УДК 004.383

М.М. САВЧУК, А.В. ФЕСЕНКО

КВАНТОВІ ОБЧИСЛЕННЯ: ОГЛЯД ТА АНАЛІЗ

Анотація. Зроблено огляд та аналіз основних понять і положень квантової моделі обчислень, ефективних квантових алгоритмів, останніх результатів, можливостей та перспектив у побудові масштабованого квантового комп'ютера. Розглянуто певний клас алгебраїчних задач у квантовій моделі обчислень, для яких існує ефективний квантовий алгоритм розв'язку. Проведено детальний аналіз наявних практичних реалізацій квантового комп'ютера. Показано, що на сьогодні немає достатнього прогресу у побудові масштабованого квантового обчислювального пристрою, проте більшість дослідників очікують на створення повноцінного квантового комп'ютера впродовж наступних 10–15 років.

Ключові слова: квантова модель обчислень, квантова криптографія, квантовий комп'ютер, ефективні квантові алгоритми, постквантові криптографічні примітиви.

ВСТУП

Нам пощастило бути свідками і сучасниками великих теоретичних відкриттів та практичних винаходів і досягнень в інформаційній сфері, які змінили все наше життя, наш світ та його розуміння. Навіть важко уявити, які нові зміни очікують нас уже в найближчому майбутньому завдяки новим досягненням у галузі телекомунікацій, класичних комп'ютерних та квантових обчислень.

Очевидно, що рівень розвитку суспільства в економічній та інших сферах його життя безпосередньо залежить від обсягу інформації, якою можуть активно користуватися різні прошарки суспільства, від уміння її ефективно зберігати, швидко обробляти та передавати. Нагадаємо, що рівні розвитку суспільства і раніше були тісно пов'язані з інформаційними революціями. Так, формування родоплемінного укладу пов'язано з виникненням і розвитком мов, мовного спілкування; створення держав давнього світу відбувалося одночасно з винаходженням і розвитком систем писемності, які давали змогу здійснювати довгострокове зберігання інформації на матеріальних носіях, її ефективну передачу в просторі і часі; європейські відродження і промислова революція пов'язані з книгодрукуванням, яке в десятки тисяч разів збільшило обсяг інформації, що використовувалася. За різними оцінювальними даними орієнтовна кількість інформації, яку після зазначених інформаційних революцій використовувало суспільство, становила відповідно 10^9, 10^{11}, 10^{17} бітів інформації.

На початку сучасної інформаційної ери перша електронна цифрова обчислювальна машина ЕНІАК (1945 р.) важила 27 тонн, споживала 174 кВт, маючи обсяг пам'яті 20 число-слів і тактову частоту 100 кГц. Цікаво, що через чотири роки у книзі 1949 р. «Популярна механіка» було дано такий прогноз: «комп'ютери майбутнього можуть важити не більше 1,5 тонн». Нині мініатюризація та швидкодія цифрових обчислювальних пристроїв досягли рівня, який дає змогу говорити про інтелектуальні системи з майже фантастичними можливостями, і межа в цьому напрямку ще не досягнута. Припустимо, що розмір процесора досягне розміру атома водню діаметром близько 10^{-10} м. Тоді частота процесора буде не більшою ніж число разів проходження світлом шляху через атом за 1 секунду, що дорівнюватиме $3 \cdot 10^{18}$ операцій на секунду або приблизно 10^{26} операцій на рік. Цього не достатньо, щоб зламати, наприклад, асиметричну криптосистему RSA з довжиною модуля 1024 біта. А криптосистему RSA з довжиною модуля 2048 бітів навіть такий комп'ютер не зламає протягом мільярда років не-

перервної роботи. Причому тут, як і в задачах з експоненціальним зростанням складності в загальному випадку, розпаралелювання не допоможе. На сьогодні найшвидші суперкомп'ютери мають швидкодію близько 10^{17} флопс. Чи буде обмежено людство в обчисленнях тільки задачами поліноміальної складності?

Альтернативною обчислювальною моделлю є квантова модель обчислень, яку можна буде повноцінно застосовувати на практиці після створення масштабованого квантового комп'ютера. У цій статті проведено аналіз основних теоретичних понять, ідей щодо обґрунтування квантових обчислень та перспектив побудови масштабованого квантового комп'ютера.

1. КВАНТОВА КРИПТОГРАФІЯ

Квантовими обчисленнями вважають не тільки обчислення на квантовому комп'ютері. До цієї сфери відносять також квантову криптографію, квантову телепортацію та інші напрямки. У традиційній криптографії носієм інформації під час передачі є імпульси струму, світла, пучки радіохвиль, зрештою, папір та інші матеріальні носії. Для представлення і кодування одного біта інформації кожного разу використовується величезна кількість електронів, фотонів, радіохвиль, частинок. У квантовій криптографії для кодування одного біта зазвичай використовується квантовий стан однієї елементарної частинки (атома, іона, електрона, фотона) або їх пари.

На відміну від традиційної криптографії, у якій використовуються математичні методи перетворення текстів і повідомлень для забезпечення їхньої захищеності від зловмисника та збереження секретності інформації, в основу квантової криптографії для захисту інформації покладено фізичні процеси та закони квантової механіки, а кодування та перенесення інформації здійснюється за допомогою об'єктів квантової механіки, наприклад, за допомогою електронів у електричному струмі або фотонів у лініях волоконно-оптичного зв'язку. Приймання повідомлень, або підслуховування (перехоплення повідомлення) можна розглядати як вимірювання певних параметрів квантових об'єктів–переносників інформації.

Вперше ідея захисту інформації з використанням квантових об'єктів була запропонована С. Візнером у 1970 р. Перший та найбільш відомий протокол квантової криптографії BB84, запропонований Ч. Беннетом і Ж. Брассаром в 1984 р. на основі ідей С. Візнера, дає змогу розв'язати проблему симетричної криптографії — передачу таємного ключа з використанням лише відкритих каналів зв'язку [1]. У 70-х роках XX століття у зв'язку з бурхливим розвитком комп'ютерних мереж, телекомунікаційних каналів, експоненціальним зростанням кількості інформації та потребою в її захисті майже в усіх галузях передача ключів спеціальними закритими каналами стала проблемою, яка здавалася нерозв'язною. У 1976 р. У. Діффі та М. Хеллман чітко сформулювали поняття важкооборотної функції та важкооборотної функції з лазівкою і запропонували нову концепцію в криптографії — асиметричну криптографію або криптографію з відкритими ключами. Першим протоколом асиметричної криптографії був саме протокол розповсюдження ключів відкритими каналами, які у симетричній криптографії використовувалися для криптографічних перетворень захисту інформації. Квантовий протокол розповсюдження ключів побудовано на основі інших принципів.

Задача квантового протоколу розповсюдження ключів BB84 — без використання закритих каналів передати від відправника A до одержувача B випадкову послідовність нулів та одиниць, з якої потім користувачі A і B обирають таємний ключ. Згенерована відправником A двійкова випадкова послідовність, кожний символ якої 0 і 1 кодується напрямком поляризації одиничного фотона (напрямком коливань електричного поля фотона), передається послідовністю фотонів волоконно-оптичною лінією. Напрямком поляризації фотонів можна керувати та вимірювати його, наприклад, за допомогою оптично активних кристалів.

Послідовність бітів передається послідовністю фотонів у базисі, обраному відправником А випадковим чином для кожного біта — прямокутному або діагональному. У прямокутному базисі 0 або 1 кодуються горизонтальним та вертикальним напрямком поляризації фотона, а в діагональному — з нахилом під кутом 45 та 135 градусів. Фактично до вимірювання інформація знаходиться у квантових бітах — кубітах і лише після вимірювання перетворюється у звичайні класичні біти. Одержувач В обирає для вимірювання випадковим чином свою послідовність базисів. Якщо базиси у користувачів А і В для окремого фотона збігаються, то під час вимірювання В отримає той самий символ послідовності (0 або 1), який був відправлений користувачем А. Якщо базиси А і В не збігаються, то відповідні символи у А і В будуть однаковими з імовірністю 0.5 за законами квантової фізики. Після вимірювання А і В, використовуючи будь-який відкритий канал, з'ясовують, які базиси у них збіглися. За відсутності прослуховування зловмисником у середньому користувачі А і В матимуть 50% однакових символів вихідної послідовності, з якої обираються таємні ключі для симетричних систем шифрування користувачів А і В.

Стійкість квантового протоколу передачі таємного ключа зумовлена тим, що факт підключення до волоконно-оптичної лінії і прослуховування несанкціонованою особою може бути гарантовано виявлений користувачами А і В. Це, своєю чергою, забезпечується законами квантової механіки та обміном між А і В після квантової передачі певною уточнювальною інформацією з використанням будь-якого відкритого каналу. Зловмисник не знає обраних користувачем А базисів, тому під час прослуховування будуть спотворені також ті символи у одержувача В, які за умови обрання користувачами А і В однакових базисів мають збігатися, що буде виявлено користувачами. У цьому разі отримана користувачами А і В послідовність не використовується. Якщо не було спроби прослуховування, то частиною послідовності можна скористатися як таємним ключем (відомим лише відправнику і одержувачу) і застосовувати її надалі у симетричних криптосистемах.

Перша реалізація квантового протоколу на фізичному пристрої відбулася в 1989 р. з передачею на відстань, що становила менше ніж один метр. Пізніше дальність передачі неодноразово збільшувалась. Нині передача вважається достатньо стабільною на відстань, як правило, до 200 км. Дальність передачі перш за все обмежується затуханням світлових сигналів у волоконно-оптичних кабелях і втратою фотонів, а також зовнішніми завадами.

З появою квантової криптографії її ентузіасти прогнозували, що невдовзі квантова криптографія створить конкуренцію для «звичайної» криптографії і навіть буде більш надійною та ефективною. Але поки що це не сталося передусім через низку технічних труднощів. Так, наприклад, якщо в класичних інформаційних передачах волоконно-оптичними каналами через кожні декілька десятків кілометрів обов'язково ставлять електронні або оптичні підсилювачі, то зробити це в квантовому протоколі BB84 неможливо, бо стан фотона, не знаючи базисів відправника А, відтворити після вимірювання неможливо за квантовими законами. Це відразу накладає жорсткі обмеження на дальність передачі. На сьогодні найбільша відстань, досягнута у разі передачі за квантовим протоколом волоконно-оптичними каналами, становить 404 км.

Інший тип квантового криптографічного протоколу базується на заплутаних квантових станах двох частинок, наприклад, фотонів. Зараз у різних країнах проводять інтенсивні дослідження квантового зв'язку, квантових криптографічних протоколів з використанням штучних супутників. Дальність квантових передач з використанням супутників сягає сотень кілометрів і навіть перевищує тисячі кілометрів. Це відкриває нові перспективи для розвитку квантового зв'язку та квантової криптографії.

2. ОСНОВНІ ПОНЯТТЯ КВАНТОВОЇ МОДЕЛІ ОБЧИСЛЕНЬ

2.1. Хронологія ідей та перших положень. У збірці [2] представлено дев'ять класичних робіт у галузі квантових комп'ютерів та квантових обчислень, у тому числі роботи Д. Дойча, Д. Джози та П. Шора, присвячені дослідженню ефективних квантових алгоритмів. Стисло відзначимо основні етапи теорії побудови квантового комп'ютера та квантових алгоритмів:

• 1980 р. — Ю.І. Манін у вступі до книги «Обчислюване та не обчислюване» («Вычислимое и невычислимое») висунув ідею квантових автоматів;

• 1982 р. — П. Беніоф і Р. Фейнман проаналізували фізичні обмеження та можливість побудови квантового комп'ютера (квантовий імітатор);

• 1985 р. — Д. Дойч надав ідеї Р. Фейнмана конкретну форму — ефективність у разі квантового паралелізму;

• 1992 р. — Д. Дойч та Д. Джоза запропонували алгоритм розв'язання задачі про розрізнення (розпізнавання) сталої та збалансованої булевих функцій від n змінних за n операцій на квантовому комп'ютері;

• 1994 р. — П. Шор розробив алгоритми факторизації і дискретного логарифмування, які дають змогу розв'язати відповідні задачі за поліноміальний час на квантовому комп'ютері;

• 1996 р. — Л. Гровер розробив квантовий алгоритм пошуку в неупорядкованій множині, зокрема його алгоритм забезпечує розв'язання задачі перебору, наприклад, знаходження розв'язку рівняння $f(x)=1$ для булевої функції f від n змінних за $O(2^{n/2})$ звернень до обчислення функції f з використанням $O(n)$ кубітів.

З детальною інформацією про наведені етапи розвитку, основи теорії квантових обчислень, сучасні дослідження, перспективи побудови квантового комп'ютера та можливі наслідки для суспільства і розуміння фізичних та інформаційних процесів можна ознайомитись у монографіях [2–4]. Стислий опис результатів досліджень київської школи теоретичної криптографії у цій галузі представлено в роботі [5].

2.2. Квантові стани та загальна концепція квантових обчислень.

Однокубітна квантова система. У квантовому комп'ютері одиницею інформації є кубіт (квантовий біт), фізична реалізація якого описується хвильовою функцією ймовірностей у двовимірному гільбертовому просторі.

Один класичний біт може перебувати тільки в одному з двох станів, які позначаються (кодуються) 0 та 1. Стан квантового біта (кубіта) описують з використанням бра і кет позначень Дірака за допомогою виразу $|\psi\rangle = a|0\rangle + b|1\rangle$, де a і b — комплексні числа, а $|a|^2+|b|^2=1$. Так би мовити, кубіт одночасно перебуває в усіх точках простору, але з різною ймовірністю. У результаті вимірювання кубіта, яке фактично є проекцією на ортогональні підпростори, отримаємо закодоване значення класичного біта: 0 з імовірністю $|a|^2$ або 1 з імовірністю $|b|^2$. Таким чином, після вимірювання кубіт відразу переходить в один з базисних станів, що відповідає класичному результату. Наприклад, після вимірювання кубіта, який описується станом $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$, отримуємо відповідне значення 0 з імовірністю 0,36 та значення 1 з імовірністю 0,64.

Квантова система з двома та більшим числом кубітів. Стан системи з двох кубітів математично може бути записаний як одиничний вектор у 4-вимірному гільбертовому просторі $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, де a, b, c, d — комплексні числа і $|a|^2+|b|^2+|c|^2+|d|^2=1$. Базисними квантовими станами є $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, які відповідають чотирьом класичним значенням 00, 01, 10 та 11, кожне з яких після повного вимірювання має ймовірність $|a|^2$, $|b|^2$, $|c|^2$, $|d|^2$ відповідно. Аналогічно система, яка містить N кубітів, описується в 2^N-вимірному гільбертовому просторі та матиме 2^N базисних станів, які відповідають 2^N класич-

ним значенням. Таким чином, результатом повного вимірювання N-кубітної квантової системи буде одне з 2^N різних класичних значень, загальна кількість яких експоненціально зростає відносно числа кубітів, і кожне значення може бути отримано в результаті вимірювання з деякою ймовірністю. Нехай існує послідовність перетворень квантової системи, які можна реалізувати фізично, така, що суттєво збільшить імовірність стану, який відповідає шуканому розв'язку цієї задачі. Тоді така квантова система може після багатократної реалізації та вимірювання знайти з високою ймовірністю відповідь на можливо непосильну для класичного комп'ютера задачу.

Загальна концепція квантових обчислень. Спрощену схему обчислення можна описати так. Система з достатнім числом спільно працюючих кубітів переводиться в певний початковий стан, що відповідає умовам задачі. Далі стан системи або її підсистем змінюється шляхом застосування послідовності перетворень, яким у математичній моделі відповідають унітарні перетворення в гільбертовому просторі (унітарні матриці). У певному розумінні квантова система паралельно виконує обчислення з усіма можливими класичними станами, число яких зростає експоненціально зі збільшенням числа кубітів, а відповіддю є єдине класичне значення. Після застосування всіх унітарних перетворень, як правило, виконується вимірювання стану системи і отримане класичне значення є результатом обчислень. Зазвичай, квантова система дає правильний результат тільки з певною ймовірністю. Для збільшення довірчої ймовірності обчислення і відповідні вимірювання повторюють потрібну кількість разів. Цю ймовірність, якщо помилки під час вимірювання не зростають дуже швидко (наприклад, експоненціально зі збільшенням числа кубітів), можна зробити як завгодно близькою до одиниці. Можна сказати, що ця квантова система є аналоговим квантовим комп'ютером.

Така концепція квантового комп'ютера і квантових вентилів — простих унітарних перетворень, які відповідають логічним операціям у класичному комп'ютері, була запропонована Д. Дойчем у 1989 р. У 1995 р. Д. Дойч винайшов універсальний логічний блок, за допомогою якого можна виконати будь-які квантові обчислення. Виявляється, що для побудови алгоритму будь-якого обчислення достатньо двох базових операцій — квантових вентилів.

Теоретично квантовий комп'ютер дає змогу виконати інтуїтивно зрозумілі алгоритми так само як і класичний комп'ютер. Складність будь-якої обчислювальної задачі, що виконується з використанням квантового комп'ютера, згідно з результатом Гровера, можна зменшити принаймні у квадратний корінь порівняно зі складністю цієї задачі, що виконується за допомогою класичного комп'ютера, а деякі експоненціально складні задачі можуть бути розв'язані за поліноміальний час. На жаль, на сьогодні відомо мало задач, розв'язання яких за допомогою квантового комп'ютера може дати суттєвий виграш. До таких задач належать задачі факторизації та дискретного логарифмування, на складності яких базується стійкість близько 95% реалізацій алгоритмів і протоколів асиметричної криптографії.

Основні проблеми у побудові квантового комп'ютера є такими:

— принципова можливість побудови масштабованого квантового комп'ютера;

— нестабільність, декогеренція через вплив зовнішнього середовища;

— фізична реалізація масштабованого квантового комп'ютера з достатньою для практичних задач кількістю спільно працюючих кубітів;

— невідомість степеня залежності помилок, оскільки надто швидке накопичення помилок зі зростанням числа кубітів не дасть змоги отримати потрібний результат у разі виконання обчислень з прийнятною кількістю повторів;

— побудова нових математичних алгоритмів, які дадуть змогу суттєво прискорити обчислення та пошук рішень для широкого класу задач.

2.3. Основні математичні поняття квантової моделі обчислень. Основою квантового комп'ютера є квантово-механічна система, обов'язково ізольована від навколишнього середовища таким чином, щоб її поведінкою можна було керувати ззовні, але щоб жодна подія, не пов'язана з процедурами контролю, не могла змінити цю поведінку.

Згідно з наведеними нижче постулатами [6] створюється модель для такої системи:

— простором станів системи є асоційований з ізольованою квантово-механічною системою векторний простір над полем комплексних чисел з визначеним скалярним добутком (гільбертів простір), стан системи в будь-який момент часу повністю описується вектором стану, що є одиничним вектором у просторі станів;

— еволюція стану (зміна стану) замкненої квантово-механічної системи описується тільки унітарним перетворенням. Якщо система має стан $|\psi_1\rangle$ у момент часу t_1 і стан $|\psi_2\rangle$ у момент часу t_2, то ці стани пов'язані унітарним перетворенням U, яке залежить тільки від моментів t_1 і t_2, таким, що $|\psi_2\rangle = U|\psi_1\rangle$;

— вимірювання квантової системи складається з набору лінійних операторів, що діють на простір станів системи, і фактично є проекцією на ортогональні підпростори;

— простір станів складної квантово-механічної системи є тензорним добутком просторів станів її складових частин.

Розглянемо поняття паралельного квантового обчислення. Основним інструментом в операціях цієї схеми є сімейство функцій, які будуть описані нижче.

Означення 1. Однокубітне перетворення Уолша–Адамара (Walsh–Hadamard) — це унітарний оператор H, що діє на однокубітну систему і задається співвідношеннями $H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ і $H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Оператор H можна записати стисло у вигляді $H(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{kx}|k\rangle$. Також безпосереднім обчисленням можна перевірити, що оператор H є інволютивним, тобто $H^2 = I_2$. Крім того, якщо знехтувати комплексними коефіцієнтами, то H є симетричним відображенням відносно прямої, яка утворює кут $\frac{\pi}{8}$ з $|0\rangle$-віссю.

Зауважимо, що n-кубітне перетворення Уолша–Адамара H_n визначається як $H^{\otimes n}$ (операція $\otimes$ означає тензорний добуток). Оскільки H — інволютивний оператор, то $H_n^2 = I_2^{\otimes n} = I_{2^n}$, тобто H_n також є інволютивним оператором. У випадку застосування до стану $|0\rangle^{\otimes n}$ оператор H_n генерує однорідну лінійну комбінацію цілих чисел від 0 до $2^n - 1$, тобто $H_n(|0..0\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$.

Перетворення Уолша–Адамара дають змогу підготувати вхідні дані для паралельного обчислення. Розглянемо процедуру обчислення як таку. Нехай $f: Z_2^m \to Z_2^k$ — деяка функція, не обов'язково оборотна. Оскільки оборотність функції f не вимагається, то її в такому вигляді не можна використовувати як перетворення в квантовому комп'ютері. Однак за рахунок використання певного додаткового об'єму пам'яті можна створити унітарне перетворення для моделювання функції f. Для цього потрібна квантова система V, що є тензорним добутком m-кубітної та k-кубітної квантових систем. Нагадаємо, що система V має базис, який складається з векторів $|x\rangle \otimes |y\rangle$, де x і y — двійкові представлення цілих

чисел в Z_2^m і Z_2^k відповідно. Визначимо лінійне перетворення $U_f : |x\rangle \otimes |y\rangle \mapsto$

$\mapsto |x\rangle \otimes |y \oplus f(x)\rangle$, де $\oplus$ позначає операцію додавання в групі Z_2^k (відоме також як *XOR*). Для фіксованого значення x величина $y \oplus f(x)$ набуває кожного значення в Z_2^k точно один раз, оскільки y набуває значень з Z_2^k. Тому результатом перетворення U_f є просто перестановка всіх 2^{m+k} елементів базису V і з цього випливає, що воно є унітарним. Крім того, $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$. У цьому сенсі U_f моделює обчислення значення функції f. Таке відображення U_f називають стандартним оракулом для функції f. Таким чином, стандартний оракул можна застосовувати для моделювання будь-якої функції, оборотної чи ні, на квантовому комп'ютері. З цього своєю чергою випливає, що будь-яку функцію, яку можна обчислити за допомогою класичного комп'ютера, також можна обчислити за допомогою квантового комп'ютера.

У тому разі, коли функція f є бієктивною (і лише за цієї умови), можна визначити простіший і більш очевидний оракул $|x\rangle \to |f(x)\rangle$. Його називають мінімальним або затираючим оракулом для f (існує задача, для якої показано, що використання для її розв'язку мінімального оракулу є експоненціально більш вигідним відносно кількості ресурсів, ніж стандартного оракулу).

Можна розглядати це як одночасне обчислення функції f для всіх можливих значень аргументу x, хоча те, що $|f(x)\rangle$ має зв'язок зі станом $|x\rangle$, для всіх x іноді може створювати труднощі. Формування стану такого виду часто називають квантовим паралелізмом. Це — простий і стандартний перший крок у багатьох квантових обчисленнях. Найважчий етап — здобуття корисної інформації з цього (надзвичайно переплутаного) результівного стану.

Подібно до класичної моделі обчислень можна створити модель будь-якої квантової схеми, використовуючи лише прості унітарні перетворення векторного простору — квантові вентилі. Кожен квантовий вентиль оперує лише кількома кубітами за один раз. У квантовій моделі існують скінченні набори вентилів, які дають змогу побудувати довільне унітарне перетворення з бажаною точністю. О. Кітаєв показав, що таке наближення можна виконати з мінімальним збільшенням використовуваних ресурсів [7], тобто у квантовій моделі всі обчислення можна моделювати з використанням певного набору простих схем. До того ж, у роботі [8] А. Яо продемонстрував еквівалентність моделі з використанням схем та квантової машини Тюрінга, яку запропонував Д. Дойч. Так само як і в класичній моделі обчислень, у квантовій моделі ефективними обчисленнями є ті, які можна виконати з використанням поліноміально обмеженої послідовності елементарних вентилів.

Означення 2. Розміром квантової схеми (перетворення) є мінімальна кількість елементарних операцій над фіксованим набором простих вентилів, потрібна для побудови цієї схеми (перетворення).

У такий спосіб можна оцінювати складність квантових операцій або перетворень. Більш того, ця оцінка якісно не змінюється у разі заміни набору твірних вентилів на інший, що є загальноприйнятим.

Здебільшого основний інтерес становлять саме ефективні квантові обчислення. Як правило, такі обчислення складаються з двох частин, які досить часто є незалежними: ефективного квантового процесу і ефективної класичної обробки даних, отриманих в результаті проведених вимірювань впродовж квантового процесу.

Квантові комп'ютери є ймовірнісними за своєю природою. Тому абсолютна більшість алгоритмів є також імовірнісними, але цього досить для ефективного розв'язання задачі (за умови ефективності ймовірнісного алгоритму). Достатньо провести експеримент декілька разів і визначити остаточний результат за більшістю результатів експерименту. Такий підхід може гарантувати вірну відповідь з імовірністю, яка є як завгодно близькою до одиниці.

3. ЕФЕКТИВНІ КВАНТОВІ АЛГОРИТМИ

На сьогодні задача про приховану підгрупу є вдалим об'єднанням прикладів задач, які можна ефективно розв'язати за допомогою квантового комп'ютера, на відміну від наявних алгоритмів для класичного комп'ютера, що вперше відзначено в роботі [9].

Задача 1 (про приховану підгрупу, англ. Hidden Subgroup Problem, HSP). Нехай задано множину твірних елементів групи G, деяку скінченну множину X і відображення $f: G \to X$ з додатковою умовою, що існує така підгрупа $H \subseteq G$, що для довільних елементів $g_1, g_2 \in G$ виконується тотожність $f(g_1) = f(g_2)$ тоді й тільки тоді, коли $g_1 H = g_2 H$ (за таких умов будемо казати, що відображення f приховує підгрупу H). Потрібно знайти множину твірних елементів підгрупи H за допомогою обчислення функції f.

Зауваження 1. Частковий випадок задачі про приховану підгрупу, коли група G є абелевою, називається абелевою задачею про приховану підгрупу.

Твердження 1 [7]. Якщо в умовах задачі 1 функція f є ефективно обчислюваною в класичній моделі обчислень, а група G — абелева, то у квантовій моделі обчислень існує ефективний алгоритм розв'язку цієї задачі.

О. Кітаєв у роботі [7] виділив властивість комутативності групи як достатню умову існування ефективного розв'язку задачі 1 у квантовій моделі обчислень. Досі у більшості робіт щодо доведення існування ефективного в квантовій моделі обчислень алгоритму розв'язку деякої задачі використовують її зведення до абелевої задачі про приховану підгрупу, тобто твердження 1.

Основною проблемою є побудова таких квантових алгоритмів, щоб оброблення результатів з відновлення прихованої підгрупи виконувалося за поліноміальний час на класичному комп'ютері. В абелевому випадку зробити це дають змогу алгоритм Евкліда та ефективний алгоритм розв'язання системи лінійних рівнянь.

Різниця між квантовими обчисленнями та ймовірнісним методом розв'язання полягає лише в тому, що матриці перетворень у квантовому випадку можуть містити довільні комплексні числа, а в імовірнісному — лише невід'ємні дійсні числа, до того ж унітарні перетворення зберігають норму вектора в просторі L_2, а імовірнісні перетворення — в L_1.

Д. Дойч першим показав, що, можливо, квантова модель обчислень має перевагу над класичною моделлю. Але варто зазначити, що йдеться про оцінку складності відносно кількості запитів до оракула, що обчислює досліджувану функцію. Функцію $f: Z_2 \to Z_2$ називають сталою, якщо $f(0) = f(1)$, і збалансованою, якщо $f(0) \neq f(1)$. Нехай задано деяку функцію $f: Z_2 \to Z_2$ за допомогою оракула. Використовуючи запити до оракула щодо обчислення значень функції, потрібно визначити, до якого типу вона належить. У разі використання класичних детермінованих обчислень потрібно зробити два запити до оракула, а у квантовій моделі обчислень достатньо одного.

Узагальнення попередньої задачі зроблено в роботі [10], де розглядаються функції $f: Z_2^m \to Z_2$, $m \in N$. Функцію f називають збалансованою, якщо потужності прообразів 0 та 1 однакові, та сталою, якщо значення функції f є однаковим на всій області визначення. Алгоритм Дойча–Джози у квантовій моделі обчислень дає змогу розрізнити ці два випадки з використанням одного запиту до оракула щодо обчислення функції f [10]. Ця задача є частковим випадком задачі 1 про приховану підгрупу, де група $G = Z_2^m$, множина $X = Z_2$, а відображення $f: Z_2^m \to Z_2$ приховує підгрупу H, яка збігається з групою G у випадку сталої функції f та містить половину елементів групи G у випадку збалансованої функції f. Для $m = 1$ задача зводиться до оригінальної задачі Дойча.

У 1993 р. Е. Бернштейн та У. Вазірані розглянули таку задачу: про відображення $f\colon \{0,1\}^n \to \{0,1\}$ відомо, що існує таке значення $a \in \{0,1\}^n$, що $f(x) = a \cdot x$ для всіх значень $x \in \{0,1\}^n$, де операція «$\cdot$» є позначенням суми за модулем 2 добутків відповідних бітів (аналогічно скалярному добутку над Z_2), і потрібно знайти невідоме значення a. Цю задачу було ефективно розв'язано в квантовій моделі обчислень з використанням одного запиту щодо обчислення функції f, хоча у класичній моделі обчислень потрібно n запитів. Задача Бернштейна–Вазірані також є частковим випадком абелевої задачі про приховану підгрупу, коли група $G = Z_2^n$, множина $X = Z_2$, а відображення $f\colon Z_2^n \to Z_2$ приховує підгрупу $H = \{y \mid a \cdot y = 0\}$.

У 1994 р. Д. Саймон розглянув відображення $f\colon Z_2^m \to Z_2^m$ про яке відомо, що або всі значення $f(x)$, $x \in Z_2^m$, є різними (випадок 1–1), або існує таке значення $s \in Z_2^m$, що для довільних елементів $x, y \in Z_2^m$ виконується рівність $f(x) = f(y)$ тоді і тільки тоді, коли $x = y$ або $x = y \oplus s$ (випадок 2–1). Він запропонував квантовий алгоритм розв'язання задачі розрізнення цих випадків, використовуючи в середньому $O(m)$ запитів до оракула щодо обчислення функції f (пізніше Ж. Брассар і П. Хоєр поліпшили результат $O(m)$ запитів в середньому до $O(m)$ запитів у найгіршому випадку). Для будь-якого алгоритму, навіть імовірнісного, у класичній моделі обчислень необхідною кількістю запитів для розв'язання цієї задачі є $\Omega(2^{m/2})$. Отже саме квантовий алгоритм Саймона був першим алгоритмом, який розв'язував певну задачу експоненціально швидше ніж будь-який алгоритм в класичній моделі обчислень відносно необхідної кількості запитів до оракула. Розглянута задача є частковим випадком задачі 1 про приховану підгрупу, де група $G = Z_2^m$ з операцією $\oplus$, множина $X = Z_2^m$, а відображення $f\colon Z_2^m \to Z_2^m$ приховує підгрупу H, яка збігається з тривіальною $H = \{0\}$ у випадку 1–1 та $H = \{0, s\}$ у випадку 2–1.

У 1994 р. з'являється робота П. Шора [11], яка й досі є одним з найвидатніших результатів дослідження квантової моделі обчислень. У ній представлено поліноміальні алгоритми розв'язання задач факторизації цілих чисел та дискретного логарифмування у квантовій моделі обчислень. Більш точно в [11] і в наступній роботі [12] у 1997 р. П. Шор використав відоме зведення задачі факторизації цілого числа $n \in N$ до задачі пошуку показника δ, якому належить випадково обране ціле число $1 < a < n$ за модулем n.

Задача пошуку показника, задача дискретного логарифмування та інші представлені вище задачі зводяться до абелевої задачі про приховану підгрупу, що дає змогу скористатися твердженням 1.

Незважаючи на те, що досить багато зусиль було докладено до пошуків ефективних квантових розв'язків задачі про приховану підгрупу для неабелевих груп G, майже всі відомі квантові алгоритми з поліноміальним часом були знайдені для груп, дуже близьких до абелевих. Було запропоновано цілий клас задач, подібних до задачі про приховану підгрупу і, як наслідок, пов'язаних з нею.

Задача 2 (про прихований зсув, англ. Hidden Shift Problem, Hidden Translation Problem, DHSP) [13]. Нехай задано множину твірних елементів групи G, та дві ін'єктивні функції — f_0 і f_1, які відображають групу G у деяку множину X з додатковою умовою, що існує такий елемент $u \in G$, який називається зсувом, що для будь-якого значення $g \in G$ виконується співвідношення $f_0(g) = f_1(g \circ u)$. Потрібно знайти невідоме значення зсуву u, скориставшись обчисленням функцій f_0 і f_1.

Твердження 2. Абелева задача про прихований зсув для циклічної групи Z_N є еквівалентною задачі про приховану підгрупу для діедральної групи D_N.

Значна гнучкість постановки задач про приховану підгрупу та про прихований зсув дає змогу використовувати їх під час розв'язання досить великої кількості різноманітних задач, наприклад, як це було зроблено в роботі [14] для деяких задач комбінаторної теорії груп.

4. ОГЛЯД НАЯВНИХ РЕАЛІЗАЦІЙ КВАНТОВИХ ОБЧИСЛЮВАЛЬНИХ ПРИСТРОЇВ

Побудова достатньо потужного квантового комп'ютера у вигляді реального фізичного пристрою є однією з фундаментальних задач сучасної фізики. На сьогодні існують лише обмежені реалізації квантових обчислювальних пристроїв.

Відомо, що є два основних види реалізацій квантових обчислювальних пристроїв: універсальні (наприклад, 50-кубітний квантовий комп'ютер IBM) та неуніверсальні (наприклад, пристрої компанії D-Wave). Головною відмінністю є те, що універсальні квантові обчислювальні пристрої розробляють з метою виконання довільних дозволених операцій та розв'язання довільних задач. Неуніверсальні обчислювальні пристрої створюють для розв'язання деякого обмеженого класу задач, наприклад, для оптимізації певних алгоритмів машинного навчання.

Згідно з Д. ДіВінченцо існує визначений набір вимог до реального універсального квантового обчислювального пристрою, а саме:

- масштабованість (можливість збільшення числа кубітів;
- можливість ініціалізації квантових регістрів (кубітів) у будь-який початковий стан;
- здатність квантових вентилів відпрацьовувати протягом часу, меншого, ніж час декогеренції;
- реалізація повного набору вентилів (Тюрінга);
- можливість зчитування інформації з квантових регістрів.

Серед основних технологій реалізації квантового обчислювального пристрою слід виділити такі:

- твердотільні квантові точки (логічним кубітом є направленість електронного або ядерного спіну в квантовій точці, керування здійснюється за допомогою зовнішніх потенціалів чи лазерного імпульсу);
- надпровідні елементи (логічним кубітом є присутність або відсутність куперівської пари в певній області, керування здійснюється за допомогою зовнішнього потенціалу чи магнітного потоку);
- іони в вакуумних пастках Пауля (логічним кубітом є основний або збуджений стан зовнішнього електрону в іоні, керування здійснюється за допомогою лазерних імпульсів);
- використання заплутаних станів фотонів.

Основними проблемами в побудові достатньо великих квантових обчислювальних пристроїв є зовнішній вплив, який може зруйнувати стан квантової системи або значно його спотворити, та помилки, що виникають під час вимірювань і виконання елементарних перетворень.

Молода канадська компанія D-Wave (https://www.dwavesys.com/) ще в 2007 р. заявила про створення 16-кубітного квантового комп'ютера. Комп'ютер міг розв'язувати пазли судоку та інші задачі пошуку за шаблоном. Дослідники стверджували, що вони зможуть створити практичні системи до 2008 р. Скептики відразу заперечили, що до створення практичних квантових комп'ютерів має минути ще кілька десятиліть.

Наприкінці 2007 р. було повідомлено про квантовий процесор Orion на 28 кубітах. Вже 11 травня 2011 року було анонсовано новий процесор One, який був названий «першим комерційним квантовим комп'ютером» і працював на 128-кубітному чіпсеті. У 2012 р. в роботі [15] стверджувалося, що компанія D-Wave Systems побудувала квантовий пристрій, який оперує 84 кубітами. Того

самого року був анонсований квантовий комп'ютер Vesuvius (або D-Wave Two) з 512 кубітами, а 20 серпня 2015 року було створено версію D-Wave 2X з 1152 кубітами.

24 січня 2017 року компанія D-Wave Systems Inc. опублікувала звіт, згідно з яким компанія, що займається кіберзахистом державних та комерційних організацій Temporal Defense Systems Inc. (TDS, http://temporaldefense.com), стала першим покупцем майбутнього нового пристрою D-Wave 2000Q, який коштує 15 мільйонів доларів та оперує 2000 кубітами.

Попри наведені непрямі докази існування переплутаності в процесі обчислення пристрою D-Wave в деяких роботах, більшість дослідників не визнають пристрій D-Wave квантовим. Хоча показано, що деякі відомі квантові алгоритми, такі як алгоритми Саймона та Бернштейна-Вазірані, можна використовувати в адіабатичній квантовій моделі, проте немає жодних повідомлень про спроби зробити це на пристроях D-Wave. Більш того, зазначена вище компанія наголошувала на тому, що алгоритми Гровера та Шора не можна реалізувати на пристроях D-Wave.

У 2015 р. дослідники компанії Google заявили (без прямих доказів), що згідно з їхніми дослідженнями пристрій D-Wave використовує квантові ефекти, однак при цьому в так званому «1000-кубітному» комп'ютері кубіти насправді зібрано в кластери по 8 кубітів кожний. У роботі [16] проаналізовано всю доступну інформацію про пристрої D-Wave, внаслідок чого зроблено висновок, що пристрої D-Wave не дають жодної обчислювальної переваги над класичним комп'ютером.

У 2001 р. вчені з компанії IBM заявили про успішне випробування квантового комп'ютера ємністю 7 кубітів (3 кубіти в першому регістрі і 4 кубіти в другому регістрі), реалізованого на основі явища ядерного магнітного резонансу. Ними було виконано факторизацію числа 15 за допомогою алгоритму Шора.

У 2007 р. група вчених університету Квінсленда повідомила про експериментальну демонстрацію виконання алгоритму Шора з використанням квантових логічних вентилів на основі поляризації фотонів. Для демонстрації було факторизовано також число 15 за допомогою 7 кубітів (3 кубіти в першому регістрі і 4 кубіти в другому регістрі).

Того самого 2007 р. вчені Університету науки і технологій Китаю також повідомили про експериментальну демонстрацію реалізації алгоритму Шора з використанням квантових логічних вентилів на основі фотонів. Вони так само факторизували число 15 з використанням лише 6 кубітів (2 кубіти в першому регістрі і 4 кубіти в другому регістрі).

У 2009 р. описано успішну експериментальну демонстрацію алгоритму Шора з використанням інтегрованого хвильоводу на основі кремнієвого чіпа. Чотири кубіти на основі фотонів було використано для факторизації числа 15: 1 кубіт у першому регістрі і 3 кубіти в другому регістрі.

У 2012 р. група дослідників університету Каліфорнії повідомила про нову експериментальну демонстрацію алгоритму Шора з використанням фазових кубітів та надпровідних хвильових резонаторів. Ця група також розклала на множники число 15 з використанням 4 кубітів: 2 кубіти в першому регістрі і 2 кубіти в другому регістрі.

Також у 2012 р. в роботі Е. Мартіна-Лопеза та ін. було представлено експериментальну демонстрацію алгоритму Шора для факторизації числа 21 з використанням лише двох кубітів на основі фотонів.

У 2012 р. проведено експериментальну демонстрацію квантового алгоритму факторизації цілих чисел на основі ядерного магнітного резонансу для факторизації числа 143 з використанням 4 кубітів і адіабатичного підходу. Основною відмінністю цієї роботи є реалізація не алгоритму Шора, а його альтернативи — перетворення задачі факторизації цілих чисел на задачу оптимізації. Цю ідею вперше було представлено К. Бургесом у 2001 р. та удосконалено в 2010 р. Шеллером та Шутцхольдом.

У 2015 р. група дослідників на чолі з Т. Монцем повідомила про нову експериментальну демонстрацію алгоритму Шора з використанням іонних пасток для розкладання числа 15. Для цього використовували п'ять $^{40}Ca^{+}$ іонів у лінійній пастці Паулі. Було застосовано масштабовану схему алгоритму Шора, але зі зменшеною кількістю кубітів — 1 кубіт в першому регістрі і 4 кубіти в другому регістрі.

У зазначених вище роботах описано реальні експериментальні демонстрації реалізації алгоритму Шора, при цьому показовою є робота Н. Даттані та Н. Браєнса [17]. У першій редакції вона мала назву «Квантова факторизація числа 44929 за допомогою 4 кубітів» і містила інформацію про розклад чисел 3599, 13081 та 44929 за допомогою квантового алгоритму, який використовує 4 кубіти. Третя редакція роботи [17] мала назву «Квантова факторизація числа 56153 за допомогою 4 кубітів» і містила інформацію про розкладання на множники вже більшого числа — 56153 та, на додаток, числа 11663. Ці результати можна вважати своєрідним рекордом, оскільки у попередніх роботах було описано факторизацію набагато менших чисел. Особливість цієї роботи полягає в тому, що автори не провели жодних нових експериментів, а лише скористалися попередніми експериментальними результатами і показали, що можна розкласти на множники певний клас цілих чисел за допомогою додаткових обчислень у рамках класичної моделі обчислень.

В оригінальній версії квантового алгоритму Шора факторизації цілих чисел для розкладання числа N, що фактично означає пошук періоду функції $f(x) = a^x \bmod N$, $x \in Z_N$, для деякого значення $a \in Z_N^*$ (тобто пошук мультиплікативного порядку елемента $a \in Z_N^*$), перший регістр повинен мати розмір $2\log N$ кубітів (для обчислення квантового перетворення Фур'є та забезпечення обмеженої помилки у випадку використання відповідних дробів), а другий регістр — розмір $\log N$ кубітів, достатній для значень функції. Таким чином, загальна кількість необхідних кубітів дорівнює $3\log N$. У своїх дослідженнях К. Залка показав, що можна зменшити кількість необхідних кубітів до $2 + \frac{3}{2}\log N$. Пізніше цю ідею було підтверджено, і фактично в першому регістрі використовується лише один кубіт і так зване напівкласичне перетворення Фур'є. Оскільки умовою досягнення такого зменшення необхідних ресурсів є неодноразове використання та повторна ініціалізація одного кубіта нульовим значенням у межах одного проходження схеми квантового алгоритму, цей метод назвали методом повторного використання кубіта (англ. qubit recycling). Його застосовують майже у всіх зазначених вище експериментальних демонстраціях виконання алгоритму Шора.

Більш того, в усіх наведених роботах використано відомості про шуканий результат безпосередньо під час його обчислення, оскільки розклад невеликих чисел і так є відомим. Існують деякі числа, мультиплікативний порядок яких є невеликим, але його значення дає змогу отримати бажаний розклад вхідного цілого числа. Тому кількість необхідних кубітів значно скоротиться, якщо виконати певні обчислення заздалегідь за допомогою класичної моделі. Таку версію алгоритму Шора називають компонованим (англ. compiled) алгоритмом Шора. Саме вона використовується в більшості практичних реалізацій. До того ж, число 15 має певну особливість — всі елементи мультиплікативної групи кільця лишків Z_{15} мають мультиплікативний порядок, що дорівнює 2 або 4, тобто степеня 2. Це означає, що немає потреби у використанні відповідних дробів та додаткових кубітів, навіть у разі застосування оригінальної версії алгоритму Шора. Можна також використати число 11, яке відповідає показнику 2 і дає змогу розкласти число 15, що було зроблено в деяких експериментах.

Нещодавно Ж. Жу та М. Геллер показали, як можна розкласти числа 51 і 85 з використанням лише 8 кубітів (без проведення експерименту). Як і число 15,

числа 51 і 85 є добутком двох простих чисел Ферма (виду $2^{2^k}+1$). Було показано, у який спосіб можна знайти числа, що мають невеликий мультиплікативний порядок за модулем добутку простих чисел Ферма.

Дж. Смолін та інші розвинули цю ідею та довели, що для довільного складеного числа pq, де p і q — прості числа, існує число a, яке належить показнику 2 за модулем pq, і дає змогу розкласти число pq на множники.

З точку зору демонстрації можливостей сучасних експериментальних квантових обчислювальних пристроїв слід припинити використання компонованих версій алгоритмів і, наприклад, замість демонстрації алгоритму Шора зосередитися на його основній квантовій частині — пошуку періоду періодичної функції. Іншими словами, результатом реалізації алгоритму має бути знаходження періоду довільної функції з обмеженням щодо розмірів області визначення та значень. З огляду на дані щодо кількості використовуваних кубітів, наведені у відомих роботах, можна дійти висновку, що протягом останніх 15–20 років не відбулося майже жодних змін в обчислювальних можливостях відповідних експериментів. Так, відбулися зміни в методах і технологіях, які дали змогу покращити контроль та зовнішні умови, а не в можливостях для знаходження періоду періодичної функції з більшою областю визначення.

У 2016 р. компанія IBM заявила про створення квантового комп'ютера ємністю 5 кубітів, один з яких використовується для корекції помилок. Цей обчислювальний пристрій базується на п'ятикубітному надпровідному чіпі з геометрією зірки та реалізацією повної алгебри Кліфорда. Він є програмованим і дає змогу створювати вентилі та моделювати їх роботу.

У травні 2017 року компанія IBM заявила про реалізацію квантових обчислювальних пристроїв з 16 і 17 кубітами, а в листопаді 2017 року IBM анонсувала 50-кубітний квантовий обчислювальний пристрій (для обчислень використовуються лише 20 кубітів, а решта слугує для корекції помилок). У ньому кожний кубіт може перебувати в когерентному стані до 90 мікросекунд, а це означає, що час для всіх операцій не може перевищувати цього значення. Однак, треба зазначити, що 50-кубітний квантовий обчислювальний пристрій IBM є достатньо енергоефективним — він споживає від 10 до 15 кВт, що приблизно дорівнює споживанню енергії 10 типових серійних мікрохвильових печей (без урахування енергії, потрібної для охолодження пристрою перед роботою, яке здійснюється протягом 36 годин).

Програма Quantum Experience дає змогу отримати віддалений доступ до цього обчислювального пристрою, моделювати та запускати різні алгоритми, включаючи алгоритм Шора, з використанням класичної мережі Інтернет для з'єднання з хмарою IBM. На сьогодні програма Quantum Experience забезпечує доступ до двох 5-кубітних пристроїв та одного 16-кубітного пристрою і має близько 75 тисяч користувачів, які запустили близько двох з половиною мільйонів експериментів. Здебільшого це науковці, які за результатами моделювання опублікували декілька десятків робіт.

У січні 2018 року компанія Intel також приєдналася до гонки квантових обчислювальних пристроїв і оголосила про створення надпровідного квантового чипу з назвою Tangle Lake, який містить 49 кубітів.

5 березня 2018 року співробітники компанії Google представили новий квантовий процесор під назвою Bristlecone ємністю 72 кубіти, побудований на основі 9-кубітного квантового пристрою, представленого компанією кілька років тому. Початковий 9-кубітний квантовий пристрій передбачав використання кубітів, об'єднаних у лінійний масив. Для нього вдалося досягти досить низького рівня помилок — частка помилок була на рівні 1% для зчитування даних, 0,1% для однокубітних квантових вентилів і 0,6% для двокубітних квантових вентилів. У но-

вому квантовому пристрої використовуються двомірні структури. Кубіти утворюють два квадратних масиви 6 на 6, розташовані один над одним, завдяки чому система може відстежувати та виправляти помилки під час обчислень. На момент анонсу детальні характеристики нового пристрою не були розкриті, але дослідники сподіваються, що він демонструватиме приблизно такий самий рівень помилок як і його попередник. Більш того, вони мають оптимістичну надію досягти так званої квантової переваги.

Під терміном «квантова перевага» розуміють демонстрацію того, що квантовий обчислювальний пристрій розв'яже певну обчислювальну задачу (можливо, спеціально створену для такої мети) швидше, ніж будь-який класичний сучасний суперкомп'ютер (або всі сучасні суперкомп'ютери разом). Досягнення цього рівня фактично означатиме початок ери квантових пристроїв та квантової моделі обчислень. Більшість вчених сподіваються, що за теперішнього рівня помилок це станеться тоді, коли квантові пристрої оперуватимуть 100 та більше кубітами. Однак, результати обчислень, виконаних спеціалістами компанії Google, свідчать про те, що для цього достатньо 49 кубітів, якщо число вентилів буде перевищувати число 40, а помилка двокубітних квантових вентилів буде меншою, ніж 0,5%. Подальші дослідження цього пристрою дадуть змогу більш точно обчислити рівень відповідних помилок та проаналізувати його можливості.

Квантові обчислювальні пристрої компаній IBM, Google та Intel на вигляд є універсальними пристроями з реальними характеристиками. Однак, кількість кубітів, доступних для використання, зазвичай є суттєво меншою заявленої кількості через потребу в додаткових операціях для корекції помилок. Тому стверджувати про досягнення квантової переваги ще зарано, оскільки на сьогодні навіть звичайний ноутбук може змоделювати роботу 30–40 кубітів за допомогою програмних засобів. Наприклад, доступні для обчислень 20 кубітів дають змогу знайти періоди таких періодичних функцій, що у випадку реалізації звичайного алгоритма Шора можна гарантовано здійснити успішне розкладання на множники максимум для числа 89. Це говорить про те, що наразі відбувається накопичення експериментів, технологій та досвіду і на пристроях з такою кількістю кубітів ставити рекорди ще зарано, але загальна задача пошуку періоду періодичної функції може стати ефективним мірилом потужності і «квантовості» майбутніх обчислювальних пристроїв.

ВИСНОВКИ

Зроблено огляд та аналіз основних понять і положень квантової моделі обчислень, ефективних квантових алгоритмів, останніх результатів, можливостей та перспектив у галузі побудови масштабованого квантового комп'ютера. Розглянуто результати останніх досліджень щодо розв'язання алгебраїчних задач у квантовій моделі обчислень і можливого застосування цих результатів для побудови нових та аналізу давно відомих криптографічних перетворень. З'ясовано, що на сьогодні є лише невелика кількість задач, для яких існують ефективні квантові алгоритми, що будуть розв'язувати їх на практиці за поліноміальний час на противагу класичному комп'ютеру. До класу таких задач належать задачі факторизації великих чисел та дискретного логарифмування, на складності яких ґрунтується стійкість переважної більшості алгоритмів і протоколів асиметричної криптографії. Іншими словами, після створення масштабованого квантового комп'ютера ці алгоритми і протоколи будуть зламані. Але навіть якщо коло ефективно розв'язуваних задач не буде розширено, завдяки алгоритму Гровера складність будь-якої задачі на квантовому комп'ютері буде у квадратний корінь разів менша ніж на класичному

комп'ютері. Тоді масштабовані квантові комп'ютери можна буде застосовувати для розв'язання задач у галузі економіки, планування, комбінаторної оптимізації тощо.

Отримані на сьогодні експериментальні і практичні результати свідчать про відсутність достатнього прогресу у побудові масштабованого квантового обчислювального пристрою з точки зору реалізації відомих квантових алгоритмів. Допоки практичні реалізації квантових систем не будуть оперувати більшою кількістю кубітів ніж кількість кубітів, робота яких може бути змодельована за прийнятний час на класичному комп'ютері, важко стверджувати про якісь переваги та методи оцінювання. Проте більшість дослідників очікують на створення повноцінного квантового комп'ютера, який зможе, наприклад, зламати RSA-4096, впродовж наступних 10–15 років, щоправда, з імовірністю прогнозу 0.5. Тому вже зараз потрібно підготувати відповідні варіанти заміни для постквантових криптографічних перетворень та протоколів з оцінкою стійкості та складності впровадження, а також детально розробити різні модифікації перетворень з урахуванням можливостей алгоритму Гровера.

СПИСОК ЛІТЕРАТУРИ

1. Bennett C., Brassard G. Quantum cryptography: Public-key distribution and coin tossing. *Proc. International Conference on Computers, Systems and Signal Processing* (Bangalore, India. 1984). P. 175–179.
2. Квантовый компьютер и квантовые вычисления. Ижевск: Ижевская республиканская типография, 1999. 288 с.
3. Прескилл Дж. Квантовая информация и квантовые вычисления. Том 1. Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2008. 464 с.
4. Ааронсон С. Квантовые вычисления со времен Демокрита. Москва: Альпина нон-пикшн, 2018. 494 с.
5. Савчук М.Н. О работах киевской школы теоретической криптографии. *Кибернетика и системный анализ*. 2010. Т. 46, № 3. С. 52–68.
6. Nielsen M.A., Chuang I.L. Quantum computation and quantum information. Cambridge: Cambridge University Press,. 2000. 676 p.
7. Kitaev A. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*. 1997. Vol. 52, N 6. P. 53–112.
8. Yao A. Quantum circuit complexity. *Proc. 34th Annual Symposium on Foundations of Computer Science*. 1993. P. 352–361.
9. Boneh R., Lipton R. Quantum cryptanalysis of hidden linear functions. *Proc. 15th Annual International Cryptology Conference (Santa Barbara, California, USA, August 27, 1995). Advances in Cryptology. Crypto'95. Lecture Notes in Computer Science*. 1995. Vol. 31. P. 424–437.
10. Deutsch D., Jozsa R. Rapid solution of problems by quantum computation. *Proc. Royal Society of London, Series A*. 1992. N 439. P. 553–558.
11. Shor P.W. Algorithms for quantum computation: discrete logs and factoring. *Proc. 35th Symposium on the Foundations of Computer Science* (Santa Fe, NM, USA, 20–22 Nov., 1994), 1994. P. 124–134.
12. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*. 1997. Vol. 26, Iss. 5. P. 1484–1509.
13. van Dam W., Hallgren S., Ip L. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*. 2006. Vol. 36, N 3. P. 763–778.
14. Фесенко А.В. Уязвимости криптопримитивов на основе задачи поиска сопрягающего элемента и степени в квантовой модели вичислений. *Кибернетика и системный анализ*. 2014. Т. 50, № 5. С. 184–186.

15. Bian Z., Chudak F., Macready W., Clark L. , Gaitan F. Experimental determination of Ramsey numbers. *Physical Review Letters.* 2012 Vol. 111, Iss. 13. P. 130505. DOI: https://doi.org/10.1103/PhysRevLett.111.130505. URL: https://arxiv.org/abs/1201.1842.

16. Cho A. Quantum or not, controversial computer yields no speedup. *Science.* 2014. Vol. 344, N 6190. P. 1330–1331. DOI: https://doi.org/10.1126/science.344.6190.1330.

17. Dattani N.S. , Bryans N. Quantum factorization of 56153 with only 4 qubits. *Quantum Physics Archive.* arXiv:1411.6758 [quant-ph]. 2014. URL: https//arxiv.org/abs/1411.6758.

Надійшла до редакції 20.09.2018

М.Н. Савчук, А.В. Фесенко
КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: ОБЗОР И АНАЛИЗ

Аннотация. Выполнен обзор и анализ основных понятий и положений квантовой модели вычислений, эффективных квантовых алгоритмов, последних результатов, возможностей и перспектив в построении масштабированного квантового компьютера. Рассмотрен некоторый класс алгебраических задач в квантовой модели вычислений, для которых существует эффективный квантовый алгоритм решения. Проведен детальный анализ существующих практических реализаций квантового компьютера и показано, что пока что нет достаточного прогресса в построении масштабированного квантового вычислительного устройства, но, тем не менее, большинство исследователей ожидают создание полноценного квантового компьютера в течение следующих 10–15 лет.

Ключевые слова: квантовая модель вычислений, квантовая криптография, квантовый компьютер, эффективные квантовые алгоритмы, постквантовые криптографические примитивы.

M.M. Savchuk, A.V. Fesenko
QUANTUM COMPUTING: SURVEY AND ANALYSIS

Abstract. The authors conduct a survey and analysis of the main concepts and postulates of the quantum computing model, efficient quantum algorithms, recent results, capabilities, and prospects in constructing a scalable quantum computer. A certain class of algebraic problems in a quantum computation model is considered, for which there and efficient quantum solution algorithm exists. A detailed analysis of available quantum computer implementations has been carried out and it has been shown that sufficient progress has yet been made in constructing a scalable quantum computing device; nevertheless, most of researchers expect a quantum computer to be created in the next 10–15 years.

Keywords: quantum computing model, quantum cryptography, quantum computer, efficient quantum algorithms, postquantum cryptographic primitives.

Савчук Михайло Миколайович,
чл.-кор. НАН України, доктор фіз.-мат. наук, в.о. завідувача кафедри Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»,
e-mail: mikhail.savchuk@gmail.com.

Фесенко Андрій В'ячеславович,
кандидат фіз.-мат. наук, старший викладач Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», e-mail: andrey.fesenko@gmail.com.