УДК 519.6
DOI: 10.32626/2308-5916.2019-19.145-150

І. З. Якименко, канд. техн. наук,
М. М. Касянчук, канд. фіз.-мат. наук,
С. В. Івасьєв, канд. техн. наук
Тернопільський національний економічний університет, м. Тернопіль

КРИПТОСИСТЕМА РАБІНА НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ

У роботі наведено теоретичні основи криптосистеми Рабіна з використанням тільки операції додавання, завдяки чому досягається зменшення часової складності процесу шифрування / дешифрування інформаційних потоків. Запропонований підхід дозволяє збільшувати розмірності вхідних параметрів для підвищення стійкості без втрати швидкодії. Представлено приклад застосування запропонованої реалізації криптосистеми Рабіна.

Ключові слова: *криптосистема Рабіна, векторно-модульний метод модулярного множення, квадратичний лишок, операція додавання, часова складність.*

Вступ. На сьогоднішній день криптосистема Рабіна є однією з найбільш ефективних [1], оскільки для шифрування потрібна лише операція піднесення до квадрату за модулем, а не модулярне експоненціювання, як в асиметричних криптосистемах RSA та Ель-Гамаля [2]. Крім того, її стійкість ґрунтується на проблемі факторизації [3, 4] та пошуку квадратичного лишку [5]. Дана операція має субекспоненційну складність [6], тому для забезпечення достатньої стійкості при сьогоднішніх обчислювальних потужностях розрядність числових полів повинна бути більшою 1024 біт [7].

Поряд з перевагами, існує ряд недоліків, найголовніший з яких стосується процесу розшифрування з використанням китайської теореми про залишки, який характеризується значною часовою складністю при виконанні базових операцій [8, 9]. Інший недолік — це певні обмеження до вхідних параметрів, які повинні задовольняти рівність $p \bmod 4 = q \bmod 4 = 3$ для спрощення пошуку квадратичного лишку при дешифруванні. Крім того, в класичній криптосистемі Рабіна застосовується позиційна система числення, що у зв'язку із використанням багаторозрядних чисел призводить до зменшення швидкодії процесу шифрування/дешифрування та збільшення часової складності. Тому постає актуальна задача реалізації криптосистеми Рабіна на основі нових підходів, які дозволяють зменшити часову складність процесу шифрування/дешифрування шляхом заміни обчислювально складних арифметичних операцій операцією додавання.

Класична криптосистема Рабіна. Для генерування ключів у криптосистемі Рабіна вибираються два випадкових багаторозрядних

простих числа p і q. Шукається їх добуток $n = p \cdot q$, де число n є відкритим ключем, числа p і q — закритим.

Процес шифрування повідомлення M (текст) відбувається згідно такого виразу:

$$C = M^2 \bmod n. \tag{1}$$

При дешифруванні криптограми C вводяться додаткові допоміжні величини f і s:

$$f = C \bmod p;\ s = C \bmod q. \tag{2}$$

Для знаходження M необхідно знайти квадратичні лишки за модулями p і q:

$$x^2 \bmod p = f, \tag{3}$$

$$y^2 \bmod q = s. \tag{4}$$

В результаті отримуємо чотири системи порівнянь:

$$\begin{cases} M_1 \bmod p = x; \\ M_1 \bmod q = y; \end{cases} \quad \begin{cases} M_2 \bmod p = x; \\ M_2 \bmod q = -y; \end{cases}$$
$$\begin{cases} M_3 \bmod p = -x; \\ M_3 \bmod q = y; \end{cases} \quad \begin{cases} M_4 \bmod p = -x; \\ M_4 \bmod q = -y. \end{cases} \tag{5}$$

Одне з рішень (5) буде шуканим повідомленням M.

Слід зазначити, що для пошуку усіх розв'язків (5) достатньо знайти тільки два з них, наприклад M_1 та M_2. Тоді інші розв'язки шукаються з виразу $M_{3,4} = n - M_{1,2}$.

Однак використання класичних підходів при виконанні арифметичних операцій для шифрування/дешифрування на основі криптосистеми Рабіна характеризується великою часовою складністю. Тому у даній роботі пропонується реалізація криптосистеми Рабіна з використанням тільки операції додавання.

Криптосистема Рабіна на основі операції додавання. Для зменшення часової складності криптосистеми Рабіна при генерації ключів та шифруванні запропоновано використати векторно-модульний метод [10]. Одне з вибраних чисел p і q (наприклад, p) записується в двійковій формі: $p = \sum_{i=0}^{k-1} p_i \cdot 2^i$, де k — його розрядність, $p_i = 0$ або1. Далі будується вектор-рядок $q_i = 2 \cdot q_{i-1} = 2^i q_0 = q$ (табл. 1).

Таблиця 1

Представлення вектор-рядків для множення

i	$k-1$	…	2	1	0
p_i	p_{k-1}	…	p_2	p_1	p_0
$q_i = 2 \cdot q_{i-1}$	q_{k-1}	…	q_2	q_1	$q_0 = q$

Результат множення $n = p \cdot q$ знаходиться згідно такої формули:

$$n = p \cdot q = \sum_{i=0}^{k-1} p_i \cdot q_i . \qquad (6)$$

Отже, операція множення замінюється операцією додавання тих q_i, для яких відповідні $p_i = 1$.

Аналогічно будується табл. 2 для шифрування. Число M записується в двійковій формі $M = \sum_{i=0}^{k-1} d_i \cdot 2^i$ ($d_i = 0$ або 1) і формується вектор-рядок $m_i = 2 \cdot m_{i-1} \bmod n$, $m_0 = M$.

Таблиця 2

Представлення вектор-рядків для множення за модулем

i	$k-1$	…	2	1	0
d_i	d_{k-1}	…	d_2	d_1	d_0
$m_i = 2 \cdot m_{i-1} \bmod n$	m_{k-1}	…	m_2	m_1	$m_0 = M$

Результат шифрування знаходиться згідно формули:

$$C = M^2 \bmod n = \left(\sum_{i=0}^{k-1} d_i \cdot m_i \right) \bmod n. \qquad (7)$$

Відповідно, операція множення за модулем замінюється операцією модулярного додавання тих m_i, для яких відповідні d_i дорівнюють 1.

В порівнянні з класичним підходом, даний метод характеризується меншою часовою складністю [11].

Для знаходження x і y в (3), (4) необхідно обчислити значення кореня квадратного за модулем. Класичні підходи з використання символів Якобі або Лежандра є трудомісткими [12]. Тому пропонується метод, який вимагає тільки операції додавання та перевірки, чи є число повним квадратом, що суттєво зменшує часову складову методу Рабіна. Отже, для того, щоб знайти значення $x \bmod p = \sqrt{f}$, необхідно виконати наступну послідовність дій: $f + p$, $f + 2p$, … , $f + i \cdot p$, де i — значення, при якому число $f + i \cdot p$ буде повним квадратом. Аналогічним чином шукається $y^2 \bmod q = s$.

Для розв'язку систем (5) також пропонується використати метод додавання модуля. Для прикладу розглянемо першу систему порівнянь (5). Оскільки будь-яку конгруенцію $M_1 \bmod p = x$ можна представити у вигляді $M_1 = \lambda p + x$, де $\lambda = 0, 1, 2, \ldots$, то до залишку x потрібно додавати модуль p стільки разів, поки не буде виконуватись конгруенція $(x + \lambda p) \bmod q = M_1 \bmod q = y$.

Слід відмітити, що в класичних методах (китайській теоремі про залишки та алгоритмі Гарнера) необхідно шукати обернений елемент за модулем [13, 14], що супроводжується великою обчислювальною складністю і, відповідно, призводить до погіршення часових характеристик при реалізації криптоалгоритму Рабіна.

Приклад використання запропонованих методів. Нехай таємні ключі p = 47, q = 31, тоді згідно (6) і табл. 1 отримується: $n = p \cdot q = 31 \cdot 47 =$ 992 + 248 + 124 + 62 + 31 = 1457 (табл. 3).

Таблиця 3

Пошук добутку $n = p \cdot q = 31 \cdot 47$

i	5	4	3	2	1	0
p_i	1	0	1	1	1	1
$q_i = 2 \cdot q_{i-1}$	992	496	248	124	62	31

Нехай відкритий текст M = 118. На основі формул (1), (7) та таблиці 2 формується табл. 4.

Таблиця 4

Процедура шифрування

i	6	5	4	3	2	1	0
d_i	1	1	1	0	1	1	0
$m_i = 2 \cdot m_{i-1} \bmod n$	267	862	431	944	472	236	118

Звідси отримується значення шифртексту: $C \equiv 118^2 \bmod 1457 =$ = (267 + 862 + 431 + 472 + 236) mod 1457 = 811, тобто операція модулярного множення замінюється операцією додавання за модулем.

При дешифруванні криптограми C використовуються вирази (2)–(4): f = 811 mod 47 = 12, s = 811 mod 31 = 5. Далі формуються послідовності, в яких шукається повний квадрат:

12, 12+47 = 59, 59+47 = 106, 106+47 = 153, 153+47 = 200,
200+47 = 247, 247+47 = 294, 294+47 = 341, 341+47 = 388,

388+47 = 435, 435+47 = 482, 482+47 = 529, $\sqrt{12} (\bmod 47) \equiv 23$ та 24;

5, 5+31=36, $\sqrt{5} (\bmod 31) \equiv 6$ та $31 - 6 = 25$.

Отже, потрібно розглянути чотири системи конгруенцій:

$$\begin{cases} M_1 \bmod 47 = 23; \\ M_1 \bmod 31 = 25; \end{cases} \quad \begin{cases} M_2 \bmod 47 = 24; \\ M_2 \bmod 31 = 25; \end{cases}$$

$$\begin{cases} M_3 \bmod 47 = 23; \\ M_3 \bmod 31 = 6; \end{cases} \quad \begin{cases} M_4 \bmod 47 = 24; \\ M_4 \bmod 31 = 6. \end{cases} \qquad (8)$$

Розв'язок перших двох з них зручно представити у вигляді табл. 5.

Таблиця 5

Процедура дешифрування

λ	0	1	2	3	4
Перша система					
$23+47\cdot\lambda$	23	70	117	164	211
$(23+47\cdot\lambda)$ mod 31	23	8	24	9	25
Друга система					
$24+47\cdot\lambda$	24	71	118		
$(24+47\cdot\lambda)$ mod 31	24	9	25		

Отже, розв'язками (8) є значення $M_1 = 211$, $M_2 = 118$ (відкритий текст), $M_3 = 1457 - 211 = 1246$, $M_4 = 1457 - 118 = 1339$, які отримані без використання громіздких операцій та необхідності контролю переповнення розрядної сітки при виконанні проміжних обчислень.

Висновки. У роботі наведено теоретичні основи для реалізації криптоалгоритму Рабіна за допомогою використання тільки операції додавання. Це дозволяє збільшити швидкодію процесу шифрування/дешифрування інформаційних потоків шляхом уникнення виконання обчислювально громіздких операцій (множення, пошуку квадратного кореня за модулем, пошуку оберненого елемента тощо). Застосування такого підходу дозволяє будувати надійні та ефективні системи захисту за рахунок збільшення розмірності вхідних параметрів (розміру повідомлення, ключа), що призводить до підвищення стійкості та зменшення часової складності криптосистеми Рабіна.

Список використаних джерел:

1. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 2003. 780 p.
2. Arpit K., Mathur A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem. *Int. J. Sci. Res. Public*. 2013. Vol. 3. P. 1–4.
3. Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. *Proc. of 16th International Conference on Control, Automation and Systems* (ICCAS–2016). Gyeongju, Korea. Vol. 1. October, 2016. P. 1484–1486.
4. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The Method of Factorizing Multi-Digit Numbers Based on the Operation of Adding Odd Numbers. *Proceedings of the conference «Advanced Computer Information Technology* (ACIT 2018)» (Ceske Budejovice, Czech Republic). P. 232–235.
5. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. Тернопіль ; Київ, 2002. 504 с.
6. Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. McGraw-Hill Science, Engineering, 2006. 336 p.

7. Королев М. Е., Лапина Н. А. Сравнение производительности алгоритмов формирования электронной цифровой подписи. *Проблемы современной науки и образования.* 2017. С. 13—18.
8. Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S., Rabin's modified method of encryption using various forms of system of residual classes. *Proceedings of the XIV International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics* (CADSM-2017)». Polyana-Svalyava (Zakarpattya), Ukraine. 2017. P. 222–224.
9. Касянчук М. М., Якименко І. З., Івасьєв С. В., Мандебура Н. М., Неміш В. М. Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем. *Вісник Хмельницького національного університету.* Технічні науки. 2017. № 6 (255). С. 191–197.
10. Kozaczko D., Kasianchuk M., Yakymenko I., Ivasiev S. Vector Module Exponential in the Remaining Classes System. *Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS–2015). Warsaw, Poland. 2015. Vol. 1. P. 161–163.
11. Yakymenko I. Z., Kasianchuk M. M., Ivasiev S. V., Melnyk A. M., Nykolaichuk Y. M. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *Proceedings of the 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (TCSET-2018). 2018. P. 550–554.
12. Івасьєв С.В., Якименко І.З. Касянчук М. М. Вдосконалений алгоритм пошуку символів Якобі. *Методи та системи оптико-електронної і цифрової обробки зображень та сигналів.* 2015. Том 29, № 1. С. 45–50.
13. *Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M.* Research of Time Characteris-tics of Search Methods of Inverse Element by the Module. *Proceedings of the 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS–2017). 2017. Vol. 1. P. 82–85.
14. Касянчук М. М., Якименко І. З., Івасьєв С. В., Момотюк О. В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. *Інформатика та математичні методи в моделюванні.* 2017. Т. 7, № 3. С. 178–186.

RABIN'S CRYPTO SYSTEM ON THE BASIS OF THE ADDITION OPERATION

The paper presents the theoretical backgrounds of the Rabin's cryptosystem using only on the addition operation in virtue of reducing the time complexity of the encryption / decryption process of information flows. The proposed approach allows to increase the dimension of the input parameters to improve stability without loss of performance. An example of application of the proposed implementation of Rabin's cryptosystem is presented.

Key words: *cryptosystem Rabin, vector-modular method of modular multiplication, quadratic residue, add-on operation, time complexity.*

Одержано 04.02.2019