DOI 10.15276/imms.v11.no1-2.16
УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 1-2, pp. 16-26

РОЗРОБКА ТРЬОХМОДУЛЬНОЇ КРИПТОСИСТЕМИ РАБІНА НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ

Касянчук М.М., Лотоцький О.Я., Яцків С.В., Івасьєв С.В., Тимошенко Л.М.[1]

Західноукраїнський національний університет, вул. Львівська, 11, м.Тернопіль, 46020; E-mail: kasyanchuk@ukr.net, lmt0902@gmail.com, jazkiv@ukr.net, stepan.ivasiev@gmail.com
[1]Державний університет «Одеська політехніка», пр.Шевченка, 1,Одеса, 65044.
lmt0902@gmail.com

Сьогодні одним з найпоширеніших алгоритмів асиметричної криптографії є криптосистема Рабіна. Процес шифрування у ній подібний до криптосистеми RSA, однак замість модулярного експоненціювання використовується операція піднесення до квадрату за модулем. Це забезпечує більшу порівняно з RSAшвидкодію алгоритму шифрування без втрати криптостійкості. Однак процес розшифрування вимагає значних обчислювальних та апаратних затрат. Тому метою даної роботи є розробка трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання, а також дослідження її обчислювальної складності. Для виконання операції модулярного множення пропонується використати векторно-модульний метод, в якому множення замінюється операцією додавання відповідних величин. Для пошуку квадратичного лишку та відновлення десяткового числа за його залишками замість використання відповідно символів Якобі або Лежандра та китайської теореми про залишки використовуються методи додавання модуля та додавання добутку модулів. Це дозволяє зменшити обчислювальні складності вказаних операцій. Наведено схему трьохмодульної криптосистеми Рабіна та приклад її реалізації з використанням тільки операції додавання. Використання в даному підході однотипних суматорів замість мультиплексорів та перемножувачів дасть можливість зменшити апаратну та структурну складність схемотехнічного проектування трьохмодульної криптосистеми Рабіна. Для порівняння обчислювальної складності різних реалізацій криптосистеми Рабіна розглянуто її найбільш трудомісткі операції. Проведені дослідження свідчать про те, що реалізація трьохмодульного криптоалгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Представлено графічну залежність обчислювальної складності від розрядності чисел та кількості модулів. Показано, що із збільшенням цих аргументів обчислювальна складність реалізації криптосистеми Рабіна істотно зростає.

Ключові слова: трьохмодульна криптосистема Рабіна, додавання, векторно-модульний метод, обчислювальна складність, квадратичний лишок, китайська теорема про залишки.

Вступ

Використання засобів асиметричної криптографії набуває все більшого поширення в різного роду інформаційних системах [1].З одного боку, це пов'язано з потребою суб'єктів системи у надійному механізмі забезпечення автентичності даних, які передаються, а з іншого - з тим, що сучасні криптографічні методи мають високий ступінь стійкості до криптоаналізу, що дозволяє суб'єктам системи бути абсолютно впевненими в їх надійності [2].

Однак найбільш поширені асиметричні криптосистеми Ель-Гамаля, RSA, Рабіна [3] мають низьку продуктивність процесів шифрування/дешифрування інформації, оскільки їх математична реалізація ґрунтується на складних обчисленнях, що вимагають величезних витрат машинного часу і ресурсів. Крім того, для забезпечення достатнього рівня захисту інформації ставляться жорсткі вимоги до вхідних параметрів, які повинні бути не меншими 2048 біт. В результаті цього асиметричні

криптосистеми переважно використовуються для обміну криптографічними ключами і цифрового підпису.

Можливим рішенням проблеми низької продуктивності процесів шифрування/дешифрування інформації може бути створення асиметричних криптосистем на основі непозиційних систем числення [4], атакож використання векторно-модульного методу привиконанні модулярних операцій множенняіпіднесення до степеня [5]. Найбільш перспективною для цього є система залишкових класів (зокрема, її досконала [6]і модифікована досконала [7] форми), яка дозволяє зменшити обчислювальну складність [8] на основі розпаралелення процесу обчислень,і виконання арифметичних операцій за допомогою векторно-модульного методу.

Аналіз досліджень та публікацій

Аналіз наукових досліджень показує [9, 10], що асиметрична криптосистема Рабіна, у якій процес шифрування подібний до RSA(замість експоненціювання використовується піднесення до квадрату), забезпечує більшупорівняно з RSAшвидкодію алгоритму без втрати криптостійкості. Однак процес дешифрування вимагає значних обчислювальних та апаратних затрат у зв'язку з наявністю складних операцій пошуку квадратного кореня за модулем та відновлення десяткового числа за його залишками, який відбувається, як правило, на основі китайської теореми про залишки (КТЗ) [11].

Тому задача зменшення обчислювальної складності процесів шифрування/дешифрування інформаційних потоків у криптоалгоритмі Рабіна з використанням лише обчислювально простої операції додавання є надзвичайно актуальною[12].

Криптосистема Рабіна ґрунтується на складності факторизації та пошуку квадратичного лишку [13, 14]. Починається схема шифрування із генерації відкритого і таємного ключів.Для цього вибирають два простих великих числа p та q, які задовольняють умовам $p \equiv q \equiv 3 \bmod 4$. Це суттєво спрощує і прискорює пошук квадратних коренів за модулями pтаq. Потім обчислюють значення $N=p\cdot q$. Число Nвиступає відкритим ключем, а p та q - закритим.

Шифрування відкритого повідомлення M відбувається за формулою

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

При дешифруванні шифртексту C вводять додаткові допоміжні величини v і m:

$$v=C\bmod p; \quad m=C\bmod q. \tag{2}$$

Для відновлення M потрібно знайти квадратичні лишки v таm відповідно за модулями p та q:

$$x^2 \equiv v(\bmod\ p), \tag{3}$$

$$y^2 \equiv m(\bmod\ q), \tag{4}$$

У результаті утворюються чотири системи порівнянь (i=1…4):

$$\begin{cases} M_i \equiv \pm x(\bmod\ p); \\ M_i \equiv \pm y(\bmod\ q). \end{cases} \tag{5}$$

Один з розв'язків (5), пошук якого здійснюється на основі КТЗ[15], і буде відкритим повідомленням M .

Аналіз літературних джерел дозволив виявити недоліки класичної криптосистеми Рабіна. Зокрема, у [16] авторам вдалося досягнути більшої криптостійкості без збільшення обчислювальної складності шляхом заміни квадратичної конгруенції на кубічне рівняння.

В [17] зазначено переваги використання гаусівських цілих чисел для генерації відкритого ключа криптосистеми Рабіна. Це дозволило розробити відповідну арифметику для теореми Вільсона і КТЗ, а також для обчислення символів Лежандра і квадратичних залишків.

У [10, 18] розглянуто трьох модульну криптосистему Рабіна (або H-Rabin), стійкість якої базується на розкладі добутку трьох чисел $N=pqr$ де p, q та r - прості числа. Це дозволяє збільшити величину блоку відкритого тексту без втрати криптостійкості, що забезпечує більшу захищеність криптосистеми від відповідних видів атак.Крім того, обґрунтовано використання модифікованої досконалої форми системи залишкових класів у криптосистемі Рабіна.

Однак у зазначених удосконаленнях використовуються обчислювально громіздкі медулярні операції множення багаторозрядних чисел, піднесення до квадрату, пошуку квадратичного залишку та оберненого елемента тощо.

Мета і задачі дослідження

Отже, метою даної роботи є розробка трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання, а також дослідження її обчислювальної складності.

Для досягнення поставленої мети потрібно вирішити такі задачі:

- проаналізувати обчислювальні складності основних операцій трьохмодульної криптосистеми Рабіна;
- обґрунтувати використання векторно-модульного методу виконання модулярного множення;
- обґрунтувати використання методів додавання модуля та добутку модулів відповідно для пошуку квадратичного залишку та відновлення десяткового числа за його залишками;
- оцінити обчислювальну складність криптоалгоритмуРабіна на основі використання тільки операції додаваннята порівняти його з існуючими методами.

Основна частина

Трьохмодульна криптосистема Рабіна на основі операції додавання.

Для зменшення обчислювальної складності у трьохмодульній криптосистемі Рабіна[10, 18] при шифруванні пропонується використовувати векторно-модульний метод модулярного множення. При цьому на першому етапі вибирають три великих простих числа p, q та r і обчислюють значення $N= p\cdot q\cdot r$, де N - відкритий ключ, числа p, q та r– таємний.

Шифрування відкритого повідомлення M відбувається за допомогою числа N за формулою (1).

На основі векторно-модульного методу модулярного множення значення $M \cdot M \bmod N$ шукають таким чином.

Відкритий блок M представимо у двійковій формі: $M = \sum_{i=0}^{n-1} a_i \cdot 2^i$, де $a_i = 0,1$, $n-$ розрядність модуля. Далі будуємо два вектор-рядки. В першому запишемо елементиa_i, в другому - $h_0 = 2^0 M \bmod N$, $h_i = 2 \cdot h_{i-1} \bmod N$ (таблиця 1).

Таблиця 1.

Вектор-рядки для модулярного множення

i	n-1	…	2	1	0
a_i	a_{n-1}	…	a_2	a_1	a_0
$h_i = 2 \cdot h_{i-1} \bmod N$	h_{n-1}	…	h_2	h_1	$h_0 = 2^0 \cdot M \bmod N$

Результат модулярного множення $M \cdot M \bmod N$ шукаємо згідно формули:

$$C = M^2 \bmod N = \left(\sum_{i=0}^{n-1} a_i \cdot h_i \right) \bmod N . \quad (6)$$

Отже, модулярне множення замінюємо операцією додавання тих h_i, для яких відповідні a_i рівні 1. Порівняно з класичними,даний метод характеризується меншою обчислювальною складністю виконання операції модулярного множення.

При дешифруванні криптограми C, аналогічно (2), вводимо допоміжні додаткові величини s, w і u:

$$s = C \bmod p ; w = C \bmod q ; u = C \bmod r . \quad (7)$$

Відповідно до (3), значення x, y і z шукають з таких порівнянь:

$$x^2 \equiv s(\bmod p) , y^2 \equiv w(\bmod q) , z^2 \equiv u(\bmod r) . \quad (8)$$

Для пошуку x, y та z потрібно обчислити значення квадратного кореня за модулем. Класичні підходи із використання символів Якобі чи Лежандра є досить трудомісткими [19]. Тому доцільно використати метод, що вимагає операції додавання і перевірки, чи є число повним квадратом. Така процедура дозволяє суттєво зменшити обчислювальну складність криптосистеми Рабіна. Отже, для пошуку значення $\sqrt{s} \bmod p$ необхідно виконати таку послідовність дій: $s + p$, $s + 2p$, …, $s + i \cdot p$, де i - значення, при якому $s + i \cdot p$ буде повним квадратом. Аналогічно обчислимо $y^2 \equiv w(\bmod q)$, $z^2 \equiv u(\bmod r)$. Оскільки розв'язками порівнянь (6)-(8) буде 6 значень, то для пошуку M треба розв'язати вісім систем порівнянь, які утворюються комбінацієювсіх можливих варіантів параметрів x, y та z (i=1…8):

$$\begin{cases} M_i \equiv \pm x(\bmod\ p); \\ M_i \equiv \pm y(\bmod\ q); \\ M_i \equiv \pm z(\bmod\ r). \end{cases} \quad (9)$$

Шуканим повідомленням M буде одиніз розв'язків систем порівнянь (9). Для їхвирішення доцільно використати метод на основі додавання добутку модулів, який

дозволяє зменшити обчислювальну складність в порівнянні з класичним: використанням КТЗ та алгоритму Гарнера [20].

На рисунку 1 представлена схема трьохмодульної криптосистеми Рабіна.

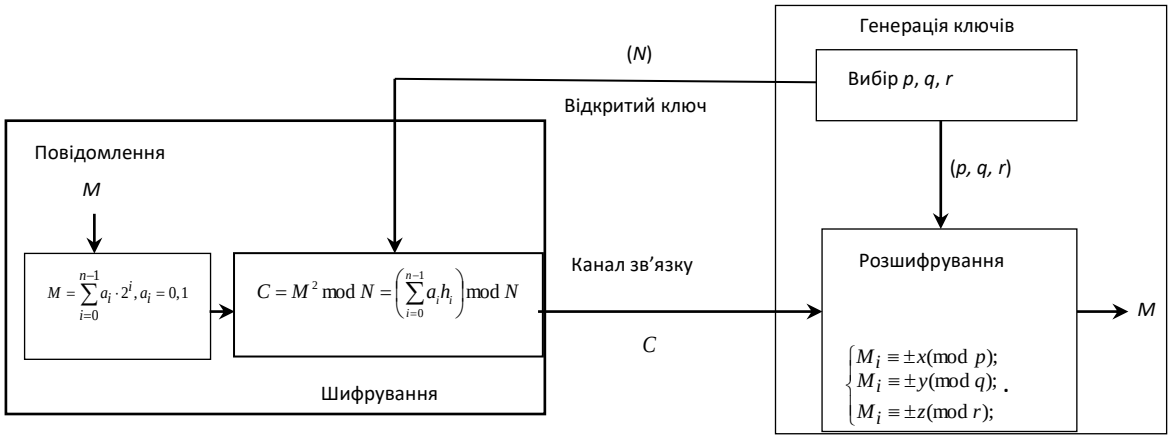

Рис. 1. Схема трьохмодульної криптосистеми Рабіна

Для прикладу розглянемо одну із систем порівнянь (9), в якій параметри *x*, *y*, *z* додатні. Оскільки будь-яку конгруенцію $x \bmod p = M_1$ можна представити у вигляді $x = \gamma p + M_1$, де γ = 0, 1, 2, …, то до залишку $M_1^{(1)} = x$ потрібно додавати модуль *p* стільки разів, доки не буде виконуватись конгруенція $M_1^2 \equiv y(\bmod q)$, де $M_1^{(2)} = M_1^{(1)} + \gamma_1 p$. Далі треба додавати добуток *pq*, доки не буде виконуватись конгруенція $M_1^{(3)} \equiv z(\bmod r)$, де $M_1^3 = M_1^2 + \gamma_2 pq = M_1$. Аналогічно знаходять розв'язки інших систем порівнянь (9).

Слід зазначити, що в КТЗ та алгоритмі Гарнера необхідно шукати мультиплікативний обернений елемент за модулем [21]. При використанні багаторозрядних чисел класичні методи (повним перебором усіх можливих варіантів, використання теореми Ейлера чиалгоритму Евкліда [22]) характеризуються великою обчислювальною складністю, що призводить до збільшення обчислювальних характеристик при реалізації крипто алгоритму Рабіна.

Приклад застосування розробленого методу

Нехай, наприклад,таємним ключем криптосистеми Рабіна буде три простих числа *p*=29, *q*=23 *і r* =17. Далі обчислюємо значення відкритого ключа: $N = p \cdot q \cdot r = 29 \cdot 23 \cdot 17 = 11339$.

У якості відкритого тексту для шифрування вибираємо повідомлення *M*=381. Тодіза формулою(1) на основі векторно-модульного методу модулярного множення обчислюємо значення $C = 381^2 \bmod 11339$.

Для цього повідомлення *M* записуємо в двійковій системі числення: $M = 381 = 101111101_2$. Далі здійснюємо побудову двох вектор-рядків. У першому вказуємо елементи a_i, які можуть дорівнювати 0 або 1, в другому - елементи $h_0 = 2^0 \cdot 381 \bmod 11339 = 381$, $h_1 = 2 \cdot 381 \bmod 11339 = 762$, $h_2 = 2 \cdot 762 \bmod 11339 = 1524$, $h_3 = 2 \cdot 1524 \bmod 11339 = 3048$, $h_4 = 2 \cdot 3048 \bmod 11339 = 6096$, $h_5 = 2 \cdot 6096 \bmod 11339 = 853$, $h_6 = 2 \cdot 853 \bmod 11339 = 1706$, $h_7 = 2 \cdot 1706 \bmod 11339 = 3412$, $h_8 = 2 \cdot 3412 \bmod 11339 = 6824$ (таблиця 2).

Таблиця 2

Вектор-рядкимодулярного множення381^2 mod11339

i	8	7	6	5	4	3	2	1	0
M_i	1	0	1	1	1	1	1	0	1
h_i	6824	3412	1706	853	6096	3048	1524	762	381

Результат модулярного множення $381 \cdot 381 \bmod 11339$ шукаємо за формулою (2):

$$C = 381^2 \bmod 11339 = (381+1524+3048+6096+853+1706+6824) \bmod 11339 = 9093.$$

Отже, модулярне множення замінюємо операцією модулярного додавання тих h_i, для яких відповідні a_i рівні 1.

При дешифруванні криптограми C, згідно (7), визначаємо допоміжні додаткові величини: $s = 9093 \bmod 29 = 16$; $w = 9093 \bmod 23 = 8$; $u = 9093 \bmod 17 = 15$.

Відповідно до (8), значення x, y і z обчислюємо з таких порівнянь: $x^2 \equiv 16 (\bmod 29)$, $y^2 \equiv 8 (\bmod 23)$, $z^2 \equiv 15 (\bmod 17)$.

Отже, значення $\sqrt{16} \bmod 29 = \pm 4$ (-4mod29=25). Щоб знайти $\sqrt{8} \bmod 23$ згідно вище описаного методу,потрібно виконати таку послідовність дій: $8, 8+23=31$, $31+23=54$, $54+23=77$, $77+23=100$. Оскільки 100 є повним квадратом, то $\sqrt{8} \bmod 23 = \pm 10$ (-10mod 23=13). Аналогічно відбувається пошук $z \equiv \sqrt{15} (\bmod 17) = \pm 7$ (-7mod 17=10). Відповідно до (9), для розшифрування треба розв'язати вісім систем порівнянь, які утворені комбінаціями всіх можливих варіантів x, y та z(i=1…8):

$$\begin{cases} M_i \equiv \pm 4 (\bmod 29); \\ M_i \equiv \pm 10 (\bmod 23); \\ M_i \equiv \pm 7 (\bmod 17). \end{cases} \quad (10)$$

Розв'язок однієї з восьми систем буде шуканим значенням M. Для зручності доцільно сформувати вісім трійок отриманих залишків: 1) (4, 10, 7); 2) (4, 10, 10);3) (4, 13, 7); 4) (4, 13, 10);5) (25, 10, 7); 6) (25, 10, 10);7) (25, 13, 7); 8) (25, 13, 10). У таблиці 3 продемонстровано процедуру розв'язку систем порівнянь у перших двох випадках, які відрізняються тільки останніми залишками. Видно, що вирішення першої системи отримуємо на п'ятій ітерації -M_1=1367. Після цього можна продовжити додавання добутку модулів $p \times q$=23·29=667 доки на десятій ітерації не буде справджуватися друга система: M_2=4702.Аналогічно будуємо таблицю4 для наступних двох систем конгруенцій.

Таблиця 3

Процедура розв'язку перших двох системконгруенцій, які відповідають трійкам (4, 10, 7); (4, 10, 10)

i	4+(i-1)×29	(4+(i-1)×29)mod23
1	4	4
2	33	10
$p \times q$=23·29=667		

	33+(*i*-3)×667	(33+(*i*-3)×667)mod17
3	33	16
4	700	3
5	1367	7
6	2034	11
7	2701	15
8	3368	2
9	4035	6
10	4702	10

Таблиця 4

Процедура розв'язку перших двох системконгруенцій, яківідповідаютьтрійкам(4, 13, 7); (4, 13, 10)

i	4+(*i*-1)×29	(4+(*i*-1)×29)mod23
1	4	4
2	33	10
3	62	16
4	91	22
5	120	5
6	149	11
7	178	17
8	207	0
9	236	6
10	265	12
11	294	18
12	323	1
13	352	7
14	381	13
p×*q*=23·29=667		
	381+(*i*-15)×667	(33+(*i*-15)×667)mod17
15	381	7
16	1048	11
17	1715	15
18	2382	2
19	3049	6
20	3716	10

Розв'язок третьої конгруенції одержимо на п'ятнадцятій ітерації – M_3=381, а четвертої – на двадцятій: M_4=3716.

Решту чотири розв'язки можна знайти як різницю відкритого ключа *N*і знайдених розв'язків: M_5=11339-1367=9972, M_6=11339-4702=6637, M_7=11339-381=10958, M_8=11339-3716=7623.

Отже, розв'язок M_3=381 відповідає відкритому тексту, всі інші розв'язки не будуть відповідати правильному випадку шифруваннявідкритого тексту.

Порівняння обчислювальних складностейкриптоалгоритмуРабіна на основівекторно-модульного та класичного методів

Для порівняння обчислювальної складності різних реалізаційкриптосистеми Рабіна необхідно розглянути найбільш трудомісткі операції,до яких відносятьмодулярнемноження, пошук квадратичного лишка та відновлення числа за його залишкамиз використаннямкитайської теореми про залишки в класичному методі і додавання модулів або добутку модулів у запропонованому підході.

Обчислювальна складність операції модулярногомноженнявекторно-модульним методом, в якому операція множеннязамінюється операцією додавання, характеризується лінійно-логарифмічною залежністю $O\left(\frac{n}{2}\log n\right)$.

З врахуванням того, що в запропонованому підході процес розшифрування зводиться до відновлення числа за його залишками на основі додавання добутку модулів зі складностями $O(n)$ і $O(n^2)$ відповідно, то загальнаобчислювальна складність становитиме $O\left(n^2\left(\frac{k^2+k}{2}\right)+\frac{n}{2}\log n\right)$, k – кількість модулів. Для прикладу, якщо $k=3$, то складність становить $O\left(6n^2+\frac{n}{2}\log n\right)\approx O(n^2)$.

У класичній криптосистемі Рабіна, яка ґрунтується на розв'язанні систем конгруенцій з використанням китайської теореми про залишки чи алгоритму Гарнера, обчислювальна складність становить $O1\left(kn^3+n^2(2k+1)+nk\right)\approx O1\left(n^3\right)$ та $O2\left(kn^3+n^2\left(\frac{k^2+k+2}{2}\right)\right)\approx O2\left(n^3\right)$ відповідно.

На рисунку 2 представлена поверхня, яка характеризує графічні залежності обчислювальної складності запропонованого методу від кількості модулів та їх розрядності. Бачимо, що функція складності істотно зростає із збільшенням аргументів.

Проведені дослідження свідчать про те, що реалізація запропонованого алгоритмічного забезпечення трьох модульного крипто алгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Крім того, важливо, що даний підхід повинен спростити апаратну реалізацію та структурну складність при схемотехнічному проектуванні трьохмодульної криптосистеми Рабіна за рахунок використання однотипних суматорів замість перемножувачів та мультиплексорів.

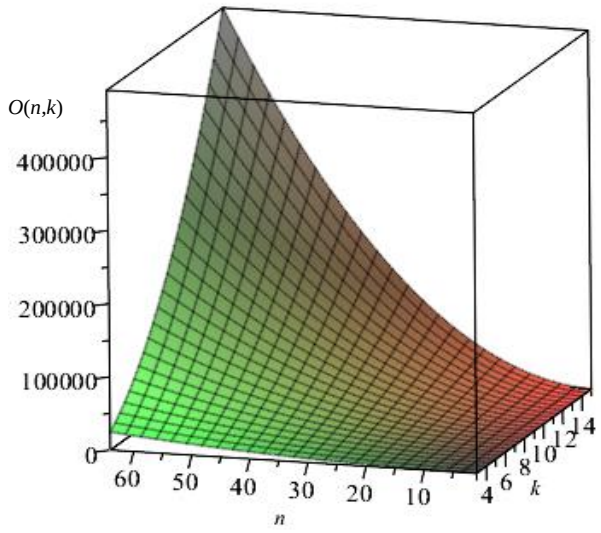

Рис. 2. Графічна залежність обчислювальної складності запропонованого методу від кількості модулів та їх розрядності

Висновки

У роботі представлено розробку трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання. Використання векторно-модульного методу виконання модулярного множення дозволяє пришвидшити процес шифрування/дешифровування інформаційних потоків шляхом заміни операції множення операцією додавання. Використання методів додавання модуля та добутку модулів замість відповідно символів Якобі або Лежандра та китайської теореми про залишки для пошуку квадратичного лишку та відновлення десяткового числа за його залишками дає можливість зменшити обчислювальну складність вказаних операцій. Даний підхід при схемотехнічному проектуванні трьохмодульної криптосистеми Рабіна дозволяє використовувати однотипні суматори замість мультиплексорів та перемножувачів, зменшуючи при цьому апаратну та структурну складність реалізації. Проведені дослідження свідчать про те, що реалізація трьох модульного крипто алгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Показано, що із збільшенням розрядності чисел та кількості модулів обчислювальна складність реалізації криптосистеми Рабіна істотно зростає.

Список літератури

1. Adki V., Hatkar S.A Survey on Cryptography Techniques.*International Journal of Advanced Research in Computer Science and Software Engineering*. 2016. Vol. 6 (6).P. 469-475.
2. Ambedkar B.R., Gupta A., Gautam P., Bedi S. An Efficient Method to Factorize the RSA Public Key Encryption.*Communication Systems and Network Technologies:*Proceeding of International Conference. 2011.P. 108–111.
3. Касянчук М.М., Якименко І.З., Волинський О.І., Пітух І.Р. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона. *Вісник Хмельницького національного університету. Технічні науки.* 2011. №3. С. 265-273.

4. Roy R., Datta D., Bhagat S., Saha S., Sinha A. Comparative Study and Analysis of Performance samong RNS, DBNS, TBN Sand MNS for DSP Applications. *Journal of Signal and Information Processing*. 2015. Vol. 6. P. 49-65.
5. Николайчук Я.М., Касянчук М.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера. *Інформатика та математичні методи в моделюванні*. 2011. №2. С. 123–130.
6. Касянчук М.М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія). Тернопіль: Економічна думка (ТНЕУ), 2019. 224 с.
7. Касянчук М.М. Побудова трьохмодульної модифікованої досконалої форми системи залишкових класів на основі розв'язку квадратного рівняння. *Інформатика та математичні методи в моделюванні*. 2016. Т.6, №1. С. 19–25.
8. Ananda Mohan P.V. Residue Number Systems: The ory and Applications. Birkhäuser, 2016. 351 p.
9. Elia M., Schipani D. Onthe Rabinsignature. *J. Discrete Math. Sci. Cryptogr*. 2013.Vol. 16.№6,P.367-378.
10. Kasianchuk M. Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S. Rabin's modified method of encryption using various forms of system of residual classes. *The Experience of Designing and Application of CAD System sin Microelectronics* (*CADSM-2017*): Proceedings of the XIV International Conference. Polyana-Svalyava. 2017. P.222-224.
11. HemaV., Ganaga Durga M. Data Integrity Checking Based On Residue Number System and Chinese Remainder Theorem In Cloud. *International Journal of Innovative Researchin Science, Engineering and Technology*. 2014.Vol.3 (3). P. 2584-2588.
12. Касянчук М.М., Якименко І.З., Івасьєв С.В. Криптосистема Рабіна на основі операції додавання. *Математичне та комп'ютерне моделювання: Технічні науки.* 2019. В.19. С.145-150.
13. Hoffstein J.,Pipher J., Silverman J. An Introduction to Mathematical Cryptography. Springer Science + Business Media, LLC, 2008. 524 p.
14. JeffreyH., JillP., JosephH. An Introduction to Mathematical Cryptography. Berlin: Springer, 2008. 540 p.
15. Srivastava A., Mathur A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem.*International Journal of Scientific and Research Publications*. 2013. Vol. 3 (6). P. 1-4.
16. Zheng Tian-Xiang. Enhanced Rabincrypto system based on cubic congruence equation. *Journal of Computer Applications*. 2009. №7.P. 121-129.
17. Yahia Awad, Abdu lNasser El-Kassar, Therrar Kadri. Rabin Public-Key Crypto system in the Domain of Gaussian Integers. Proceedings of the International Conference on Computer and Applications (ICCA). 2018.P. 1-11.
18. Hayder R.H. H-Rabim Cryptosystem. *Journal of Mathematics and Statistics*. 2014. Vol. 10 (3). P. 304-308.
19. Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. Mc Graw-HillScience, Engineering, Math. 2006. 336 p.
20. Svidan O., Zilic A. Directresidue-to-analog conversion scheme based on Chinese remainder theorem. *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems*. 2010.P. 687–690.
21. 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.

22. ZhengbingHu., Dychka I., Onai M.,Bartkoviak A. The Analysis and Investigation of Multiplicative Inverse Searching Method sinthe Ring of Integers Modulo M. *International Journal of Intelligent Systems and Applications (IJISA)*. 2016. Vol. 8, №11. P. 9-18.

DEVELOPING RABIN THREE-MODULAR CRYPTOSYSTEM BASED ON THE OPERATION OF ADDITION

Kasianchuk M.M., Lototsky O.Ya., Yatskiv S.V., Ivasiev S.V., Tymoshenko L.M.

West Ukrainian National University, 11, Lvivska Str., Ternopil, 46020, Ukraine;
E-mail: kasyanchuk@ukr.net, lmt0902@gmail.com,
jazkiv@ukr.net, stepan.ivasiev@gmail.com

Nowadays, one of the most common algorithms for asymmetric cryptography is the Rabin cryptosystem. The encryption process is similar to the RSA cryptosystem, but instead of modular exponentiation, the operation of squaring modulo is used. This provides faster performance of the encryption algorithm without the loss of cryptosecurity compared to RSA. However, the decryption process requires considerable time and hardware costs.

Therefore, the purpose of this work is to develop a three-modular Rabin cryptosystem using only the addition operation, as well as to study its time complexity. To perform the operation of modular multiplication, it is proposed to use a modular-vector method, in which multiplication is replaced by the operation of adding the appropriate values. The methods of adding module and product of modules are used to find the quadratic surplus and for decimal number recovery by its residues instead of using the Jacobi or Legendre symbols and the Chinese Reminder Theorem. This makes it possible to reduce the time complexity of these operations.

The scheme of three-modular Rabin cryptosystem and an example of its implementation based only on the addition operation are given. The use of one-type adders instead of multiplexers and multipliers in this approach allows one to simplify the hardware and structural complexities of the circuit design of a three-modular Rabin cryptosystem. To compare the time complexities in different implementations of the Rabin cryptosystem, its most time-consuming operations are considered.

The research conducted show that the implementation of a three-modular Rabin crypto algorithm based only on the addition operation makes it possible to reduce the time complexity of basic operations from cubic to quadratic one. The graphical dependence of time complexity on digit capacity and a number of modules is presented. It is shown that with the increase of these arguments the time complexity of the implementation of the Rabin cryptosystem significantly increases.

Keywords: Rabin three-modular cryptosystem, addition, modular-vector method, time complexity, quadratic surplus, Chinese Remainder Theorem.