15. *Lukashov V., Romanko S, Timofeev S, Protsenko A*. Rate of Components Evaporation from Sulfuric Acid Solution During Its Concentrating in Air Flow / Chemistry & Chemical Technology, Vol. 11, No. 3, pp.344-348, 2017
16. ANSYS FLUENT 12.0 User's Guide. ANSYS, Inc. is certified to ISO 9001:2008, 2009 – 2070 pp.
17. *Azarenkov N.A., Rudychev V.G., Pismenetskiy S.A.* Solid and liquid waste processing and reducing of personnel doses / «Journal of Kharkiv National University» physical series «Nuclei, Particles, Fields», issue 3 /55/, 1017, 2012– pp.117-122
18. *Greenshields C.* OpenFOAM User Guide version 6. The OpenFOAM Foundation, 2018 – 237 pp.
19. Сайт SolidWorks Flow Simulation https://hawkridgesys.com/solidworks/ (відкритий доступ станом на 02.10.2018)
20. *Raskob W., Landman C. Trybushnyi D.* Functions of decision support systems (JRodos as an example): overview and new features and products (el source https://www.radioprotection.org/articles/radiopro/pdf/2016/03/radiopro160015-s.pdf)
21. HotSpot Health Physics Codes Version 3.0 User's Guide/ National Atmospheric Release Advisory Center, LNLL, 2014 – 198 pp.
22. RASCAL 4.3 User's Guide / Ramsdell Environmental Consulting, LLC, 2013– 125 pp.
23. Сайт Sandia https://www.sandia.gov/ (відкритий доступ станом на 02.10.2018)
24. WinMACCS, a MACCS2 Interface for Calculating Health and Economic Consequences from Accidental Release of Radioactive Materials into the Atmosphere MACCS User's Guide / U.S. Nuclear Regulatory Commission, 2007 – 233 pp.
25. Богорад В. І., Бєлов Я. Ю., Кириленко Ю. О. та ін. Поєднання апаратних засобів мобільної лабораторії RanidSONNI та комп'ютерних технологій СППР RODOS для прогнозу наслідків виникнення пожежі в зоні відчуження Чорнобильської АЕС / Журнал «Ядерна та радіаційна безпека», №3(79).2018, – С.10-15

http://doi.org/10.5281/zenodo.3612242

Поступила 16.09.2019р.

УДК 681.3

А.В. Ільєнко, Київ
С.С. Ільєнко, Київ
О.В. Прокопенко, Київ

ОЦІНКА ПРОДУКТИВНОСТІ АЛГОРИТМІВ ГОМОМОРФНОГО ШИФРУВАННЯ ВІДПОВІДНО ДО ДСТУ ISO/IEC 14756:2010

Abstract. We proposed the method for evaluating the performance of applications and implementations of homomorphic encryption algorithms to ensure the integrity and confidentiality of information in modern systems and networks based on the DSTU ISO 14756: 2010 standard. The procedure for evaluating performance is determined in stages. The series of experiments is conducted.

Вступ

В зв’язку з глобальними викликами формування кібернетичного простору в державних та міждержавних масштабах, та загрози втручання в процеси передачі інформації збоку «опонентів» виникає обґрунтована необхідність в володінні потужними засобами безпечної обробки та передачі інформації, сформованої в електронному вигляді. Особливо актуальні задачі захищеної інформації та швидкості зворотного зв’язку в таких напрямках як авіаційна та ракетно-космічна галузі (бездротовий зв'язок «земля-повітря», «повітря-повітря»), банківська сфера (безпека електронних грошових операцій), військова сфера (інформація стратегічного характеру), інформаційно-комунікаційні системи та мережі, тощо. Отже захищеність та продуктивність системи обробки даних є одним з її найбільш важливих властивостей інформаційної системи. Саме про продуктивність інформаційної системи далі і йтиме мова в даному дослідженні.

Під поняттям «*оцінка продуктивності програмного забезпечення»* буде надалі розуміти діяльність, що включає в себе всі методи оцінки продуктивності обробки даних в інформаційних системах, де продуктивність виражається числовими характеристиками, а також може включати оцінку, наскільки якісно продуктивність задовольняє вимогам користувачів.

Постановка задачі дослідження

В даній статті буде описаний метод оцінки продуктивності програм, що виконують криптографічні операції з відкритим текстом на базі алгоритмів гомоморфного шифрування на основі забезпечення цілісності та конфіденційності інформації.

Для вирішення поставленої задачі було зроблено наступне:

1. Проаналізовані різні методи гомоморфного шифрування [9, 10] і, визначено переваги та недоліки повністю та частково гомоморфних систем.
2. Виділені подальші шляхи удосконалення алгоритму Гентрі [6, 7], для подальшого їх використання при проведенні процедури шифрування та дешифрування інформації.
3. Написані програмні реалізації для проведення процедури шифрування та дешифрування з використанням алгоритму RSA, Ель-Гамаля, Гентрі та удосконаленого алгоритму Гентрі з метою подальшого проведення оцінки продуктивності за ДСТУ ISO/IEC 14756:2010.
4. За результатами проведених експериментів, були зроблені висновки про продуктивність використання удосконаленого алгоритму Гентрі, для вирішення поставленої задачі забезпечення цілісності та конфіденційності інформації.

Для користувача інформаційної системи критичне питання полягає в тому, чи буде її продуктивність достатньою для виконання необхідних обчислень. В даний час існує велика кількість методів для опису та вимірювання продуктивності програмного забезпечення. Кожен метод був розроблений для певного типу системи обробки даних і його використання в

конкретному середовищі. Для вирішення цих проблем ISO було розроблено новий метод, який можна застосувати для широкого спектру типів систем обробки даних та додатків. ДСТУ ISO/IEC 14756:2010 представляє сучасні принципи вимірювання продуктивності комп'ютера і вимірювання ефективності часу запуску і виконання програмного забезпечення. Використання даного стандарту дозволяє проводити оцінку продуктивності програмного забезпечення. ДСТУ ISO/IEC 14756:2010 визначає 3 класи характеристик продуктивності програмного забезпечення: перший клас описує те, що комп'ютер знаходиться в змозі зробити. Це комплекс заходів, правильність роботи і розрахованих результатів, тобто характеризує зручність; другий клас описує, наскільки стабільним і послідовним являється комп'ютер під час експлуатації. Це відноситься до надійності роботи в самому широкому сенсі; третій клас відноситься до швидкості роботи. Одним з найважливіших аспектів є швидкість виконання завдань, тобто час для доставки результатів завдань. Іншим аспектом є ряд завдань, які можуть виконуватися в даний момент часу [5].

Вирішення поставленої задачі

Під поняттям гомоморфного шифрування буде надалі розуміти модель шифрування, яка дозволяє виконувати математичні дії з зашифрованим текстом і отримувати зашифрований результат, який відповідає результату аналогічної операції, що проводиться з відкритим текстом. Безперечно, сам факт можливості здійснення таких операцій являється основною перевагою алгоритмів і виділяє їх серед інших алгоритмів шифрування/дешифрування [1, 3, 4].

Проаналізувавши криптографічні алгоритми, можна стверджувати, що найбільш ефективними, надійними і найчастіше використовуваними алгоритмами гомоморфного шифрування є алгоритм RSA, що належить до класу частково гомоморфних криптографічних систем, та алгоритм Гентрі, який є єдиним представником класу повністю гомоморфних криптографічних систем. Проведений аналіз дозволяє стверджувати, що якщо брати до уваги показник швидкодії алгоритму, а саме швидкість виконання операцій шифрування/дешифрування інформації, алгоритм Гентрі має переваги в порівнянні з алгоритмом RSA, проте значно поступається по показникам криптостійкості. Це пояснюється тим, що в алгоритмі RSA в відкритому ключі показник N являється добутком взаємно простих чисел n та q. При цьому в надійній системі шифрування вони мають мати довжину не менше 512 біт кожний. Окрім цього, в алгоритмі RSA складність математичних операцій в процедурах шифрування та дешифрування значно вища (обчислення числа по модулю N, піднесення до степеня m^e,), також для генерації секретного ключа d необхідно реалізувати алгоритм Евкліда. Вся ця сукупність операцій потребує значних обчислювальних ресурсів. Що стосується алгоритму Гентрі, то в ході шифрування/дешифрування інформації використовуються тільки операції додавання та множення, при цьому

секретний ключ алгоритму обчислюється як $p=2K+1$, де K – довільне число і математична складність генерації такого ключа набагато менша. При цьому, криптоаналітику, який хоче розшифрувати криптограму, для знаходження ключа шифрування необхідно лише підібрати число K (так як за умовою алгоритму, ключ шифрування – непарне число), а ця задача легко реалізується в випадку, якщо число K погано підібране [8 – 10].

Також проведений аналіз дозволив визначити подальші шляхи удосконалення алгоритму Гентрі на базі підвищенням показників криптостійкості за рахунок введення додаткового шифрування сеансового ключа асиметричним алгоритмом RSA та використання генератора простих чисел, на основі чого отримано гібридну систему шифрування, що поєднує властивості та переваги симетричної та асиметричної системи, описано процедуру шифрування та дешифрування інформації за допомогою розробленої криптографічної системи. 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, так як для криптоаналізу та розшифрування ключа зловмиснику необхідно буде вирішити задачу розкладу параметра N на прості співмножники p та q, а при вдалому підборі цих параметрів (не менше 512 біт) таку задачу вирішити практично неможливо за сучасних умов. Математичні основи удосконаленого алгоритму Гентрі представлено в [2, 5, 7].

Оцінка продуктивності розроблених програмних реалізацій алгоритмів гомоморфного шифрування/дешифрування було зведено до визначення часу виконання програмою функцій шифрування/дешифрування, генерації ключів та визначення факторів, які впливають на дані показники з метою визначення «слабких місць» програми та алгоритму. Тобто було визначено показники швидкодії алгоритму. Дана процедура буде виконана в декілька етапів. Обов'язковою умовою для цього є проведення експериментального дослідження, що полягає в визначенні часу виконання програмних функцій при зміні факторів, що впливають на продуктивність програмної реалізації.

Спосіб оцінки продуктивності програмного забезпечення, визначений у стандарті ДСТУ ISO / IEC 14756, заснований на принципі, згідно якого оцінювана система розглядається як «чорний ящик». Система складається з обладнання, програмного забезпечення і мережевих компонентів. Цей набір розглядається як чорний ящик, який з'єднаний через набір його інтерфейсів для своїх користувачів. Користувачами зазвичай є люди або машини, які подають завдання до системи через інтерфейс.

Пов'язуючи цей пункт до програмних реалізацій, які підлягають оцінці, можна стверджувати, що програмний засіб є системою обробки даних з апріорно невідомими показниками якості та продуктивності. Оцінювана система складається з обладнання (персонального комп'ютера, на якому

встановлена програма), безпосередньо програмного забезпечення, і користувачів.

Результати визначення продуктивності, незалежно від того, робиться це за допомогою методу вимірювання або методом прогнозування, є значення експлуатаційних показників, тобто фізичні величини. Загальна оцінка не є числовими значеннями, ("погано", "достатньо" або "надмірне"). Повинно бути визначено, які діапазони значень продуктивності відповідають кожному з цих трьох числових значень.

Продуктивність P визначимо як сукупність наступних показників: $P = (B, TME, E)$, де B – пропускний вектор, TME – середній час виконання вектора B, E – вектором регресії.

Розглянемо поетапно процедуру оцінки продуктивності.

1 етап. Визначення пропускного вектора B. На цьому етапі визначається кількість типів завдань, які виконуються програмною реалізацією. Формула (1) являється формулою для обчислення загального пропускного вектора.

$$B(M) = \sum_{i=1}^{M} \frac{B(M_i)}{T(R)}; , \tag{1}$$

де $T(R)$ – час відведений на експеримент, $B(M_i)$ – час виконання кожної функції.

Для обчислення пропускного вектора проведено експеримент, що полягав у визначенні часу роботи кожної функції. При цьому час, відведений на проведення експерименту задається апріорно (120 с).

2 етап. Визначення T (середнього часу виконання вектора B). Цей параметр показує співвідношення часу, який було витрачено для виконання всіх функцій програми за замовчуванням і часу, який задано апріорно для виконання всіх функцій. При проведенні експерименту було вибрано значення 120 с, так як цього часу цілком вистачає інформаційному обладнанню з середніми параметрами продуктивності для виконання всіх функцій програми незалежно від вибраних параметрів алгоритмів шифрування (див. формулу 2).

$$T(M) = \frac{\sum_{i=1}^{M} M_i}{T(R)}; , \tag{2}$$

3 етап. Визначення коефіцієнтів регресії E. На цьому етапі визначено, які ключові фактори впливають на продуктивність програми і проведено ряд експериментів, змінюючи вплив цих факторів на продуктивність програмних реалізацій. Наведемо фактори, що впливають на продуктивність програм.

Далі вибрано верхній і нижній рівень для кожного фактора. При цьому

використовуються наступні позначення: +1 відповідає верхньому рівню фактора; - 1 відповідає нижньому рівню фактора.

Таблиця 1

Зведені характеристики програмних реалізацій класичного та удосконаленого алгоритму Гентрі

Характеристика програмного забезпечення	Програмна реалізація класичного алгоритму Гентрі	Програмна реалізація удосконаленого алгоритму Гентрі
Кількість функцій, які виконую–ться програм–ними забез–печенням	M1 – функція шифрування M2 – функція дешифрування M3 – функція додавання відкритого тексту M4 – функція множення відкритого тексту M5 – функція додавання закритого тексту M6 – функція множення закритого тексту M7 – генерація ключа	M1 – генерація ключа M2 – шифрування ключа M3 – функція додавання відкритого тексту M4 – функція множення відкритого тексту M5 – функція шифрування M6 – функція додавання шифрованого тексту M7 – функція множення шифрованого тексту M8 – дешифрування ключа M9 – функція дешифрування
Кількість факторів, що впливають на продуктивність програмного забезпечення	X1 – Довжина відкритого тексту X2 – Шифрування суми X3 – Довжина ключа X4 – Шифрування добутку X5 – Дешифрування криптотексту без проведення математичних операцій	X1 – Довжина відкритого тексту X2 – Шифрування суми X3 – Довжина ключа RSA, що застосовується при шифруванні сеансового ключа Гентрі X4 – Шифрування добутку X5 – Значення параметра *e*

Рівні факторів визначаються за тим, наскільки впливає вибір того чи іншого параметра на швидкість та продуктивність виконання програмних функцій. Верхній рівень фактору означає використання більш надійних засобів, які забезпечують криптостійкість алгоритму, при цьому швидкість виконання програмних функцій буде більша, і навпаки, нижчий рівень – забезпечує більшу швидкодію, проте з їх використанням зменшується криптостійкість та надійність програми. Наступним етапом було проведення

експерименту (32 експерименти), що полягали в вимірюванні швидкості виконання (в секундах) програмою функцій шифрування та дешифрування, при цьому в кожному новому експерименті відбувається заміна одного з факторів з верхнього рівня на нижній (комбінуються фактори).

Коефіцієнти рівня регресії були найдені за наступною формулою:

$$K_j = \frac{\sum_{i=1}^{N} X_{ji} Y_j}{N};, \qquad (3)$$

де N – кількість експериментів, i – номер фактору, Y – час виконання програмних функцій, j – номер експерименту.

Рейтинг виміряних значень продуктивності

Виміряна продуктивність *P = (B , TME , E)* являє собою набір фізичних величин. Користувач системи зацікавлений , чи задовольняють вони вимогам користувача в повному обсязі. Після виміряних значень продуктивності можна зробити висновок про те, наскільки дані показники влаштовують користувача системи, з отриманих значень коефіцієнтів можна визначити, які з них мають найбільший вплив на продуктивність програми, яким чином можна збільшити чи зменшити вплив тих чи інших коефіцієнтів на продуктивність. При виконанні експериментальних досліджень в роботі результати визначення продуктивності програмного засобу можуть вказати на «слабкі місця» програми чи криптографічного алгоритму, що реалізований в програмному вигляді. При цьому модернізація даних недоліків приведе до покращення показників продуктивності і ефективності програмного засобу.

При виконанні роботи було використано механізм оцінки продуктивності програмних засобів та криптографічних алгоритмів, що в них реалізовані та враховане наступне:

1. Для оцінки продуктивності програмного забезпечення згідно ДСТУ ISO 14756:2010 розраховувалися наступні параметри продуктивності: загальна пропускна спроможність (пропускний вектор); середній час виконання завдань; коефіцієнти регресії.

2. Для оцінки продуктивності були визначені всі функції, які реалізує програма і фактори, які є найбільш впливовими на продуктивність програмного забезпечення.

3. Розрахувавши коефіцієнти регресії, можна в подальшому стверджувати, які з визначених факторів є найбільш впливовими на продуктивність програмного забезпечення і на основі даних обчислень будуть модернізовані алгоритми таким чином, щоб покращити показники швидкості виконання криптографічних функцій та алгоритмів.

Таблиця 2

Порівняльна характеристика алгоритмів після проведених досліджень за показниками продуктивності

Параметр	RSA	Ель-Гамаля	Гентрі	Удосконалений алгоритм Гентрі
Характеристика гомоморфності	Часткова	Часткова	Повна	Повна
Кількість виконуваних програмою функцій	7	8	7	9
Загальний пропускний вектор $B(M)$	0,6193	0,5768	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%	20,57%	25,1%	15,1%
Середній час виконання програмних функцій за всі експерименти	4,69 с	4,35 с	5,25 с	4,01 с
Фактор,який найбільш впливає на швидкість виконання програмних функцій	Довжина ключа	Довжина ключа	Довжина ключа	Значення параметра e
Фактор,який найменше впливає на швидкість виконання програмних функцій	Тип криптопровайдера	Тип криптопровайдера	Наявність хеш-функції	Шифрування суми

Висновки

В даному дослідженні була проведена оцінка продуктивності програм та реалізації алгоритмів гомоморфного шифрування для забезпечення цілісності

та конфіденційності інформації в сучасних системах та мережах. Всі етапи визначення продуктивності програми та виміру швидкості виконання програмних функцій сформовані на базі стандарту ДСТУ ISO 14756:2010. На основі використання даного стандарту проведено відповідні дослідження та зроблені висновки щодо переваг та слабких місць кожного з запропонованих алгоритмів. Основними показниками оцінки продуктивності інформаційної системи представлені показники швидкості виконання операцій, зв'язаних з шифруванням/ дешифрування інформації.

1. *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.
2. *Kazmirchuk S., Ilyenko A, Ilyenko I.* Digital signature authentication scheme with message recovery based on the use of elliptic curves. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds.) ICCSEEA 2019. AISC, vol. 938, pp. 279–288. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16621-2_26.
3. *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.
4. *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.
5. ДСТУ ISO/IEC 14756:2010. Інформаційні технології. Вимірювання та рейтингове оцінювання продуктивності комп'ютерних програмних систем. – К. : Держстандарт України, 2010. – 45 с.
6. *Ільєнко А.В.* Оцінка ефективності оптимізованої криптосистеми Гентрі з умови забезпечення конфіденційності інформації / А.В. Ільєнко// Наукоємні технології. – № 1 (33). – 2017. – С.41-45, doi.org/10.18372/2310-5461.33.11557.
7. *Ільєнко А.В*. Сучасні шляхи удосконалення процедури формування та верифікації електронно-цифрового підпису / А.В. Ільєнко, Г.О. Миронова // Наукоємні технології. – № 1 (37). – 2018. – С.61-66, doi.org/10.18372/2310-5461.37.12370.
8. *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
9. *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.
10. *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.

http://doi.org/10.5281/zenodo.3612244

Поступила 5.09.2019р.