УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.03**

Є.Ю. КАПТЬОЛ, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ МОЖЛИВОСТЕЙ ТА ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ЗАДАЧ КРИПТОЛОГІЇ НА КВАНТОВОМУ КОМП'ЮТЕРІ

Вступ

Обґрунтовано вважається, що застосування квантового комп'ютера при вирішенні задач криптоаналізу щодо існуючих криптоперетворень асиметричного типу скоріше всього приведе до їх зламу. Але для цього ще потрібно розробити та виготовити квантові комп'ютери відповідної кубічної розрядності та розробити відповідне математичне та програмне забезпечення. Тому питання програмування задач взагалі криптології, особливо криптоаналізу, з орієнтацією на квантовий комп'ютер, стає все більш актуальним. Такі можливості появились завдяки успіхам у справі створення робочого варіанту екземпляру квантового комп'ютера [1 – 3]. Але, як виявилось, як математичне так і програмне забезпечення квантового комп'ютера є суттєво специфічними і не вкладаються в наші звичні рамки. В той же час, необхідність вирішення задач криптоаналізу на квантовому комп'ютері пояснюється його суттєвою перевагою перед класичним у швидкодії. Така перевага здебільшого базується на використанні квантовими комп'ютерами квантових властивостей, що є недоступними для класичних комп'ютерів. Наприклад, завдяки квантовим властивостям існує можливість розглядати одразу весь регістр замість одного елемента, як це робиться в класичному комп'ютері. Вказане дає суттєву перевагу в швидкодії обчислень.

Для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятору (до 32 кубітів) [6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Слід помітити, що ці гейти однокубітні та двохкубітні, а один з них трикубітний. Робоча реалізація методу Гровера в свою чергу потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності серед універсальних. Враховуючи вказане, необхідно виробити три схеми застосування методу Гровера на квантовому комп'ютері для квантового регістру з чотирьох кубітів для отримання квантового регістру.

Мета статі – обгрунтування підходів до аналізу можливостей та вивчення особливостей програмування задач криптоаналізу на квантових комп'ютерах, а також оцінка сучасного стану можливостей його реалізації на однокубітних, двохкубітних та трикубітному гейті.

1. Особливості та можливості квантового комп'ютера

Квантові комп'ютери, як показує аналіз, суттєво відрізняються від класичних самими принципами роботи. В них використовується специфічна квантова інформатика. Вона цілком базується на властивостях квантових об'єктів [1 – 3]: В першу чергу на здатності квантової частки приймати одночасно декілька станів завдяки квантової суперпозиції станів. Також суттєвими є здатність систем, що складаються з декількох квантових часток перебувати в переплутаних (корельованих) станах та нелокальність, що є їх наслідком. Важливим є вплив процесу вимірювання на стан вимірюваного об'єкта аж до його знищення, а також практична неможливість здійснити клонування квантових станів квантових часток.

Наведені вище властивості слідують з властивостей квантової фізики, вони є підґрунтям для квантової інформатики. Причому квантова фізика є складною в розумінні та відрізняється від класичної на принциповому рівні.

На основі квантових властивостей квантових об'єктів розроблено специфічну квантову математику, яку покладено в основу квантових алгоритмів криптоаналізу. Основні з них [4]:

- алгоритм Шора для здійснення факторизації надвеликих цілих чисел;
- алгоритми вирішення задач дискретного логарифму в скінченному полі;
- алгоритми дискретного логарифмування в групі точок еліптичних кривих;

- алгоритм пошуку в несортованій базі (Гровера);
- алгоритми криптоаналізу перетворень в кільцях поліномів та фактор-кільцях тощо.

Як правило, вказані алгоритми забезпечують вирішення задач, що є або неможливими для вирішення за допомогою класичних комп'ютерів, або нерентабельно складними з точки зору обчислювального ресурсу, що необхідний для отримання практичного результату [1 – 4]. Однією з властивостей квантових алгоритмів є те, що вони мають ймовірнісну природу, тобто результат можна отримати тільки з певною ймовірністю. Тобто проблемність вирішення задачі криптоаналізу в необхідності отримання, при вимірюванні стану квантового регістру після завершення роботи алгоритму, результату з необхідною ймовірністю.

Як теоретично, так і практично підтверджено, що застосування квантових алгоритмів на класичному комп'ютері не тільки не дає переваги, а є дуже невигідним з точки зору швидкодії [5]. Так, наприклад, реалізація методу Гровера на класичному комп'ютері є невигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазового повторення терації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори, в той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

Необхідно зазначити, що поява квантового комп'ютера, регістр котрого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є суттєво необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів. Достатність умови в тому, що окрім власне квантового комп'ютера необхідним ще є наявність відповідного математичного та програмного забезпечення, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням котрих можна провести криптоаналіз. Хоча, без сумнівів, створення квантового комп'ютера призведе до появи значної загрози для сучасних криптографічних систем з боку вже розроблених квантових алгоритмів, таких як алгоритми Гровера та Шора тощо.

2. Аналіз можливостей та наявності забезпечень для вирішення задач криптоаналізу

Таким чином, завдяки сучасним успіхам в створенні квантового комп'ютера існує можливість доступу до програмування квантового комп'ютера за допомогою хмарних сервісів. Так, для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 1, 5 та 15 кубітів [1, 6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Також можна скористатися квантовим симулятором (до 32 кубітів) [1, 6].

Наш практичний аналіз показав, що загальнодоступними для використання є однокубітні та двохкубітні, та один з них трикубітний гейти. Але робочі реалізації, наприклад методу Гровера, потребують наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності, тобто універсальних.

Наш пошук показав[1, 6], що серед доступних для загального доступу квантових комп'ютерів наявні: $ibmq\_16\_melbourne$ (15 кубітів), $ibmq\_london$ (5 кубітів), $ibmq\_burlington$ (5 кубітів), $ibmq\_essex$ (5 кубітів), $ibmq\_ourense$ (5 кубітів), $ibmq\_vigo$ (5 кубітів), $ibmq\_5\_yorktown - ibmqx2$ (5 кубітів), $ibmq\_armonk$ (1 кубіт). Квантовий симулятор $ibmq\_qasm\_simulator$ може використовуватись для реалізації алгоритмів, що передбачають використання регістрів з довжиною до 32 кубітів.

3. Особливість квантового програмування для методу Гровера

Одним з основних квантових методів, що є необхідними для вирішення задач криптології є метод Гровера. Розглянемо його детальніше.

Алгоритм Гровера будується з використанням методу Гровера, він є квантовим алгоритмом, що призначений для проведення вичерпного пошуку унікального елементу в несортованій базі даних, що містить $N = 2^n$ елементів, де n позначає довжину задіяного для представлення пошукового простору квантового регістру (кількість кубітів в ньому), а N є розміром пошукового простору [2, 5].

Особливість алгоритму Гровера полягає в тому, що, завдяки квантовим властивостям та використанню функції «чорної скриньки» (у вигляді квантового оракула), він потребує лише $O(\sqrt{N})$ групових операцій замість $O(N)$ у класичних алгоритмів. Квадратичне прискорення у порівнянні з класичними алгоритмами досягається завдяки використанню квантових властивостей, таких як квантова суперпозиція станів.

Хоча інші квантові алгоритми при порівнянні з класичними аналогами можуть забезпечити експоненційне прискорення, а алгоритм Гровера може забезпечити лише квадратичне прискорення, слід зауважити, що навіть таке прискорення є дуже значним та його значущість збільшується зі зростанням N. Для прикладу, методом Гровера 128-бітний криптографічний ключ можна зламати приблизно за 2^{64} звернень до функції «чорної скриньки», що можна визначити як 2^{64} звернень до ітерації Гровера, а отже 2^{64} ітерацій методу. В той же час як 256-бітний криптографічний ключ можна зламати за, приблизно, 2^{128} ітерацій. Виходячи саме з цього твердження для збільшення стійкості проти квантових атак іноді пропонують збільшувати довжину криптографічних ключів в два рази [3].

Метод Гровера, як і більшість квантових методів, є ймовірнісним, тобто правильна відповідь може бути виміряна з квантового регістру з певною ймовірністю, яка не повинна перевищувати 1. Також слід зауважити, що при виконанні більшого числа ітерацій, чим потрібно, ймовірність виміру правильного результату зменшується, тому це потрібно відповідним чином відслідковувати [5].

Метод Гровера має ряд можливостей для застосування, одним з котрих є реалізація його як алгоритму криптоаналізу симетричних перетворень, функцій гешування, асиметричного шифру в кільці поліномів тощо у зв'язку з його можливим узагальненим використанням [1, 5]. Для криптоаналізу симетричних блокових перетворень метод можна звести до алгоритму пошуку сеансового чи довгострокового ключа тощо. У випадку функцій гешування метод можна застосувати для пошуку колізій тощо. Метод Гровера має значні потенційні можливості, котрі беруться в розрахунок з огляду на сучасний стан розробки квантового комп'ютера.

4. Сутність та застосування методу Гровера

Для розуміння методу Гровера необхідно визначити квантову суперпозицію станів [1, 5]. Нехай $|\psi\rangle$ – суперпозиція всіх станів (згідно нотації Дірака):

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

З урахуванням цього алгоритм приймає такий вигляд:

1) Встановлення системи в стан суперпозиції $|\psi\rangle$.

2) Виконання «ітерації Гровера» (або ж G) $\frac{\pi}{4}\sqrt{N}$ разів, де $N = 2^n$ та N становить розмір пошукового простору, а n – розмір квантового регістру, що використовується для представлення пошукового простору. При цьому G включає в себе два етапи:

- застосування квантового оракула (O);
- застосування оператора дифузії, що здійснює «інверсію щодо середнього» та має вигляд $2|0\rangle\langle 0|-I$.

3) Виконання класичних вимірювань регістру для отримання результату роботи алгоритму, що з ймовірністю близькою до 1 буде вірним.

Практичний приклад

З метою демонстрації дії методу Гровера на практиці розглянемо приклад використання алгоритму пошуку несортованою базою даних з невеликим розміром пошукового простору, як було зроблено в [5].

Приклад [5]. Припустимо, що система може приймати $N = 72057594037927936 = 2^{56}$ станів, що означає, що база для пошуку складається з 72057594037927936 елементів. Також припустимо, що стан системи, котрий ми хочемо отримати в результаті пошуку, x_0, має індекс 234.

1) Для опису системи необхідно $n = 56$ кубітів. Згідно з алгоритмом Гровера ініціалізуємо квантовий регістр, що складатиметься з $n = 56$ кубітів, що є необхідною умовою для представлення пошукового простору, що має розмір $N = 2^{56}$, встановивши регістр у початковий стан, що має наступний вигляд:

$$|\psi_0\rangle = |000...000\rangle,$$

де кількість нулів дорівнює 56.

2) Проведемо перетворення Адамара, що дозволяє встановити систему в стан квантової суперпозиції, що робить значення амплітуди, що пов'язана з кожним станом, таким, щоб ймовірність перебування в кожному з 2^{56} можливих станів була рівною. Цей крок матиме наступний вигляд:

$$|\psi\rangle = H^{\otimes 56}|000...000\rangle = (H|0\rangle)^{\otimes 56} = \frac{1}{268435456}\sum_{i=0}^{2^{56}}|i\rangle$$

Таким чином, маємо квантовий регістр, встановлений в стан суперпозиції, що геометрично можна представити як наведено на рис. 1.

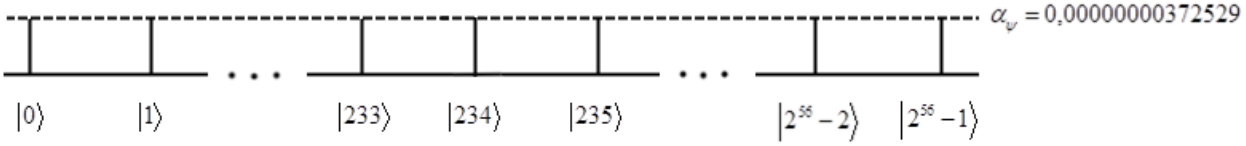

Рис. 1. Геометричне представлення регістру з 256 кубітів в стані суперпозиції

3) Визначаємо кількість потрібних ітерацій G:

$$\frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{2^{56}} = \frac{2^{28}\pi}{4} \approx 210828714{,}133156$$

Далі для використання в розрахунках округлимо число ітерацій до 210828714 у зв'язку з округленням вниз.

4) Після цього визначимо

$$|u\rangle = \frac{1}{\sqrt{2^{56}-1}}\sum_{\substack{i=0\\ i\neq 301}}^{2^{56}-1}|i\rangle = \frac{|0\rangle+|1\rangle+...+|2^{56}-2\rangle+|2^{56}-1\rangle}{\sqrt{2^{56}-1}}.$$

Також маємо, що

$$|\psi\rangle = \frac{\sqrt{2^{56}-1}}{2^{28}}|u\rangle + \frac{1}{2^{28}}|234\rangle.$$

5) Далі, зі здійснення звернення до оракула починається перша ітерація. Після застосування оракула маємо

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{2*2^{28}}|234\rangle = |\psi\rangle - \frac{1}{536870912}|234\rangle.$$

Стан даного регістру після застосування оракула під час першої ітерації Гровера має геометричне відображення, що наведено на рис. 2.

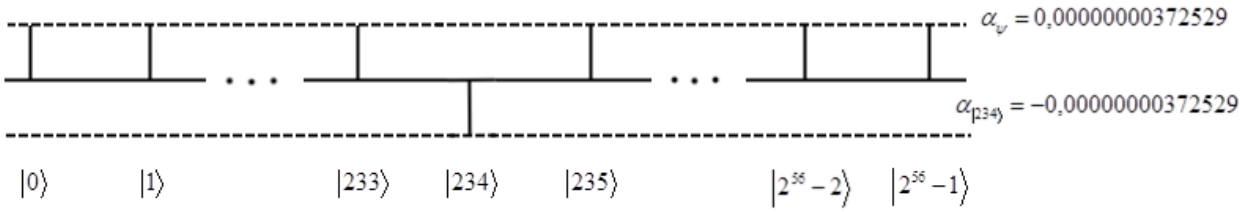

Рис. 2. Геометричне відображення стану регістру після застосування оракула під час першої ітерації G

Далі відбувається виконання оператора дифузії, в результаті чого отримуємо:

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle = 0{,}9999999999999999861|\psi\rangle + 0{,}0000000018626|234\rangle;$$

Геометричне відображення стану регістру після першої ітерації зображено на рис. 3.

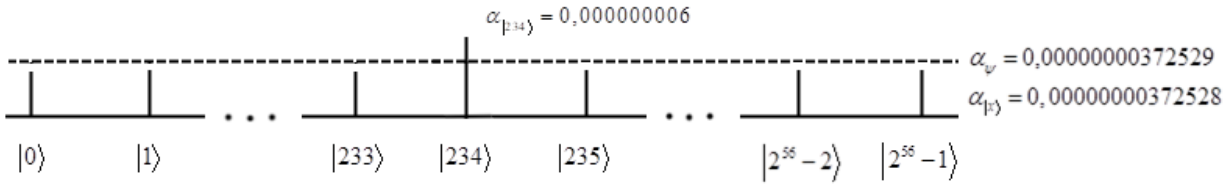

Рис. 3. Геометричне представлення стану квантового регістру після проведення першої ітерації G.

Далі аналогічним чином проводиться ще 210828713 ітерацій.

Під час проведення останньої, 210828714-й ітерації маємо в результаті застосування оракула:

$$|\psi_{421657427}\rangle = 0{,}00000000000003|\psi\rangle - 0{,}9999999999999841|234\rangle.$$

Стан даного регістру після застосування оракула під час останньої ітерації Гровера має геометричне відображення, що наведено на рис. 4.

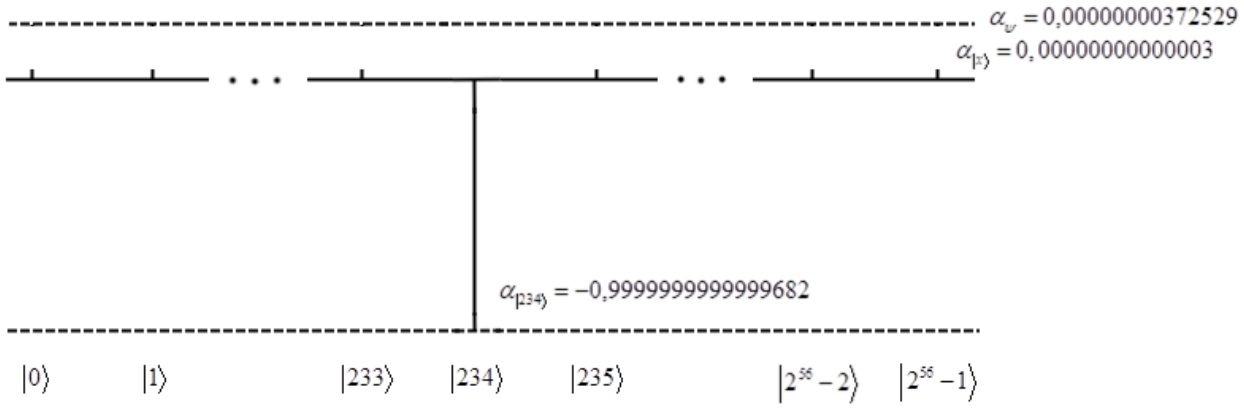

Рис. 4. Геометричне відображення стану регістру після застосування оракула під час останньої ітерації G

Після застосування оператора дифузії під час останньої ітерації маємо:

$$|\psi_{421657428}\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_{421657427}\rangle = -0{,}00000000000001|\psi\rangle + 0{,}9999999999999841|234\rangle$$

Геометричне представлення результатів останньої ітерації наведено на рис. 5.

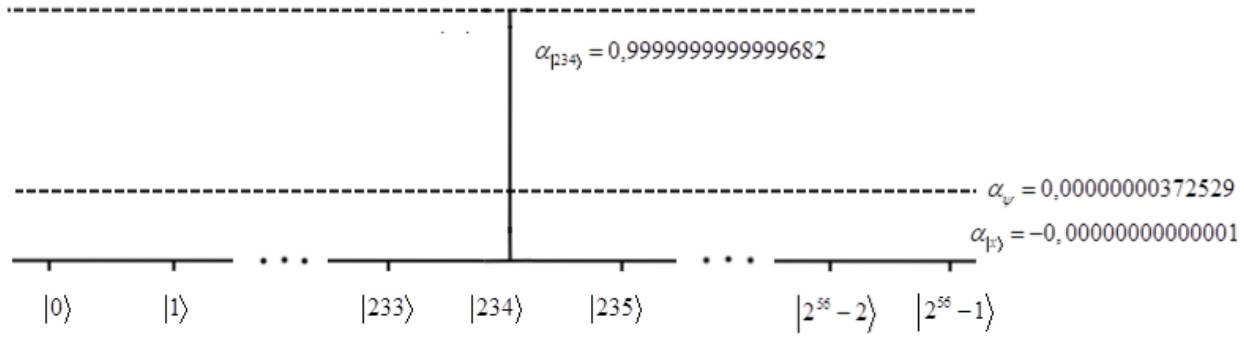

Рис. 5. Геометричне представлення стану квантового регістру після проведення останньої ітерації G

Ймовірність отримання потрібного елементу в результаті вимірювання регістру після проведення дванадцяти ітерацій становить:

$$P \approx |0{,}9999999999999841|^2 \approx 0{,}9999999999999682 \approx 99{,}99999999999682\%.$$

Таким чином, на цьому прикладі, враховуючи попередні, можна побачити, що зі зростанням N похибка дійсно стає незначною.

Також слід зазначити, що приклад було розраховано з використанням програмної моделі проведення пошуку методом Гровера, що була модернізована на швидкодію. В загальному вигляді програмна модель, використана для розрахунків, відповідає загальній програмній моделі методу Гровера, але відрізняється тим, що оракул було спрощено до елементарної функції пошуку, що також проводилася повністю лише в частині відповідальній за ініціалізацію. Така побудова моделі дозволила провести розрахунки без вирішення складної задачі пошуку, але зі збереженням достовірності результатів розрахунків на рівні, що відповідає рівню достовірності результатів програмної моделі, що проводить виконання складної задачі пошуку.

5. Схеми застосування методу Гровера на квантовому комп'ютері для квантових регістрів з використанням хмарних сервісів

Для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятору (до 32 кубітів) [6].

Вони виконують квантові операції та можуть реалізовувати квантові гейти. Слід помітити, що ці гейти однокубітні та двохкубітні, а один з них трикубітний. Робоча реалізація методу Гровера в свою чергу потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності серед універсальних.

З урахуванням наведеного було вироблено три схеми застосування методу Гровера на квантовому комп'ютері для квантового регістру з чотирьох кубітів для отримання результату «0», що може бути представлено рядком бітів $|0000\rangle$, та три схеми для отримання результату 4, що може бути представлено рядком бітів $|0100\rangle$. Схеми відрізняються кількістю застосування ітерацій Гровера. Так, в перших схемах застосовується одна ітерація Гровера, в других – дві ітерації, в третіх – три ітерації. Ці схеми було випробувано на доступних для загального доступу тестових квантових комп'ютерах компанії IBM та доступному через той же сервіс квантовому симуляторі [6]. Серед квантових комп'ютерів, що використані в дослідженні, були: $ibmq\_16\_melbourne$, $ibmqx2$ (він же $ibmq\_5\_yorktown - ibmqx2$), $ibmq\_burlington$. Квантовий симулятор $ibmq\_qasm\_simulator$ може розраховувати схеми, що передбачає використання до 32 кубітів.

Як вже було зазначено, особливості реалізації метода Гровера для квантового регістру, що складається з чотирьох кубітів на квантовому комп'ютері, включають в себе необхідність застосування 3-кубітних квантових гейтів. В той же час інструментарій для взаємодії з доступними квантовими комп'ютерами не включає в себе квантові гейти, що оперують над потрібною кількістю кубітів. Потрібні квантові гейти можна замінити сукупностями наявних в інструментарії квантових гейтів, що дають той самий ефект.

Результати виконаних випробувань можуть вказувати як на недосконаліть методів, використаних для представлення багатокубітних гейтів у вигляді сукупності одно- та двокубітних гейтів, так і на недосконаліть розроблених квантових комп'ютерів, що має бути перевірено в майбутніх дослідженнях.

Результати застосування методу Гровера з однією ітерацією для отримання $|0000\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0000\rangle$ становить 46,875 %, в той час як при проведенні реальних вимірювань цей результат було отримано лише 6,152% разів на $ibmq\_burlington$, 7,52 % – на $ibmqx2$ та 8,789 % – на $ibmq\_16\_melbourne$ квантових комп'ютерах.

Результати застосування методу Гровера з двома ітераціями для отримання $|0000\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0000\rangle$ становила 91,211 %, в той час як насправді було отримано лише 6,543 % на $ibmq\_burlington$, 8,398 % на $ibmqx2$ та 10,156 % на $ibmq\_16\_melbourne$ квантових комп'ютерах.

Результати застосування методу Гровера з трьома ітераціями (що є остаточною кількістю ітерацій для регістру цього розміру) для отримання $|0000\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, Симулятор спрогнозував ймовірність отримання $|0000\rangle$ в 96,387 %, в той час як на реальних квантових комп'ютерах було отримано потрібний результат значно меншу кількість разів: 7,227 % – на $ibmq\_burlington$, 8,301 % – на $ibmqx2$, 9,961 % – на $ibmq\_16\_melbourne$ квантовому комп'ютері.

Результати застосування методу Гровера з однією ітерацією для отримання $|0100\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0100\rangle$ становить

46,387 %, в той час як при проведенні реальних вимірювань цей результат було отримано лише 5,469 % разів на *ibmq_burlington*, 10,547 % – на *ibmqx*2 та 6,506 % – на *ibmq_16_melbourne* квантових комп'ютерах.

Результати застосування методу Гровера з двома ітераціями для отримання $|0100\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0100\rangle$ становила 90,259 %, в той час як насправді було отримано лише 6,006 % на *ibmq_burlington*, 6,982 % на *ibmqx*2 та 6,897 % на *ibmq_16_melbourne* квантових комп'ютерах.

Результати застосування методу Гровера з трьома ітераціями для отримання $|0100\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, Симулятор спрогнозував ймовірність отримання $|0100\rangle$ в 96,436 %, в той час як на реальних квантових комп'ютерах було отримано потрібний результат за значно меншу кількість разів: 6,299 % – на Бурлінгтонському, 6,152 % – на Йорктаунському, 7,837 % на Мельбурнському квантовому комп'ютері.

Детальніше результати випробувань розроблених схем на квантових комп'ютерах наведено в табл. 1 – 6.

Таблиця 1

Результати застосування методу Гровера з однією ітерацією для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	46,875	6,152	7,52	8,789
0001	4,395	6,543	6,934	6,25
0010	2,832	6,738	5,566	7,031
0011	3,809	5,664	8,691	5,664
0100	3,613	8,594	6,445	5,566
0101	2,637	5,957	4,688	6,836
0110	3,125	6,543	4,004	4,98
0111	3,906	5,176	10,742	6,348
1000	2,539	7,422	7,422	7,52
1001	4,199	6,738	4,688	7,031
1010	2,832	7,031	4,59	6,641
1011	2,637	5,371	7,715	5,957
1100	5,566	6,934	4,199	5,273
1101	3,809	5,762	4,492	5,957
1110	3,223	3,906	4,883	5,566
1111	4,004	5,469	7,422	4,59

Таблиця 2

Результати застосування методу Гровера з двома ітераціями для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	91,211	6,543	8,398	10,156
0001	0,781	6,25	6,152	6,641
0010	0,391	6,25	5,371	6,348
0011	0,391	8,398	8,008	5,566
0100	0,684	5,762	8,594	7,227
0101	0,586	6,641	5,176	7,422
0110	0,488	6,152	4,98	5,762
0111	0,586	7,324	7,813	4,395
1000	0,195	6,445	6,348	6,738
1001	0,586	6,152	4,004	6,641
1010	0,684	5,273	4,492	5,273
1011	0,586	5,957	7,715	4,102
1100	0,684	5,273	6,738	7,422
1101	0,879	6,152	3,906	5,664
1110	0,488	5,566	5,664	6,348
1111	0,781	5,859	6,641	4,297

Таблиця 3

Результати застосування методу Гровера з трьома ітераціями для отримання $|0000\rangle$

Значення	Симулятор (1024 повтори), %	Бурлінгтон (1024 повтори), %	Йорктаун (1024 повтори), %	Мельбурн (1024 повтори), %
0000	96,387	7,227	8,301	9,961
0001	0,391	7,91	2,93	5,371
0010	0,098	6,836	6,641	8,496
0011	0,586	6,836	6,641	5,664
0100	0,195	5,664	7,715	5,859
0101	0,098	6,738	3,613	6,641
0110	0,098	6,543	7,031	5,762
0111	0,195	6,055	7,422	6,348
1000	0,195	5,859	8,594	10,742
1001	0,293	4,98	3,613	4,59
1010	0,098	5,371	5,566	6,641
1011	0,391	7,617	8,105	3,613
1100	0,098	5,566	7,227	5,859
1101	0,195	5,957	3,223	5,469
1110	0,391	5,078	6,445	4,395
1111	0,293	5,762	6,934	4,59

Таблиця 4

Результати застосування методу Гровера з однією ітерацією для отримання $|0100\rangle$

Значення	Симулятор (4096 повторів), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	3,589	8,691	7,666
0001	3,247	6,909	6,348
0010	4,053	5,859	5,811
0011	3,003	5,151	4,541
0100	46,387	5,469	10,547
0101	3,125	5,322	8,398
0110	3,076	5,957	7,666
0111	3,906	6,567	7,153
1000	3,955	9,839	3,687
1001	4,321	6,47	6,274
1010	3,516	6,03	2,881
1011	3,198	5,151	6,396
1100	3,296	5,859	4,321
1101	3,54	5,005	8,252
1110	4,175	5,591	3,296
1111	3,613	6,128	6,763

Таблиця 5

Результати застосування методу Гровера з двома ітераціями для отримання $|0100\rangle$

Значення	Симулятор (4096 повтори), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	0,537	7,861	6,738
0001	0,537	5,981	6,982
0010	0,635	8,179	3,711
0011	0,659	6,934	3,54
0100	90,259	6,006	6,982
0101	0,464	5,64	7,495
0110	0,684	6,616	4,175
0111	0,586	5,981	3,833
1000	0,781	7,3	5,688
1001	0,61	5,884	5,908
1010	0,659	5,688	8,862
1011	0,732	6,274	7,446
1100	0,659	5,493	6,03
1101	0,708	5,566	6,03
1110	0,757	5,396	8,423
1111	0,732	5,2	8,154

Таблиця 6

Результати застосування методу Гровера з трьома ітераціями для отримання $|0100\rangle$

Значення	Симулятор (4096 повтори), %	Бурлінгтон (4096 повтори), %	Йорктаун (4096 повтори), %
0000	0,22	7,52	6,299
0001	0,244	6,152	6,177
0010	0,244	6,519	3,784
0011	0,122	5,859	9,131
0100	96,436	6,299	6,152
0101	0,244	6,543	6,323
0110	0,22	6,152	3,467
0111	0,171	5,249	7,91
1000	0,391	6,738	5,762
1001	0,244	6,177	5,957
1010	0,269	5,615	3,711
1011	0,22	6,909	8,862
1100	0,195	6,641	6,738
1101	0,269	6,47	6,055
1110	0,269	5,615	3,76
1111	0,244	5,542	9,912

Висновки

1. Подальший розвиток вимагає вдосконалення представлення багатокубітних гейтів шляхом використання одно- та двокубітних гейтів, а також вдосконалення оснастки для роботи з квантовими комп'ютерами та розробки багатокубітних гейтів та впровадження їх у діючі зразки квантових комп'ютерів.

2. Хоча квантовий симулятор вказує на те, що схеми повинні надавати правильний результат із ймовірністю близькою до максимальної, результати реальних експериментів не є навіть близько такими вдалими.

3. Реалізація методу Гровера на класичному комп'ютері є невигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазового повторення терації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори, в той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими.

4. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

5. Необхідно також зазначити, що поява квантового комп'ютера, регістр котрого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є суттєво необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів.

6. Достатність умови в тому, що окрім власне квантового комп'ютера, необхідним ще є наявність відповідного математичного та програмного забезпечень, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням котрих можна провести криптоаналіз.

7. Можна стверджувати, що створення квантового комп'ютера призведе до появи значної загрози для сучасних криптографічних систем з боку вже розроблених квантових алгоритмів, таких як алгоритми Гровера та Шора тощо.

8. Питання програмування задач взагалі криптології, особливо криптоаналізу, з орієнтацією на квантовий комп'ютер, стає все більш актуальним. Такі можливості появились завдяки успіхам у справі створення робочого варіанту екземпляру квантового комп'ютера [1 – 4, 6].

9. З метою демонстрації дії методу Гровера на практиці розглянемо приклад використання алгоритму пошуку несортованою базою даних з невеликим розміром пошукового простору, як було зроблено в [1, 5].

10. Але, як виявилось, як математичне так і програмне забезпечення квантового комп'ютера є суттєво специфічними і не вкладаються в наші звичні рамки. В той же час, необхідність вирішення задач криптоаналізу на квантовому комп'ютерові пояснюється його суттєвою перевагою перед класичним у швидкодії

11. З отриманих результатів можна зробити висновок, що нинішні квантові комп'ютери ще не здатні на повноцінне контрольоване відтворення всіх квантових властивостей. Хоча можливо з більшою кількістю кубітів метод Гровера і даватиме кращий результат, що буде перевірено подальшими дослідженнями.

13. Причини таких результатів та можливість отримання кращих результатів підлягають подальшим дослідженням.

Список літератури:

1. Квантовые компьютеры. [Електронний ресурс]. Режим доступу: http://www.nkj.ru/archive/articles/5309/.
2. Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996. URL: https://arxiv.org/pdf/quant-ph/9605043.pdf
3. Feyman R. P. Quantum mechanical computers // Opt. News. 1985. February, 11. pp. 11-39.
4. Горбенко І. Д. Прикладна криптологія / І. Д. Горбенко, Ю. І. Горбенко. Харків : Форт, 2012. 868 с.
5. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І. Горбенко, Є. Ю. Каптьол // Радіотехніка. 2018. Вип. 195. С. 89-100.
6. IBM Quantum Experience Dashboard. [Електронний ресурс]. Режим доступу: https://quantum-computing.ibm.com/

Надійшла до редколегії 11.08.2020

Відомості про авторів:

Каптьол Євген Юрійович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: gorbenkoivan03@gmail.com, ORCID: https://orcid.org/0000-0003-4616-3449