УДК 004.414.28
Я. Кінах[1], І. Бойко[1], Р. Паславський[2], У. Яциковська[3], М. Карпінський[3]
[1] (Тернопільський національний технічний університет імені Івана Пулюя)
[2] (Львівський національний аграрний університет)
[3] (Академія технічно-гуманістична, Польща)

ПРОГРАМУВАННЯ ПАРАЛЕЛЬНИХ КРИПТОАНАЛІТИЧНИХ АЛГОРИТМІВ НА КВАНТОВИХ ЗАСОБАХ

UDC 004.414.28
I. Kinakh[1], I. Boyko[1], R. Paslavsky[2], U**. Yatsykovska[3], M. Karpinsky[3]**
[1](Ternopil I.Pulyu National Technical University, Ukraine)
[2](Lviv National Agrarian University, Ukraine)
[3](University of Bielsko-Biala, Poland)

PROGRAMMING OF PARALLEL CRYPTOANALYTIC ALGORITHMS ON QUANTUM MEANS

При паралельному програмуванні криптоаналітичних алгоритмів мовою QCL продуктивність в значній мірі залежить від відповідності між структурою квантових зв'язків обчислювальних елементів кубітів і структурою програми [2].

Дослідження показали, що для програмування етапу просіювання криптоаналітичного методу загального решета числового поля доцільно врахувати особливості роботи спеціалізованого рідкокристалічного наноклапана, завдяки чому отримаємо швидку зміну значення елементів розрідженої матриці на етапі вводу-виводу даних, що є трудомістким алгоритмом. При цьому елементи матриці кодуються у формі квантових сигналів на джерелі, як qureg дані [1]. Завдяки спеціалізованій рідкокристалічній наноклапаній програмно-апаратній обчислювальній системі значно зростає продуктивність виконання другого етапу удосконаленого криптоалгоритму у дсятки разів.

Мінімальне та максимальне значення часу виконання операцій додавання визначається за співвідношенням, описаним виразом:

$$\min T_{дод}^{п.к.} = (3P + 3M + 8)\cdot \Delta T_{дод}^{РЗ};$$
$$\max T_{дод}^{п.к.} = (4P + 4M + MP + 11)\cdot \Delta T_{дод}^{РЗ}.$$

Де P , К – безрозмірні параметри роботи квантового пристрою.

Тоді час виконання операції на оптоелектронному квантовому решеті можна оцінити так:

$$\Delta T = (\mathrm{M}^3 + \mathrm{M}^2 + 7\mathrm{P} + 6\mathrm{M} + 20 + \mathrm{N}(4\mathrm{P} + 4\mathrm{M} + \mathrm{MP} + 11)\Delta \mathrm{T}^{\mathrm{P3}}.$$

Де N – кількість блоків паралельного алгоритму.

Швидкодія досягається за рахунок таких чинників: здатності матричної квантової архітектури підтримувати максимальний паралелізм оптичних методів обчислень, забезпечуючи структуру удосконаленого кваново-оптичного введення-виведення, наявності квантових локальних і глобальних зв’язків між процесорними елементами на суперпозиції квантів. Отже отримано максимальне значення квантового прискорення завдяки використанню спеціалізованого квантового рідкокристалічного клапана, що пришвидшує процес криптоаналізу асиметричнах криптосистем типу RSA.

Література

1. Юдін О.К. Кодування в інформаційно-комунікаційних мережах: – Монографія. - К.:НАУ,. 2007.-308с.
2. Вакарчук І. О. Квантова механіка. — 4-е видання, доповнене. — Л. : ЛНУ ім. Івана Франка, 2012. — 872 с.