

ЗАСТОСУВАННЯ МЕТОДІВ ОПТИЧНИХ ОБЧИСЛЕНЬ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАДАЧ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Актуальною науково – технічною задачею є обґрунтування та дослідження рівня криптографічного захисту інформації в комп'ютерних мережах. При цьому особливої значимості набуває задача ефективного захисту від можливої атаки криптоаналітиків на основі оптичних комп'ютерних засобів.

Оскільки етап просіювання криптоаналітичного алгоритму загального решета числового поля є трудомістким, то для його реалізації доцільно використовувати електронно – оптичні прилади, які працюють зі швидкістю обмеженою тільки доступними електронно – оптичними компонентами [1].

Такі засоби криптоаналізу відрізняються від відомих перспективними часовими характеристиками. Це досягається за рахунок таких чинників: здатності матричної оптичної архітектури підтримувати максимальний паралелізм оптичних методів обчислень, забезпечуючи організацію розрядно-зрізового оптичного введення-виведення та обробки матриць; наявності оптичних локальних і глобальних зв'язків між процесорними елементами з властивістю перетинатись без перешкод.

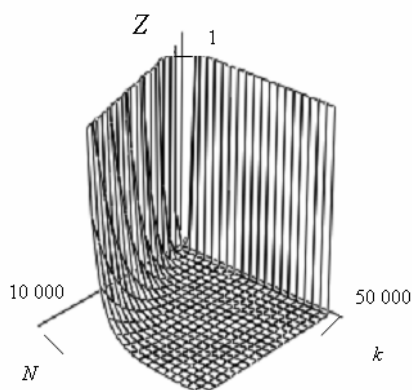
Змоделюємо роботу такого приладу:

$$Z(N, k) = \frac{N^5 - 15k^2}{(k+1)^5} + \frac{Nk^2 + N^3 + 24N^5 + k^5}{4 + 135N^5 + (Nk)^5} \quad (1)$$

де Z – функція сформована за допомогою методу вагових коефіцієнтів і є безрозмірною величиною, що показує у скільки разів зменшується час виконання удосконаленого алгоритму, порівняно з його традиційною реалізацією; N – кількість процесорів робочих станцій; k – кількість підзадач.

Запропоновані оптоволоконні засоби криптоаналізу дозволять на практиці скоротити час етапу просіювання у 8 разів для ключа довжиною 1024 біт.

Графічне представлення результату експерименту розміщено на рисунку 1:



З графіка видно, що за наведеної реалізації алгоритму час його виконання значно зменшується при довільній кількості процесорів, та підзадач. За такої реалізації цього етапу час його виконання зменшується у 7 разів.

Деяка частина сигналів відсіюється і формує на приймачі просіяну матрицю. Система рідкокристалічних клапанів складається з окремих комірок, у яких розміщено рідкий кристал. Залежно від його стану промінь змінюється, таким чином виконується операція просіювання. Згідно з принципом суперпозиції променів в одному приладі може функціонувати три джерела і три приймачі

одночасно, що дозволяє значно економити обчислювальні ресурси.

Література:

1. Н.І. Заболотна, В.В. Шолота, О.В. Маліночка Оптиелектронний векторно-матричний помножувач з плаваючою комою // Оптико-електронні інформаційно-енергетичні технології. – №2. – 2002. – С.112-122.