in the existing technical infrastructure. Thus, the development and efficiency of the ITS is based on ensuring communication between vehicles based on very accurate and up-to-date information about the environment, which, in turn, requires the use of sensitive positioning systems and intelligent communication protocols for information exchange.

References

1. Closs DJ, Davidson J, Dawe RL, Templeton SJ, Levitt KA. The role of IT in logistics. The Official Magazine of the Logistics Institute. 2007;27(6).
2. Ayyappan B, Mohan Kumar P. Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issues. In: 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM); 2016 Mar 30-31; p. 177-180.
3. Hasrouny H, Samhat AE, Bassil C, Laouiti A. VANet Security Challenges and Solutions: A Survey. Vehicular Communications. 2017;7.
4. Kour J, Sharma P. Security Breaches in VANETs and Possible Solutions. In: Proceedings of the 2023 International Conference on Smart Systems and Communication (ICSSC). 2023. DOI: 10.1109/ICSCSS57650.2023.10169394.

УДК 004.056

АНАЛІЗ ТА РЕАЛІЗАЦІЯ КВАНТОВОГО АЛГОРИТМУ ШОРА

Аль-Хамад Н.А., аспірант, naurasalkh@gmail.com, НУ "Запорізька політехніка"
Неласа Г.В., к.т.н., доцент, annanelasa@gmail.com, НУ "Запорізька політехніка"

Протягом останніх кількох років квантові обчислення стають все більш популярним напрямком досліджень. Однією з провідних компаній, що розвиває технології квантових обчислень є IBM. Наприкінці минулого року IBM встановила рекорд найбільшої квантової обчислювальної системи з процесором, який містив 433 кубіта, фундаментальних будівельних блоків квантової обробки інформації, в цьому році – 1000 кубітів. Тепер компанія націлилася на набагато більшу мету: машину на 100 000 кубітів, яку вона прагне створити протягом 10 років [1]. Мета IBM Quantum полягає в тому, щоб масштабувати квантові процесори до такого розміру, щоб вони могли вирішувати найскладніші проблеми світу. Також такі компанії як Google і Microsoft теж ставлять собі за мету побудувати повноцінний квантовий комп'ютер який здатний вирішувати проблеми з якими класичні суперкомп'ютери не здатні впоратися. Залучення

таких великих та всесвітніх компаній показує наскільки важливою та актуальною є область квантових обчислень.

Але які саме проблеми можуть вирішувати квантові комп'ютери? Можна виділити кілька прикладів проблем, де квантові комп'ютери пропонують значні переваги перед найвідомішими класичними підходами. У кожному випадку квантові алгоритми, які, як виявлено, вирішують ці проблеми, використовують квантові ефекти для досягнення переваг, які іноді називають квантовими перевагами. Нижче наведено два корисні квантові алгоритми:

1. Алгоритм Гровера шукає список із N елементів за √N кроків.

2. Алгоритм Шора швидко розкладає великі цілі числа, такі як ті, що використовуються криптографією для захисту конфіденційних даних.

Деякі способи захисту конфіденційної інформації ґрунтуються на припущеннях про те, які проблеми легко чи важко вирішити зловмиснику. Алгоритм RSA є поширеним алгоритмом шифрування, який базується на труднощах знаходження простих множників для великих чисел, тобто факторизації. RSA використовується в Інтернеті та в інших контекстах для захисту даних користувачів, припускаючи, що зловмисники не можуть легко факторизувати дуже великі числа. Нові моделі обчислень, такі як квантові обчислення можуть створити алгоритми які зможуть вирішити таке припущення про факторизацію, як наприклад алгоритм Шора.

Алгоритм Шора дозволяє вирішувати деякі типи криптографічних проблем набагато швидше, ніж класичні комп'ютери, кидаючи виклик припущенням, які зазвичай використовуються для гарантії обчислювальної безпеки. Метою алгоритму Шора є розкладання числа N на прості множники за поліноміальний час.

Основна робота квантових алгоритмів як і алгоритму Шора, полягає в тому, щоб переконатися, що ймовірність вимірювання правильного коефіцієнта в кінці набагато більша, ніж ймовірність вимірювання неправильного коефіцієнта. Скасування неправильних результатів є головної технікою квантового програмування.

Алгоритм Шора складається з двох частин:

1. Класична частина алгоритму.

2. Квантова частина алгоритму.

Класична частина полягає в зведені, яке можна зробити на класичному комп'ютері, задачі розкладання до задачі пошуку порядку.

Квантова частина полягає в вирішенні задачі пошуку періоду функції. Функція має таку форму:

$$f(x) = a^x (mod\ N) \quad (1)$$

В цій функції a – довільне число, N – число для факторизації, x – зміна, яка подається на вхід до функції.

Пошук періоду полягає у використанні квантової оцінки фази унітарного оператора[2]. Квантова схема пошуку періоду представлена на рис. 1.

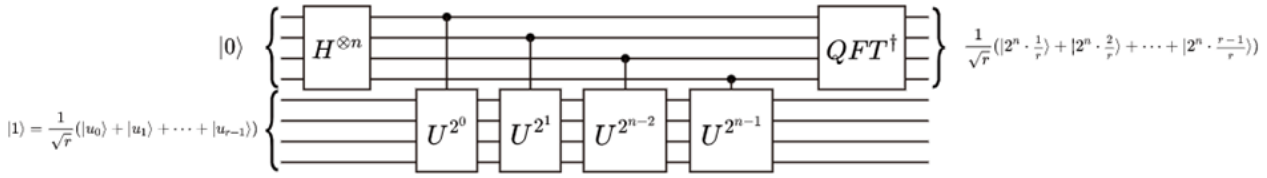

Рисунок 1 – Квантова схема алгоритму Шора для пошуку періоду функції

Взагалі, алгоритм Шора можна розділити на наступні етапи:

1. Обирається випадкове число $1 < a < N$.

2. Обчислюється найбільший спільний дільник чисел a і N – НСД(a, N). Він повинен дорівнювати одиниці.

3. Пошук квантового періоду r функції (1). Період r повинен бути парним числом.

4. Обчислюються два числа – НСД($a^{r/2} + 1$, N) і НСД($a^{r/2} - 1$, N), які є нетривіальними дільниками числа N.

Метою даної роботи є написання тестової програми факторизації чисел $N = 15$ та $N = 21$ з використанням алгоритму Шора в IBM Quantum використовуючи мову Python.

На рис. 2, 3 представлені побудовані в IBM Quantum схеми для пошуку періоду чисел $N = 15$ і $N = 21$.

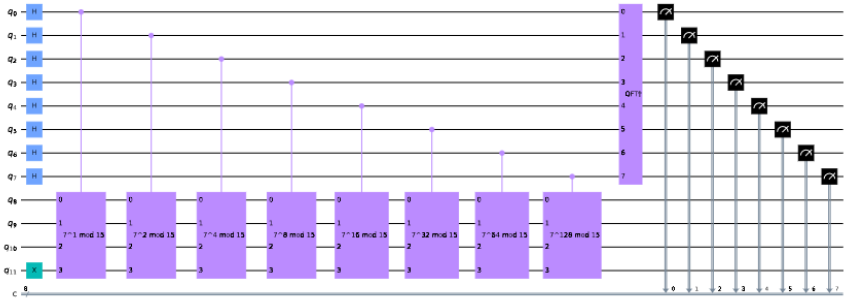

Рисунок 2 – Квантова схема алгоритму Шора для факторизації числа 15 в IBM Quantum

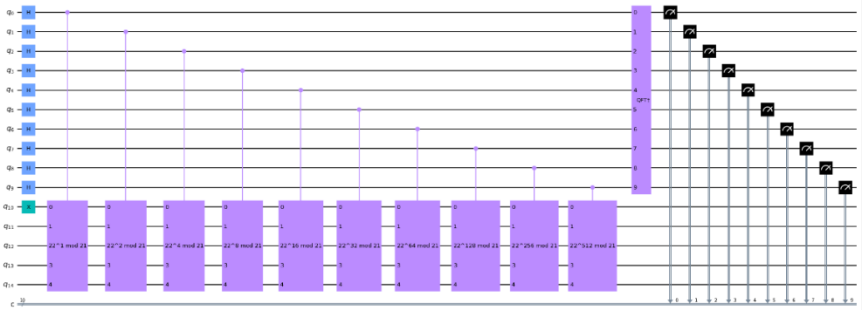

Рисунок 3 – Квантова схема алгоритму Шора для факторизації числа 21 в IBM Quantum

Результати факторизації, використовуючи алгоритм Шора, представлені на рис. 4, 5.

```
Attempt 1:
Register Reading: 00000000
Corresponding Phase: 0.000000
Result: r = 1

Attempt 2:
Register Reading: 00000000
Corresponding Phase: 0.000000
Result: r = 1

Attempt 3:
Register Reading: 01000000
Corresponding Phase: 0.250000
Result: r = 4
Guessed Factors: 3 and 5
*** Non-trivial factor found: 3 ***
*** Non-trivial factor found: 5 ***
```

Рисунок 4 – Результати факторизації числа N = 15

```
Attempt 1:
Result: r = 6
Guessed Factors: 7 and 3
*** Non-trivial factor found: 7 ***
*** Non-trivial factor found: 3 ***
```

Рисунок 5 – Результати факторизації числа N = 21

Висновок: В результаті роботи була побудована квантова схема алгоритму Шора для вирішення проблеми пошуку періоду функції, реалізовано квантовий алгоритм Шора в IBM Quantum на прикладі факторизації простих чисел 15 та 21. Досліджено, що квантові алгоритми, в тому числі алгоритм Шора, мають ймовірнісний характер знаходження рішення, тому головна задача при написанні таких алгоритмів – це скасування неправильних результатів, щоб ймовірність знаходження правильного рішення була якомога більшою.

Список використаних джерел

1. Charting the course to 100,000 qubits [Електронний ресурс]/ Режим доступу: https://research.ibm.com/blog/100k-qubit-supercomputer.
2. Qiskit documentation [Електронний ресурс]/ Режим доступу: https://qiskit.org/documentation/.