УДК 004.27

ПРОГРАМНІ СЕРЕДОВИЩА ДЛЯ ВИКОНАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ

Шемет Євген, Яровий Андрій

Вінницький національний технічний університет

Анотація

В ході проведеного дослідження проаналізовані доступні програмні середовища для виконання квантових обчислень. Проведено порівняння програмних середовищ для імітаційного моделювання квантового комп'ютера за функціональними можливостями. Відзначено актуальність дослідження квантових обчислень в задачах криптографічного кодування.

Abstract

In the given research program environments for quantum computations were analyzed. Environments have been compared by functionality. The actuality of such quantum computations in cryptographic problem solving was denoted.

Вступ

Створюється велика кількість теоретичних і практичних розробок в сфері квантових обчислень [1]. Висока актуальність теми пов'язана з можливостями, які потенційно може надавати квантовий комп'ютер. Особливо важливі можливості (і навіть загрози) пов'язані з криптографією (наприклад, технологія блокчейн), призвели до створення нового напрямку пост-квантової криптографії [2]. До-квантова криптографія базувалася на трьох складних математичних задачах: "Факторизація цілих чисел", "Визначення дискретного логарифму" та "Побудові еліптичних кривих". Всі ці задачі можуть бути ефективно вирішені за допомогою алгоритму Шора на квантовому комп'ютері [3].

Для роботи з квантовим комп'ютером можна використовувати реальний квантовий комп'ютер або імітувати його роботу.

Способи задання квантового алгоритму

Для виконання квантових обчислень в програмному середовищі необхідно використати один із зазначених способів задання квантового алгоритму:

1. QASM - спеціальна мова подібна до асемблерної [4];
2. Схема - створення схеми в графічному режимі [5];
3. Предметно-орієнтована мова (Domain-specific language) - інструменти для імітаційного моделювання, розповсюджуються у вигляді бібліотеки для певної мови програмування та надають програмний інтерфейс.

Програмні середовища для імітаційного моделювання квантового комп'ютера

Програмні середовища для імітаційного моделювання квантового комп'ютера поділяються на:

1. Локальні - коли моделювання відбувається безпосередньо на комп'ютері користувача;

2. Онлайн - коли квантовий алгоритм, заданий певним чином, передається по мережі Internet і виконується в хмарному середовищі.

Необхідно відзначити, що існує велика кількість програмних розробок для імітаційного моделювання роботи квантового комп'ютера. Проте, більшість із них створено в учбових цілях. Разом з тим, велика кількість із них застаріла та більше не підтримується розробниками [6].

Локальні симулятори

Серед локальних симуляторів варто відзначити нову розробку LIQUi|⟩ Microsoft. LIQUi|⟩ (або Liquid) - високооптимізований інструмент що дозволяє симулювати до 30 кубіт одночасно, у локальному середовищі [7]. На даний момент локальні симулятори надають найбільш широкі можливості для проведення досліджень складних алгоритмів, з схемами що вимагають велику кількість кубіт.

Liquid може працювати в трьох режимах [8]:

1. Фізичне моделювання - моделювання, що намагається відтворити фізичні аспекти роботи квантового комп'ютера. Імітаційне моделювання повільне у зв'язку з тим, що доводиться вирішувати велику кількість диференційних рівнянь. Може оперувати відносно невеликою кількістю кубітів (до 30);

2. Універсальне моделювання - гнучке імітаційне моделювання, що може оперувати з великою кількістю різних операцій (враховуючи ті, що задав користувач). Може оперувати невеликою кількістю кубітів (до 30);

3. Стабілізаційне моделювання - може опрацьовувати велику кількість кубітів одночасно (~10000). Обмежене невеликою кількістю операцій, що можуть виконуватись (група Кліфорда [9]).

Онлайн симулятори

Серед онлайн симуляторів існує дві групи розробок - симулятори, що використовуються для підготовки до виконання на реальних квантових комп'ютерах та окремі незалежні симулятори.

1.Forest - дозволяє здійснювати імітаційне моделювання роботи 26-кубітового квантового комп'ютера. Доступ через програмний інтерфейс (Python). Працює поряд з реальним квантовим комп'ютером [10].

2.IBM Q Experience - надає доступ до імітаційного моделювання на 5-ти кубітовому комп'ютері через графічний інтерфейс, та до 16-ти і 20-ти кубітовому комп'ютері через програмний інтерфейс QISKIT (Python). Працює поряд з реальним квантовим комп'ютером [11].

3.QuantumPlayground - імітаційне моделювання квантового комп'ютера від Google. Має графічній інтерфейс та дозволяє здійснювати імітаційне моделювання роботи 22-кубітового квантового комп'ютера [12].

Доступ до реального квантового комп'ютера

Наразі є кілька квантових комп'ютерів що надають доступ онлайн. Вони надаються безкоштовно або умовно безкоштовно (з певними обмеженнями).

1.Forest - надає доступ до реального 19-кубітового квантового комп'ютера. Доступ через програмний інтерфейс (Python), безкоштовно [10].

2.IBM Q Experience - дозволяє працювати на 5-ти кубітовому комп'ютеру через графічний інтерфейс, та до 16-ти і 20-ти кубітовому комп'ютеру через програмний інтерфейс QISKIT (Python). 5-ти та 16-ти кубітові процесори - безкоштовно. 20-ти кубітовий процесор - тільки для партнерів [11].

3.Quantum in the Cloud - розроблений The University of Bristol. Надає безкоштовний доступ до квантового комп'ютера на 4 кубіта [13].

Оскільки ресурс реального квантового комп'ютера обмежений, запуск алгоритму ставиться в чергу та очікує деякий час на виконання. IBM Q Experience пропонує, при наявності, отримати готові результати з минулих запусків подібних алгоритмів.

Особливістю реальних квантових комп'ютерів є те що на відміну від симуляторів, вони можуть підтримувати лише обмежену кількість зв'зків між кубітами, що обумовлене топологією.

Висновки

В ході дослідження здійснено порівняння програмних середовищ для квантових обчислень. Виокремлено ряд розробок великих міжнародних команій, таких як: Google, Microsoft, IBM, що підтверджує високу зацікавленість сучасних IT-компаній в цьому напрямку. Поряд із ними існують розробки університетів (The University of Bristol), що підтверджує актуальність даного напряму досліджень для наукових розробок. Також, виокремлено розробки невеликих компаній (стартапів), які будують свою бізнес-модель навколо квантових обчислень, що відкриває доступність квантових обчислень для невеликого бізнесу.

Не дивлячись на обмежені можливості існуючих квантових комп'ютерів, вони вже наближаються до потужностей, що можуть загрожувати криптографічній безпеці сучасних алгоритмів. Зокрема потужність окремого квантового комп'ютера порівнюють з потужністю усієї мережі розподіленої криптовалюти Bitcoin [14].

Досліджено ряд програмних сервісів, що надають безкоштовний доступ до потужностей справжнього квантового комп'ютера. Незважаючи на це, імітаційне моделювання залишається актуальним інструментом для підготовки алгоритмів до виконання на реальному квантовому комп'ютері та для імітування роботи алгоритмів високої складності, для яких й досі не існує необхідних апаратних потужностей.

Список використаних джерел:

1.Душкин Р. В. Квантовые вычисления и функциональное программирование. / Р.В.Душкин – М: ДМК Пресс, 2014. - 270 с.

2.Leon Groot Bruinderink. Towards Post-Quantum Bitcoin / Leon Groot Bruinderink – Master's thesis, Eindhoven University of Technology, 2016. - [Електронний ресурс] - Режим доступу: http://repository.tue.nl/844305

3.Daniel J. Bernstein. Introduction to post-quantum cryptography. / Daniel J. Bernstein - Department of Computer Science, University of Illinois at Chicago. – 2009.

4.Andrew W. Cross, Lev S. Bishop, John A. Smolin, Jay M. Gambetta. Open Quantum Assembly Language. – Cornell University Library, 2017. - [Електронний ресурс] - Режим доступу: https://arxiv.org/abs/1707.03429

5. Kosuke Mitarai, Makoto Negoro, Masahiro Kitagawa, Keisuke Fujii. Quntum Circuit Learning. – Cornell University Library, 2017 – [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/1803.00745

6.List of QC simulators. - [Електронний ресурс] - Режим доступу: https://www.quantiki.org/wiki/list-qc-simulators

7.LIQUi|⟩ by Microsoft. - [Електронний ресурс] - Режим доступу: http://stationq.github.io/Liquid/

8.LIQUi|⟩ User's Manual. - [Електронний ресурс] - Режим доступу: https://msr-quarc.github.io/Liquid/LIQUiD.pdf

9.Maris Ozols. Clifford group / Maris Ozols – Essays at University of Waterloo – 2008.

10. Forest. - [Електронний ресурс] - Режим доступу: https://www.rigetti.com/index.php/forest

11. IBM Q Experience. - [Електронний ресурс] - Режим доступу: https://www.research.ibm.com/ibm-q

12. Quantum Playground by Google. [Електронний ресурс] - Режим доступу: http://www.quantumplayground.net

13. Quantum in the Cloud by The University of Bristol. - [Електронний ресурс] - Режим доступу: http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud

14. Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel. Quantum attacks on Bitcoin, and how to protect against them. – Cornell University Library, 2017 – [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/1710.10377