УДК 681.3

МЕТОДИ ПОШУКУ НАЙБІЛЬШОГО СПІЛЬНОГО ДІЛЬНИКА НА ОСНОВІ ВИКОРИСТАННЯ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСІВ РАДЕМАХЕРА ТА КРЕСТЕНСОНА

Якименко І.З. [1], Пундор Ю.О.[2], Мачуляк М.В. [3], Горошко Н.М. [4]
Тернопільський національний економічний університет,
[1] к.т.н; [2] магістрант; [3] студент
[4]Тернопільська загальноосвітня школа №11, вчитель математики

І. Постановка проблеми

В задачах захисту інформації на основі використання асиметричної криптографії (алгоритмів RSA, Рабіна, Ель-Гамаля), при формуванні електронного цифрового підпису [1]–[3], дослідженні порядку еліптичної кривої [4] та в Китайській теоремі про залишки важливою операцією є пошук найбільшого спільного дільника (НСД). На сьогоднішній день найбільш відомим методом розв'язання даного класу задач є застосування алгоритму Евкліда, основним недоліком якого є те, що він є строго послідовним та неможливо його розпаралелити.

В зв'язку з цим актуальною проблемою досліджень є зменшення часової складності пошуку НСД на основі розробки теоретичних основ з використанням двійкової системи числення та системи числення залишкових класів [5]–[7].

ІІ. Мета роботи

Основною метою роботи є розробка методів пошуку НСД на основі використання теоретичних основ двійкової та системи числення залишкових класів (СЗК), що дозволить зменшити часову складність реалізації запропонованих алгоритмів.

ІІІ. Методи пошуку найбільшого спільного дільника

Знаходження НСД потребує виконання операції пошуку залишків $X(\mathrm{mod}Y)$ чисел великої розрядності. Тому розроблено метод в якому операція ділення замінюється операцією додавання залишків степеневих коефіцієнтів по заданому модулю з використанням ТЧБ Крестенсона-Радемахера, (табл. 1) та виразу (2).

Таблиця 1

Знаходження залишків степенів двійки

2^{n-1}	2^{n-2}	…	2^{i}	…	2	1
x_{n-1}	x_{n-2}	…	x_i	…	x_1	x_0
y_{n-1}	y_{n-2}	…	y_i	…	y_1	y_0

Щоб знайти елемент y_i, необхідно попередній елемент y_{i-1} помножити на 2 (дописати в кінці 0 у двійковому записі) і порівняти з модулем p_1 та $X(\mathrm{mod}Y)$ знаходити згідно виразів:

$$y_i = \begin{cases} 2 \cdot y_{i-1}, & 2 \cdot y_{i-1} < Y \\ 2 \cdot y_{i-1} - y_i, & 2 \cdot y_{i-1} \geq Y \end{cases}; \quad (1)$$

$$X \bmod Y = \left(\sum_{i=1}^{n-1} y_i \right) \bmod Y, \; x_i = 1. \quad (2)$$

В роботі запропоновані три методи пошуку найбільшого спільного дільника з використанням математичних основ двійкової системи числення та СЗК. Перший підхід полягає у вдосконаленні реалізації алгоритму Евкліда, тобто пошуку залишків $r_1 = res(X \bmod(Y))$, $r_2 = res(Y \bmod(r_1)), \ldots,$ $r_{n-1} = res(r_{n-1} \bmod(r_n))$ на основі використання алгоритму пошуку залишків великорозрядних чисел в розмежованій системі числення Радемахера-Крестенсона. Часова складність даного підходу буде $O2(n) = \left(17{,}5n \cdot \left(\log_2 \frac{n}{2} \right) \right)$.

Другий метод полягає в застосуванні ТЧБ Крестенсона, тобто поданні чисел X і Y у цілочисельній формі системи залишкових класів по простих модулях, які не перевищують половину

розрядності більшого з X, Y. Згідно виразу $z=\prod_{j=1}^{k} p_j$, де $p_j=\begin{cases} p_j, a_j=b_j=0 \\ 1, a_j\neq b_j \end{cases}$ знаходиться найбільший мультиплікативний дільник Z.

Після перевірки степенів ${p_j}^m$, де m - показник степеня, при якому залишки $a_j=b_j=0$, отримується остаточна формула знаходження НСД $Z=\prod_{j=1}^{k} {p_j}^{m_j}$. Часова складність даного методу буде $O(n)=\left(\log_2 n\cdot\left(\log_2 n+\frac{n}{2}+k\cdot\log_2 n\right)+n\cdot\log_2 n/2\right)$.

Третій метод полягає у вдосконаленні методу з використанням ТЧБ Крестенсона за рахунок вилучення кроку пошуку найбільшого мультиплікативного дільника з часовою складністю $O3(n)=\left(\log_2 n\left(\log_2 n+k\cdot\log_2 n+\frac{n}{2}\right)+\frac{n}{2}\cdot\log_2\frac{n}{2}\right)$.

У порівнянні з відомим алгоритмом Евкліда, часова складність якого рівна $O1(17{,}5n(n+1)^2)$, запропонований алгоритм знаходження НСД характеризується наступними перевагами:

1. Обчислення матриць ${a_j}^m, {b_j}^m$ двох векторів по модулях ${p_j}^m$ виконується паралельно з використанням двох процесорів.

2.Паралельно порівнюється $X^{(m)}$ і $Y^{(m)}$, та отримується $Z=\prod_{j=1}^{k} {p_j}^{m_j}$.

Отже, розроблені методи доцільно використовувати в задачах захисту інформації на основі використання асиметричної криптографії, в електронно-цифровому підписі, дослідженні порядку еліптичної кривої та в Китайській теоремі про залишки.

IV. Висновки

В роботі розроблені методи пошуку НСД на основі використання теоретичних основ двійкової та системи числення залишкових класів, які дозволяють зменшити часову складність. Крім того вперше запропонований підхід, який можна ефективно застосовувати в високопродуктивних системах захисту інформації на основі паралелізації обчислювальних процесів.

Список використаних джерел

1. Задірака В. Комп'ютерна криптологія: Підручник. / В.Задірака, О. Олексюк – К.:2002. – 504 с.
2. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.П. Шаньгин; Под ред. В.Ф.Шаньгина.– М.: Радио и связь, 1999. – 328с.
3. Фергюсон Н. Практическая криптография: Пер. с англ. / Н.Фергюсон, Б. Шнайер – М.: – Вильямс, 2005. – 424 с.
4. Якименко І.З. Прискорення алгоритму Шуфа методом паралельних обчислень./ І.З. Якименко, А.А. Хомінчук // Матеріали дванадцятої наукової конференції Тернопільського державного технічного університету імені Івана Пулюя. – Тернопіль, ТДТУ.–14-15 травня 2008 р. – С:116.
5. Kasianchuk M.M. Theoretical Foundations of the Modified Perfect form of Residue Number System./M.M. Kasianchuk, Ya. M. Nykolaychuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. 2016 – pp. 219-223.
6. Kasianchuk M.M. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes./M. M. Kasianchuk, Ya. N NykolaychukI. Z. Yakymenko// Journal of Automation and Information Sciences. – 2016. – Vol.48, №8. – P.56-63.
7. Sachenko A. Data Encoding in Residue Number System/ A. Sachenko, V. Yatskiv, R. Krepych, A. Karachka // Proceeding of the International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: IDAACS'2009, 2009. – P. 679 – 681