УДК 004.056: 681.51

УДОСКОНАЛЕННЯ РЕАЛІЗАЦІЇ АСИМЕТРИЧНИХ КРИПТОАЛГОРИТМІВ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Якименко І.З.[1)], Касянчук М.М.[2)], Кінах Я.І.[3)], Власюк І.М.[4)]
Тернопільський національний економічний університет
[1)] *к.т.н;* [2)] *к.ф.-м.н;* [4)] *магістрант*
[3)]*Тернопільський національний технічний університет ім. І. Пулюя, к.т.н*

І. Постановка проблеми

Сучасні системи захисту інформаційних потоків будуються на основі асиметричних крипто алгоритмів RSA, Ель-Гамаля[1],Рабіна[2]. Для забезпечення необхідного рівня захисту на сьогоднішній день необхідно використовувати параметри – ключі, блок шифрування та модуль криптоперетворення не менше 1024 бітз перспективою їх зростання в найближчі роки до 2048 та 4096 біт.

Вирішення даного класу задач можна здійснити з використанням системи залишкових класів (СЗК), яка володіє рядом переваг в порівнянні з двійковою – здійснення операцій паралельно та зменшення розрядності операндів, які не перевищують розрядності набору обраних модулів СЗК. Поряд з цим існують певні труднощі при переведенні з СЗК в десяткову систему числення, а саме необхідність пошуку оберненого елемента за модулем, тобто базисних чисел. Слід відмітити, що існують набори модулів, які утворюють досконалу форму СЗК (базисні числа рівні 1)[3] та модифіковану досконалу СЗК(базисні числа рівні ±1) [4], що суттєво зменшує часову складність переведення.

Тому постає задача підвищення швидкодії та зменшення складності базових операцій асиметричних крипто алгоритмів RSA, Ель-Гамаля,Рабіна на основі сумісного застосування СЗК та алгоритму векторно-модульного множення [5].

ІІ. Застосування СЗК та векторно-модульного алгоритму модулярного множення в асиметричних криптоалгоритмах

Фундаментальною теоретичною основою СЗК є алгебра і теорія чисел, зокрема китайська теорема про залишки. Тобто, будь-яке додатнє число можна представити у вигляді залишків по обраних взаємно простих модулях, і всі операції проводити над залишками. Оскільки при шифруванні/дешифруванні асиметричних криптоалгоритмівRSA, Ель-Гамаля використовується операція медулярного експоненціювання, тому пропонується використання СЗК, коли основа степеня розбивається на залишки по обраних модулях, далі застосовується векторно-модульний алгоритм модулярного. Всю процедуру можна описати такими виразами:

$$M^x \bmod p = \left(\sum_{i=1}^{l} b_i B_i m_i \right) \bmod p , \qquad (1)$$

де $m_i = (M \bmod p_i)^x \bmod p_i$, $p = \prod_{i=1}^{l} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів.

Пошук значення $m_i = (M \bmod p_i)^x \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення, представивши $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, *де* $x_j = 0,1$:

$$m_i = (M \bmod p_i)^{\sum_{j=0}^{n-1} x_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (M \bmod p_i)^{x_j \cdot 2^j} = \prod_{j=0}^{n-1} s_j \bmod p_i . \qquad (2)$$

де $s_i = M^{2^i} \bmod p_i$, при чому $s_i = (s_{i-1})^2 \bmod p_i$.

Тоді будь-який степінь x можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомого ютаблиці 1. Основними перевагами такого методу є здійснення операцій над числами значно менших розмірів в порівнянні з класичним підходом, що дозволяє пришвидшити алгоритм медулярного експоненціювання.

Таблиця 1

Вектор піднесення до степеня в базисіРадемахера–Крестенсона

x_{n-1}		x_i	…	x_1	x_0
$M^{2^{n-1}} \bmod p_i$	…	$M^{2^i} \bmod p_i$	…	$M^{2^1} \bmod p_i$	$M^{2^0} \bmod p_i$

При знаходженні значення $s_i s_{i-1} \bmod p_i$ представимо $s_i = \sum_{j=0}^{n-1} f_j \cdot 2^j$ та $s_{i-1} = \sum_{k=0}^{n-1} w_k \cdot 2^k$, де $f_j, w_k = 0,1$, n–розрядність модуля p_i. На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$h_0 = 2^0 s_i \bmod p_i,\ h_i = 2 \cdot h_{i-1} \bmod p_i, \tag{3}$$

в другому w_i, як показано в таблиці 2.

Таблиця 2

Представлення вектор-рядків модульного множення

h_{n-1}	…	h_i	…	h_1	h_0
w_{n-1}		w_i	…	w_1	w_0

Результатом модулярного множення двох n – розрядних чисел знаходиться згідно формули:

$$s_i s_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} w_i \cdot h_i \right) \bmod p_i, \tag{4}$$

Розроблений метод характеризується меншою часовою складністю порівняно з класичними.

Для виконання шифрування в крипто алгоритмі Рабіна необхідно знайти значення піднесення до квадрату за модулем. Дану операцію доцільно виконати з використанням СЗК, коли основа квадрата розбивається на залишки від ділення повідомлення M на попарно взаємно прості модулі і застосувати до них векторно-модульний алгоритм модулярного множення.

$$M^2 \bmod p = \left(\sum_{i=1}^{\kappa} b_i B_i m_i \right) \bmod p, \tag{5}$$

де $m_i = (M \bmod p_i)^2 \bmod p_i$, $p = \prod_{i=1}^{k} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, k – кількість модулів. Отже, запропонований підхід дозволить суттєво зменшити часову складність та підвищити ефективність виконання операції піднесення до степеня двійкового числа будь-якої розрядності за модулем p, яка є базовою в асиметричних криптоалгоритмах.

IV. Висновки

В роботі представлено удосконалення реалізації асиметричних алгоритмів шифрування RSA, Ель-Гамаля, Рабіна, а саме базових операцій – медулярного експоненціювання та піднесення до квадрату за модулем багаторозрядних чисел, на основі СЗК та векторно-модульного алгоритму медулярного множення, що дозволило суттєво зменшити часову складність та підвищити ефективність виконання процесу шифрування/дешифрування.

Список використаних джерел

1. Касянчук М.М, Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів / М.М. Касянчук,І.З. Якименко, Л.О. Дубчак, Н.А.Рендзеняк, Н.М.Мандебура// Вісник Хмельницького національного університету. Технічні науки. – №1(245). – 2017.– С. 127-131.
2. Якименко І.З.Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона//І.З. Якименко, М.М. Касянчук, О.І.Волинський, І.Р.Пітух./ Вісник Хмельницького національного університету. Технічні науки. – №3. – 2011.– С. 265-273.
3. Kasianchuk M. Algorithms of findings of perfect shape modules of remaining classes system/ M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy //XIII International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)”, 23-25 February, 2015, Polyana-Svalyava (Zakarpattya), Ukraine. – P.168-171.
4. КасянчукМ.М.Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки/М.М.Касянчук, І.З. Якименко, І.Р.Паздрій, Я.М.Николайчук//Вісник Хмельницького національного університету. Технічні науки. - №1(221). – Хмельницький, 2015.– с. 170-176.
5. Kozaczko D. Vector Module Exponential in the RemainingClasses System/ D. Kozaczko, M. Kasianchuk, I. Yakymenko, S.Ivasiev//Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015) – Warsaw, Poland. – V.1. – September, 2015. – P.161–163.