdot k + 1)$. Число x є секретним параметром. Припустимо, що проводиться шифрування двійкових бітів, тому m — відкритий текст, приймає значення 0 або 1.

Тоді оберемо число $z = 2r + m$, звідси — $z = m \bmod 2$.

Процедура шифрування полягає в такому:

Для кожного значення M обчислюється функція:

$$C = z + x \cdot h, \quad (14)$$

де h — довільне число.

Відповідно функція шифрування має такий вигляд:

$$C = 2r + m + (2k+1)h\,. \qquad (15)$$

Процедура шифрування сеансового ключа (секретного параметру $\boldsymbol{x}$) з використанням асиметричного алгоритму RSA:

$$X = x^e \bmod n\,,$$

де (e, n) — відкритий ключ криптосистеми RSA.

Процедура дешифрування сеансового ключа (секретного параметру $\boldsymbol{x}$) з використанням асиметричного алгоритму RSA:

$$x = X^d \bmod n\,,$$

де (d, n) — секретний ключ криптосистеми RSA.

Тоді процедура дешифрування криптограми складається з таких математичних процедур (див. формули 5–13).

$r = c \bmod x$ — функція дешифрування;

$m = r \bmod 2$ — відкритий текст.

Модернізований алгоритм Гентрі є більш надійним та криптостійким порівняно з звичайним алгоритмом, оскільки не дає можливості зловмиснику розшифрувати повідомлення на основі відкритого ключа, що передається по каналах зв'язку, оскільки дешифрування сеансового ключа можливе лише за допомогою параметра d, який по каналу не передається і може бути захищений додатковими засобами. При цьому за правильного підбору параметрів p та q (довжиною не менш ніж 1024 біт) зловмиснику практично неможливо на основі відомого n визначити p та q (задача факторизації складеного числа). Також за рахунок модернізації алгоритму буде досягнуто те, що зловмиснику не вдасться ефективно реалізувати атаку по відомому шифротексту, оскільки для успішної її реалізації необхідно буде отримати параметр d.

Оцінка ефективності оптимізованого криптографічного методу Гентрі з умов забезпечення конфіденційності інформації

Порівняльна характеристика результатів дослідження програм, що реалізовують алгоритми RSA, Гентрі та модифікованого алгоритму Гентрі відповідно, відбувалися за такими параметрами: кількість виконуваних програмою функцій, загальний пропускний вектор $B(M)$, середній час виконання програмних функцій, співвідношення часу, який було витрачено для виконання всіх функцій програми та додаткові параметри.

Приведемо зведену таблицю порівняння.

Оцінка ефективності алгоритмів після проведених досліджень за показниками продуктивності

Параметр	RSA	Гентрі	Оптимізований алгоритм Гентрі
Кількість виконуваних програмою функцій	7	7	9
Загальний пропускний вектор B(M)	0,6193	0,329	0,2958
Співвідношення часу, який було витрачено для виконання всіх функцій програми за замовчуванням і часу, який задано апріорно для виконання всіх функцій	21,79 %	25,1 %	15,1 %
Середній час виконання програмних функцій за всі експерименти	4,69 с	5,25 с	4,01 с
Фактор, який найбільш впливає на швидкість виконання програмних функцій	Довжина ключа	Довжина ключа	Значення параметра e
Фактор, який найменше впливає на швидкість виконання програмних функцій	Тип криптопровайдера	Наявність хеш-функції	Шифрування суми

Із отриманих результатів , можна зробити такі висновки:

По-перше, якщо брати до уваги показник швидкодії алгоритму, а саме швидкість виконання операцій шифрування/дешифрування інформації, оптимізований алгоритм Гентрі забезпечує значно вищу криптостійкість за рахунок додаткового шифрування сеансового ключа, проте при цьому за рахунок складності математичних обчислень, час на виконання програмних функцій зменшується. Кількісне значення середнього часу виконання процесу шифрування/дешифрування для всіх експериментів, значно менше порівняно з відомими методами (зменшення часу від 1,17 до 1,31 рази, залежно від використовуваного методу).

По-друге, існує фактор, за допомогою якого можливо значно зменшити швидкість виконання операцій шифрування та дешифрування. Цим фактором є показник e. Час виконання операцій зростає із збільшенням кількості ненульових бітів у двійковому поданні відкритої експоненти e. Щоб збільшити швидкість шифрування, значення e часто необхідно обирати рівним 17, 257 або

65 537 — простим числам, двійкове подання яких містить лише дві одиниці: 17(10) = = 10001(2), 257(10) = 100000001(2), 65537(10) = +100000000000000012 (прості числа Ферма).

Цей факт був перевірений при виконанні експериментів по виміру швидкості операцій шифрування та дешифрування (фактор X5 — «–»).

Слід зауважити, що важливим для підвищення криптостійкості є використання генератора псевдовипадкових чисел при формуванні параметрів алгоритму. Підбираючи параметри алгоритму, слід також враховувати те, що в випадку, якщо показник $d < n^{1/4}$ криптоаналітиками успішно може бути виконана атака Вінера для знаходження d, що заснована на теорії неперервних дробів.

Висновки

Проведено порівняльний аналіз гомоморфних методів шифрування інформаційних ресурсів на основі забезпечення цілісності та конфіденційності в сучасних інформаційно-комунікаційних системах та мережах. У статті описані сучасні гомоморфні системи шифрування, а саме частково гомоморфні системи та повністю гомоморфні системи шифру-вання.

Розглянуто криптосистеми RSA, Ель-Гамаля, Пейє та Гентрі. У результаті визначено особливості застосування гомоморфних криптосистем та алгоритмів при забезпеченні цілісності та конфіденційності інформаційних ресурсів, їх класифікація та властивості. Визначені шляхи оптимізації криптографічного алгоритму Гентрі, а також перспективи його використання при здійсненні хмарних обчислень.

Оцінка ефективності методів шифруванняпроведена на основі міжнародного стандарту ISO 14756 «Information technology. Measurement and rating performance evaluation software systems».

ЛІТЕРАТУРА

1. **Чунарьова А. В.**, Миколишин Д. М. Аналіз сучасних алгоритмів гомоморфного шифрування. — Режим доступу: http://www.rusnauka.com/11_NPE_2014/Informatica/4_166663.doc.htm

2. **Чунарьова А. В.** Практичні схеми реалізації алгоритмів електронного цифрового підпису // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук.-техн. зб. — К. : НТУУ «КПІ», 2013. — № 1 (25). — С. 81–88.

3. **Чунарьова А. В.** Сучасні методи гомоморфного шифрування інформаційних ресурсів // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук.-техн. зб. — К. : НТУУ «КПІ», 2015. — № 2 (30). — С. 52–57.

4. **Gentry C.** Implementing Gentry's Fully-Homomorphic Encryption Scheme. — URL: http://link.springer.com/book/10.1007/978-3-642-20465-4, doi.org/10.1007/978-3-642-20465-4_9. (eng)

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

6. **Буртыка Ф. Б.** 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), doi.org/10.15514/ispras-2014-26(5)-5. (rus).

Ільєнко А. В.

ОЦІНКА ЕФЕКТИВНОСТІ ОПТИМІЗОВАНОЇ КРИПТОСИСТЕМИ ГЕНТРІ З УМОВИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

У статті вперше визначено особливості функціонування оптимізованої криптосистеми Гентрі. Проведено аналіз існуючих гомоморфних систем шифрування інформації та на основі проведеного аналізу виділено переваги і недоліки сучасних алгоритмів. У результаті визначено особливості застосування гомоморфних криптосистем при забезпеченні цілісності та конфіденційності інформаційних ресурсів, їх класифікація та властивості. Проведений аналіз дозволив сформувати подальші шляхи оптимізації криптографічного алгоритму Гентрі, а також перспективи його використання при здійсненні хмарних обчислень. Оптимізований алгоритм Гентрі забезпечує значно вищу криптостійкість за рахунок додаткового шифрування сеансового ключа. Проведена оцінка ефективності оптимізованого криптографічного методу Гентрі з умов забезпечення конфіденційності інформації проводилася на основі міжнародного стандарту ISO 14756 «Information technology. Measurement and rating performance evaluation software systems».

Ключові слова: захист інформації, гомоморфне шифрування, криптосистема, конфіденційність.

Ilyenko A. V.

EVALUATING THE EFFECTIVENESS OF THE OPTIMIZED CRYPTOGRAPHIC SYSTEM GENTRY OF CONDITIONS FOR ENSURE THE CONFIDENTIALITY OF INFORMATION

The paper first defined the peculiarities of the optimized cryptographic Gentry. The analysis of existing homomorphic encryption of information systems and on the basis of the analysis highlighted the advantages and disadvantages of modern algorithms. As a result of identified features of the application of homomorphic cryptosystems, while ensuring the integrity and confidentiality of information resources, their classification and properties. The analysis allowed to generate further ways to optimize cryptographic algorithm Gentry, as well as his use of in the implementation of cloud computing. Optimized algorithm Gentry provides significantly greater cryptographic strength due to additional encryption of the session key. The efficiency of the optimized cryptographic method Gentry of the conditions to ensure confidentiality of the information was based on the international standard ISO 14756 «Information technology. Measurement and rating performance evaluation software systems».

Key words: information security, homomorphic encryption, cryptosystem, confidentiality.

Ильенко А. В.

ОЦЕНКА ЭФФЕКТИВНОСТИ ОПТИМИЗИРОВАННОЙ КРИПТОСИСТЕМЫ ГЕНТРИ ИЗ УСЛОВИЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

В статье впервые определены особенности функционирования оптимизированной криптосистемы Гентри. Проведён анализ существующих гомоморфных систем шифрования информации и на основе проведённого анализа выделены преимущества и недостатки современных алгоритмов. В результате определены особенности применения гомоморфных криптосистем при обеспечении целостности и конфиденциальности информационных ресурсов, их классификация и свойства. Проведённый анализ позволил сформировать дальнейшие пути оптимизации криптографического алгоритма Гентри, а также перспективы его использования при осуществлении облачных вычислений. Оптимизированный алгоритм Гентри обеспечивает значительно более высокую криптостойкость за счёт дополнительного шифрования сеансового ключа. Проведена оценка эффективности оптимизированного криптографической метода Гентри из условий обеспечения конфиденциальности информации проводилась на основе международного стандарта ISO 14756 «Information technology. Measurement and rating performance evaluation software systems».

Ключевые слова: защита информации, гомоморфное шифрование, криптосистема, конфиденциальность.

Стаття надійшла до редакції 03.02.2017 р.
Прийнято до друку 06.02.2017 р.
Рецензент – д-р техн. наук, проф. Б. Я. Корнієнко