КВАНТОВИЙ АЛГОРИТМ ШОРА ДЛЯ ВИРІШЕННЯ ПРОБЛЕМИ ФАКТОРИЗАЦІЇ ЧИСЛА

Островський А.М.
Науковий керівник – к.т.н., проф. Качко О.Г.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14,
каф. Системотехніки, тел. (057) 702-13-06)
e-mail: albert.ostrovskyi@nure.ua, факс (099) 728-75-48

The given work is devoted to the modern developments in the field of quantum computer algorithms related to cryptanalysis. The major topic of the work is a research of the Shor quantum algorithm that is designed to solve a factorization problem. The work also contains information about the current state of quantum computing technologies and known non-quantum solutions to the factorization problem. The aim of the work is to demonstrate that nowadays-cryptographic systems based on impossibility to find factors of the big number are vulnerable to quantum algorithms or will be vulnerable in the near future.

Несиметричні алгоритми шифрування широко використовуються у сучасних криптосистемах. Найвідомішим є алгоритм RSA, стійкість якого базується на складності задачі факторизації. Для забезпечення безпеки, RSA вимагає, щоб добуток випадкових простих чисел був більше ніж 300 десяткових цифр. Навіть при використанні найшвидшого комп'ютера, доступного на сьогодні, розкладання на множники цілого числа такого розміру вимагає нездійсненно великого часу. Це означає, що RSA безпечний, поки не буде знайдений ефективний алгоритм розкладання на множники.

Досліджені алгоритми розкладання числа на множники для звичайних ЕОМ. Найкращі мають субекспоненціальні складність, це метод квадратичного решета (складність $L_n(0.5,1)$) та метод Ленстра з використанням еліптичних кривих (складність $L_n(0.5,\sqrt{2})$), де L_n це нотація прийнята для позначення субекспоненціальної складності. Тобто жоден з сучасних алгоритмів не може знайти співмножники великого цілого числа з поліноміальною складністю часу [1].

Найвірогідніше рішення цієї проблеми є використання квантових обчислень. Квантова система з L дворівневих кубітів має 2^L лінійно незалежних станів, тобто квантовий обчислювальний пристрій розміром L кубіт може виконувати паралельно 2^L операцій [2]. Компанією Google вже реалізований квантовий процесор з 72 кубітів.

Вивчено квантовий алгоритм Шора для факторизації (розкладання числа на прості множники), реалізація якого, дозволяє розкласти число M за час $O(\lg^3 M)$, використовуючи O(lgM) логічних кубітів. Сутність

алгоритму - знайти період функції $f(x) = a^x (mod\ M)$, де a довільний параметр, M число, яке необхідно факторизувати. Знайшовши період функції, можемо знайти множники числа за допомогою формули $factor_{1,2} = \gcd(a^{r/2} \pm 1, M)$, де $\text{factor}_{1,2}$ – множники числа M, gcd – формула для обчислення найбільшого спільного дільника, r – період. Парадигма квантових обчислень дозволяє знайти період функції з поліноміальною складністю, чого не можна зробити в рамках класичної обчислювальної моделі [3].

Обрана обчислювальна схема для реалізації квантової частини алгоритму, яка представляє собою два квантових регістра m та n, які спочатку знаходяться у нульовому стані. На першому кроці за допомогою операції Уолша-Адамара первинний стан $|0\rangle$ регістра n переводиться в рівно імовірнісну суперпозицію усіх булєвих станів N. На другому кроці до двух регістрів застосовується унітарне перетворення (оракул S_f), яке переводить стан $|x, 0\rangle$ у $|x, f(x)\rangle$. На третьому кроці виконується квантове перетворення Фур'є (QFT), яке уявляє собою унітарне перетворення стану квантового регістра, яке задається N-мірним вектором стану. В результаті ми отримуємо $\frac{1}{N}\sum_{x=0}^{N-1}\sum_{k=0}^{N-1} \exp(2\pi\ i\ kx/N)\ |k, a^x\ mod\ M\rangle$, що є перетвореним першим регістром, де N – кількість усіх можливих булєвих станів. На четвертому кроці виконується вимірювання регістра X відносно ортогональної проекції. Результатом є $|k, a^k\ mod\ M\rangle$, де k ∈ [0, N-1]. Далі знаходимо найкраще приближення (знизу) до k/N, що і буде періодом функції, який потім використовується для знаходження множників числа за допомогою класичних обчислень. Також треба зазначити, що алгоритм є ймовірнісним, де ймовірність знаходження відповіді є $\frac{1}{N}\sum_{x:a^x \equiv a\ mod\ M}^{N-1} \exp(2\pi\ i\ kx/N)$ [4].

Алгоритм є теоретично обґрунтованим та вже використовувався для факторизації числа 15 на справжньому квантовому комп’ютері. Для подальшого дослідження алгоритму буде виконана його реалізація за допомогою однієї з мов програмування для квантових обчислень (Q# та QCL) та аналіз його роботи на більш великих числах.

Список джерел:

1. Ишмухаметов Ш.Т., Методы факторизации натуральных чисел [Текст]: учеб. пособие / Ш.Т. Ишмухаметов.– Казань:Казан.ун., 2011.- 201с.

2. Роман Душкин Квантовые вычисления и функциональное программирование / Р.В. Душкин.-М.: ДМК Пресс, 2015. – 232 с.

3. К.А. Валиев Квантовые компьюетры и квантовые вычесления/К.А. Валиев.-М.:Insitute of Physics and Technology, 2005.- 37с.

4. Shor P. Algorithms for quantum computation [Text]/Shor P.// Foundations of Computer Science.–1994.–№10.-124–134pp.