КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 519.6:511 DOI:10.34229/2707-451X.23.1.2

В.Ю. КОРОЛЬОВ, О.М. ХОДЗІНСЬКИЙ

ДОСЛІДЖЕННЯ ВПЛИВУ ПАРАМЕТРІВ КВАНТОВОГО ВІДПАЛУ НА ЯКІСТЬ РОЗВ'ЯЗКУ ЗАДАЧІ ФАКТОРИЗАЦІЇ ЧИСЕЛ

Досліджено режими роботи квантового відпалу для квантового комп'ютера фірми D-Wave для задачі факторизації числа. Виявлено, що зворотній квантовий відпал дозволяє суттєво покращити точність пошуку множників числа порівняно з підвищенням часу відпалу, кількістю запусків задачі, відпалом з паузою та відпалом із загартовування.

Ключові слова: *квантовий відпал, факторизація, асиметричні шифри, загартовування, зворотній відпал, комбінаторна оптимізація.*

Вступ. В останні два роки гібридні квантово-класичні хмарні обчислювання [1, 2] почали застосовуватись в реальному секторі економіки [2, 3] для розв'язування задач логістики, банківських трансакцій, фармакології тощо. Відомо, що теоретично квантові комп'ютери (КК) мають суттєву перевагу перед класичними комп'ютерами за часом розв'язування окремих оптимізаційних задач [4], але реальні КК на даний час мають малу кількістю кубіт порівняно з кількістю біт у класичних комп'ютерів; тому безпосередньо сучасні квантові комп'ютери можуть розв'язувати лише задачі невеликої розмірності [4]. Вирішення цієї технологічної проблеми покладається на процедури декомпозиції вихідних оптимізаційних задач на менші за розмірністю підзадачі на класичних серверах [1, 4], а отримані підзадачі розв'язують КК.

Результати розв'язку задачі факторизації чисел використовуються у сфері захисту інформації, цифровій обробці сигналів і зображень та кодуванні. Окрім широко відомого алгоритма Шора пошуку множників числа за допомогою КК, що побудовані на квантових логічних елементах, задачу факторизації можна сформулювати як задачу комбінаторної оптимізації, яку можна розв'язувати за допомогою параметризованого квантового відпалу.

Основні питання, що розглядаються у даній роботі
– дослідження впливу режимів глобального відпалу системи D-Wave на якість розв'язку задачі факторизації;
– вибір параметрів відпалу для скорочення кількісті запусків задач комбінаторної оптимізації на КК.

Раціональні значення параметрів відпалу шукають за допомогою циклічного перезапуску задачі з різними параметрами, що називають варіаційним пошуком.

Побудова методики визначення раціональних параметрів квантового відпалу дозволить скоротити час розв'язування оптимізаційних задач на квантово-класичних хмарних сервісах, щоб зменшить витрати на аренду обчислювальних потужностей для низки задач реального сектору економіки.

Керування параметрами квантового відпалювача для покращення точності розв'язку оптимізаційних задач

Вбудовування оптимізаційної задачі у стани кубіт квантового відпалювача, відповідно до моделі Ізінга, є встановлення величини зміщень кубітів та сили зчеплень між ними. Для КК D-Wave функція, що відображає енергетичні стани (Гамільтоніан) має вид [5]:

$$H_{Ising} = \underbrace{-\frac{A(s)}{2}\left\{\sum_i \hat{\sigma}_x^{(i)}\right\}}_{\text{основний стан}} + \underbrace{\frac{B(s)}{2}\left\{\sum_i h_i \hat{\sigma}_z^{(i)} + \sum_{i>j} J_{i,j}\hat{\sigma}_z^{(i)}\hat{\sigma}_z^{(j)}\right\}}_{\text{збуджені стани}},$$

де $A(s)$ – це енергія тунелювання; $B(s)$ – енергія квантової системи з вбудованою задачею; $\hat{\sigma}_x^{(i)}$, $\hat{\sigma}_z^{(i)}$ – елементи матриці Паулі для *i*-го кубіта, h_i – зміщення для кубіта, J_{ij} – сила зв'язку між кубітами *i* та *j*; параметр *s* – нормований час процесу $0 \le s \le 1$ визначає режими відпалу. Зміщення кубіта (bias) h_i – це програмно задана величина, яка керується зовнішнім магнітним полем; величина зчеплення J_{ij} також задається у програмі, визначає силу зв'язків між кубітами (couples) та описує кореляцію їх станів або ступінь квантової спутаності між ними. Зміщення та зчеплення кубітів утворюють енергетичне поле, а КК D-Wave знаходить мінімальну енергію такого поля. Цей процес називається квантовим відпалом, який описується нелінійною залежністю енергії від часу [5, 6].

На рис. 1 показано спектр (суцільна лінія) власних значень квантової системи з низько-енергетичним основним станом внизу графіка без вбудовування задачі оптимізації і низкою збуджених станів (пунктирні лінії) з вбудованою задачею нагорі графіка. Квантовий відпалювач шукає збуджений стан з мінімальним зазором між ним і основним станом. Такий збуджений стан відповідатиме наближеному розв'язку задачі оптимізації.

РИС. 1. Спектр власних значень (енергетичних станів) квантової обчислювальної системи

Режими і параметри відпалу задають його розклад у часі t. Вони визначають нормалізовану частку відпалу $s(t) = t / t_f$, що є параметром, який змінюється від 0 до 1. $s(t)$ є безперервною монотонно зростаючою функцією, яка починається з $s(t) = 0$ для часу $t = 0$ і закінчується $s(t) = 1$ при

$t = t_f$, загального часу відпалу. Час відпалу (заданий виробником КК) на одне зчитування стану становить для КК фірми D-Wave: процесор Advantage $t_f = 0.01$ мікросекунди, процесор 2000Q – $t_f = 0.02$ мікросекунди [5, 6].

Процес квантового відпалу має параметри, які визначають режими його роботи [6]:
– час виконання відпалу (annealing time) t_f, який визначає кількість мікросекунд для лінійного зростання параметра $s(t)$ від 0 до 1;
– розклад відпалу (annealing schedule), який характеризується переліком пар (t, s), котрі задають точки для лінійної інтерполяції та задаються програмістом КК. Таких пар має бути не менше двох, їх кількість визначається фірмою D-Wave для кожного квантового процесора, наприклад, для 2000Q програмісту можна задати до чотирьох пар.

Побудова розкладу відпала виконується на основі режимів:
– пауза (pause) в процесі відпалу;
– загартовування (quench);
– пауза з загартовуванням.

Наприклад, розклад для квантового відпалу в режимі "пауза з загартовуванням" задається набором з чотирьох пар чисел, що на мові Python описується наступним двомірним масивом:
[[0.0, 0.0], [40.0, 0.4], [90.0, 0.4], [91.2, 1.0]], який описує процес відпалу.

Мета застосування різних режимів відпалу та варіації їх параметрів це введення квантової системи в стан з більш низькою енергією, що означає краще наближення розв'язку задачі оптимізації. Час виконання відпалу визначає час зростання функції відпалу [5, 6] (рис. 1, графік ground state/основний стан квантової системи). Розклад відпалу визначає параметри лінійної функції (рис. 2 – розклади), якою інтерполюється нелінійна функція відпалу.

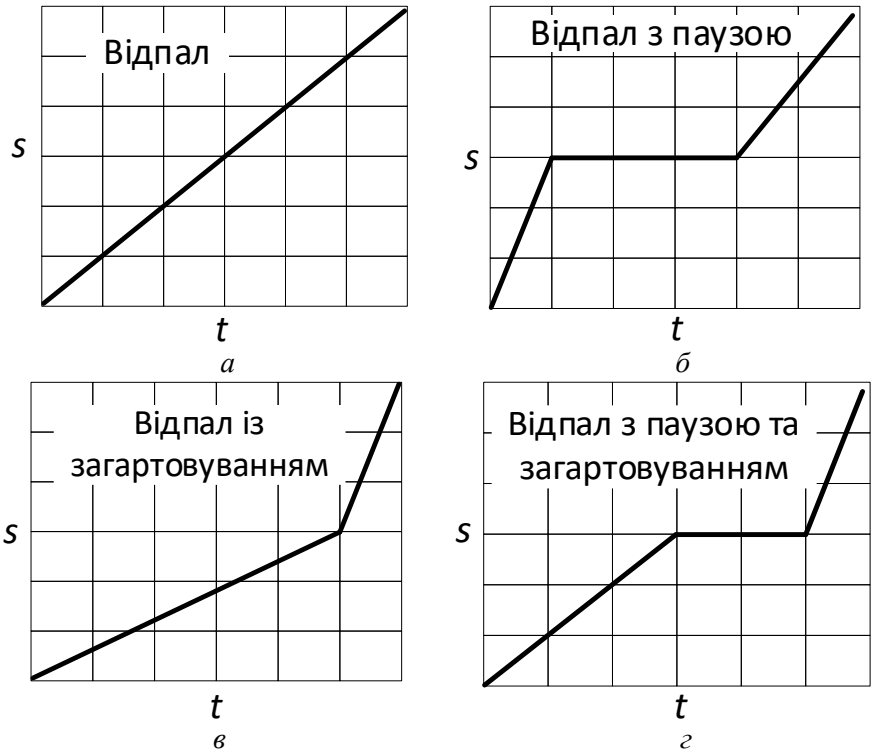


РИС. 2. *а* – відпал без варіації параметрів; *б* – розклад відпалу в режимі пауза; *в* – розклад відпалу в режимі загартовування; *г* –розклад відпалу в режимі паузи з загартовування

Розклад відпалу (рис. 2) впливає на формування основного стану квантової системи і відповідно на результат пошуку глобального мінімуму задачі комбінаторної оптимізації.

Зворотний відпал (рис. 3) – це підхід до розв'язування оптимізаційних задач, який дозволяє уточнювати відомі хороші локальні рішення, тим самим підвищуючи продуктивність обчислень для певних застосувань. Для виконання зворотного відпалу потрібно виконати спочатку (прямий) квантовий відпал для задачі оптимізації та отримати її розв'язок – вибірки, які є вхідними даними для зворотного відпалу. Алгоритм зворотного відпалу складається з таких кроків [6]:

1) відпал у зворотному напрямку від відомого класичного стану (квантового стану, що відповідає локальному мінімуму) до проміжного відпалу квантової суперпозиції;

2) пошук оптимальних рішень у цій точці середини відпалу в присутності збільшеного поперечного поля (квантовий стан);

3) перехід до нового класичного стану в кінці відпалу.

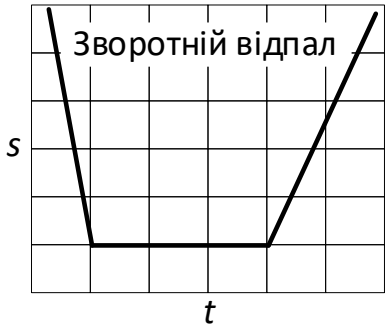


РИС. 3. Приклад побудови розкладу зворотного відпалу [[0.0, 1.0], [2.75, 0.45], [82.75, 0.45], [83.025, 1.0]]

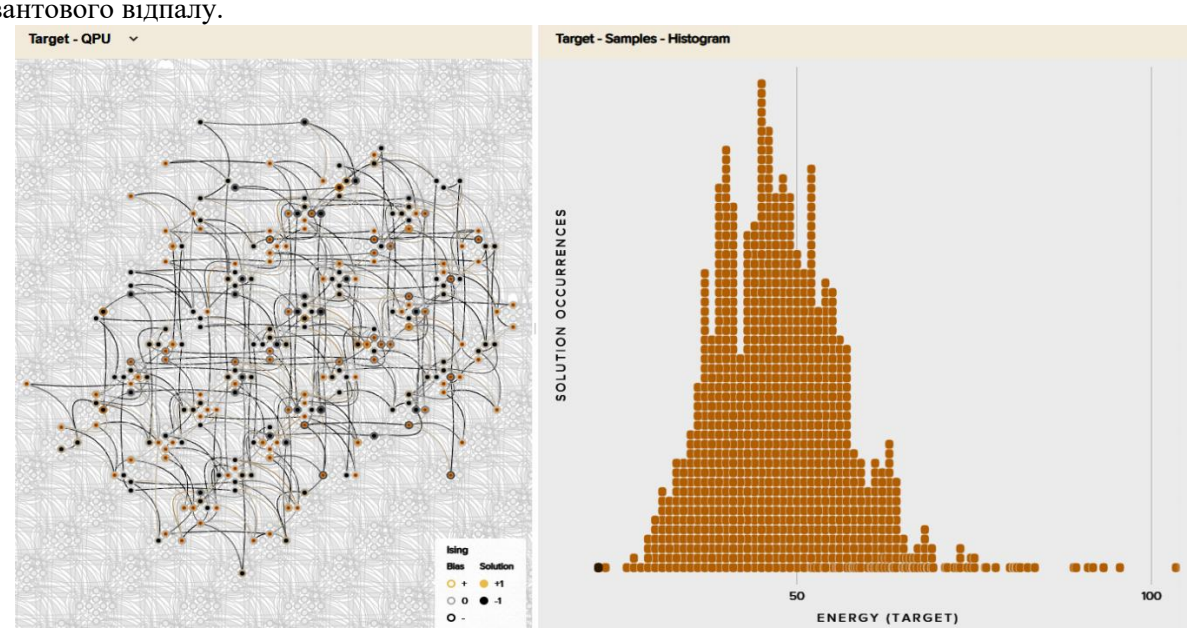
Алгоритм Шора для факторизації чисел передбачає програмування квантових логічних вентилів, що реалізовано КК IBM, фірма D-Wave анонсувала створення подібного інструментарію у 2022 році. Для КК D-Wave розроблено алгоритм факторизації [7] і вільне програмне забезпечення [8, 9], що ґрунтується на розв'язуванні задачі комбінаторної оптимізації з обмеженнями та квантових логічних схем множення. Для пошуку множників цей алгоритм [7] формує два бітові вектори однакової довжини, що дорівнює половині вхідного числа та обумовлює обмеження на значення шуканої пари чисел. Розв'язком задачі факторизації є множина пар чисел (множників), що відповідають низці енергетичних станів квантової системи. Оскільки на енергетичні стани реального квантового відпалювача діють теплові шуми, а кількість зв'язків між окремими кубітами є малою, то зі зростанням розрядності чисел статистичне розрізнення правильних пар множників погіршується і зрівнюється з неправильними. Втім, ситуацію можна покращити завдяки варіації параметрів квантового відпалу для КК D-Wave, що і є результатами досліджень викладеними у цій статті.

Окрім алгоритмічно-програмного забезпечення [7 – 9] іншими авторами досліджувалась факторизація для добутків простих чисел [10 – 14], а також запропоновано алгоритми факторизації, що засновані на скороченні колонок для добутку [13 – 16], що дозволило знайти одинадцятибітні множники для двадцятиодного бітного числа 1630729. Оскільки автори алгоритмів не надали відповідних програм, то перевірити можливість покращити точність розв'язку за допомогою зворотного квантового відпалу не є можливим.

Чисельні експерименти з розв'язування задачі факторизації за методом квантового відпалу показали, що збільшення сумарного часу відпалу понад $t_f = 500$ мікросекунд та кількості запусків задачі понад 1000 разів у більшості випадків не покращують якість розв'язку, а застосування режимів відпал з паузою та відпал з загартовування погіршують статистику для правильних розв'язків. Натомість процедура зворотного відпалу (за якою спочатку знаходять наближений розв'язок задачі

за методом прямого квантового відпалу, а потім шукають "глибший" енергетичний мінімум рухаючись від знайденого локального мінімуму також за методом квантового відпалу) підвищує точність розв'язку. Процедура зворотнього відпалу дозволяє отримати правильний розв'язок при кількості запусків прямого відпалу на порядок (10 разів) менше ніж зворотного відпалу (100 і 1000 запусків відповідно). Це дозволяє покращити результат без суттєвого при збільшенні запусків на 10 % порівняно зі звичайного процедурою відпалу. Вибір випадкового локального пошуку у дещо широкому інтервалі від початкового стану або детермінованого пошуку у вузькому інтервалі з однаковими кроками не вплинув на якість отриманих розв'язків або частоту їх появи. Параметр "сила зв'язку між кубітами" (chain strenght) склав 4 – 10.

В результаті розв'язування задачі факторизиції процесор DW_2000Q_6 за допомогою модифікованим авторами роботи програмного забезпечення для зворотного відпалу дозволяє [8, 9] отримати правильні множники для числа до 11*13 = 143, для більшого числа, наприклад, 15*17 = 255 довжини ланцюгів перевищують 7 і множники обчислюються неправильно. Для процесора Advantage4.1 17*19 = 323 обчислюється правильно (рис. 4), ланцюги, що перевищують 7 кубітів відсутні, тільки при 10000 запусків зворотного відпалу, для Advantage6.1 – 19*23 = 423 із аналогічними умовами. Температура квантової системи, що відповідає розв'язку не є мінімальною, кількість статистичних попадань 5–9 % при кількості запусків 1000 і більше, отже це правильний результат лише для пошуку пар множників. Тобто результат правильний, але він не є глобальним енергетичним мінімумом і, по-суті, є результатом перебору тисячі отриманих пар значень у результаті виконання квантового відпалу.



а *б*

РИС. 4. *а* – топологія розміщення кубітів та зв'язків для КК D-Wave Advantage6.1; *б* – гістограма для множини пар розв'язків для факторизації числа 423 = 19*23 для 10000 запусків задачі

Для квантово-класичного процесора hybrid_binary_quadratic_model_version2 максимальне значення склало 59*61 = 3599. Для гібридного алгоритма з табуйованим пошуком та симульованим відпалом 293*307 = 89951 з використанням бюджетного персонального комп'ютера середньої швидкодії за час 3–5 хвилин. У технічних звітах D-Wave та публікаціях незалежних дослідників стверджується, що за алгоритмом [7] і обчислювальними схемами [8, 9] можна знайти множники чисел значення яких коливаються навколо 291311 з використанням високопродуктивних обчислювальних серверів.

У таблиці авторами даної статті наведено результати розв'язку задачі факторизації за допомогою квантового відпалу та зворотного квантового відпалу (подано неповну множину пар множників з метою економії місця). Зворотній квантовий відпал показує більше ніж у два рази кращу статистику появи правильних пар множників порівняно з (прямим) квантовим відпалом. При застосуванні алгоритму для факторизації чисел з розрядністю вісім і більше біт починає даватись взнаки обмеження на кількість зв'язків між кубітами; процедура вбудовування задачі у КК використовує частину кубіт для передачі даних між квантовими логічними схемами, що погіршує підтримання низької температури і знижує статистику для правильного розв'язку з мінімальною енергією до одного або двох частот появи у гістограмі.

ТАБЛИЦЯ. Порівняння розв'язку задачі факторизації числа "21" за методом квантового відпалу та зворотного квантового відпалу (множини пар множників наведені частково)

Квантовий відпал			Зворотній квантовий відпал		
Множники	Правильність	Відсоток появи у чисельному та гістограма у псевдографічному поданні	Множники	Правильність	Відсоток появи у чисельному та гістограма у псевдографічному поданні
(7, 3)	Так	18 **********	(7, 3)	Так	39 **********
(3, 7)	Так	3 *	(3, 7)	Так	15 ********
(5, 5)	Ні	1	(5, 5)	Ні	3 *
(5, 1)	Ні	1	(5, 1)	Ні	3 *
(1, 5)	Ні	0	(1, 5)	Ні	7 ***
(7, 1)	Ні	5 **	(7, 1)	Ні	2 *
(3, 3)	Ні	2 *	(3, 3)	Ні	6 ***
(1, 7)	Ні	1	(1, 7)	Ні	5 **
(5, 7)	Ні	6 ***	(5, 7)	Ні	1
(3, 1)	Ні	1	(3, 1)	Ні	2 *
(1, 3)	Ні	1	(1, 3)	Ні	2 *
(3, 5)	Ні	1	(3, 5)	Ні	5 ***
(5, 3)	Ні	10 *****	(5, 3)	Ні	4 **
(1, 1)	Ні	0	(1, 1)	Ні	1
(7, 5)	Ні	2 *	(7, 5)	Ні	1
(5, 4)	Ні	0	(5, 4)	Ні	1
(3, 6)	Ні	1	(3, 6)	Ні	0
(7, 7)	Ні	8 ****	(7, 7)	Ні	0
(1, 4)	Ні	0	(1, 4)	Ні	0
(4, 3)	Ні	2 *	(4, 3)	Ні	0
(7, 4)	Ні	1	(7, 4)	Ні	0
(3, 4)	Ні	0	(3, 4)	Ні	0
(4, 7)	Ні	2 *	(4, 7)	Ні	0
(3, 0)	Ні	0	(3, 0)	Ні	0
(4, 1)	Ні	0	(4, 1)	Ні	0
(6, 3)	Ні	4 **	(6, 3)	Ні	0
(5, 2)	Ні	2 *	(5, 2)	Ні	0
(7, 0)	Ні	1	(7, 0)	Ні	0
(0, 3)	Ні	0	(0, 3)	Ні	0
(5, 6)	Ні	1	(5, 6)	Ні	0
(5, 0)	Ні	0	(5, 0)	Ні	0
(1, 6)	Ні	1	(1, 6)	Ні	0

Гістограма частот пар множників у таблиці позначена символами псевдографіки – "*".

Також помічено, що розв'язання задачі факторизації за методом відпалу показало сукупно більшу імовірність для пари множників, якщо принаймні один з них правильний. Це може бути корисним для побудови евристичного алгоритму прискорення пошуку множників для великих чисел, де результати мають низку статистичну і енергетичну розрізненість, оскільки реальні КК характеризуються високим рівнем шумів і обмеженою кількістю зв'язків між кубітами.

Результати. Дослідження результатів розв'язування задачі факторизації на КК за методом відпалу в різних режимах показало, що зворотній відпал дозволяє покращити статистику розв'язків для правильних множників більш ніж у два рази [18], а використання відпалу з режимами паузи та загартовування навпаки погіршують статистичний поріг достовірності розв'язків. Збільшення часу відпалу понад 500 мілісекунд та кількості запусків задачі факторизації понад 1000 разів у більшості випадків не покращує статистику появи правильних пар множників.

Висновки. Алгоритми асиметричної криптографії на яких ґрунтуються протоколи передачі ключів шифрування засновані на високій обчислювальній складності пошуку множників чисел великої розрядності для класичних комп'ютерів. Для теоретичних КК задача факторизації не має високої обчислювальної складності, тому КК створюють потенційну загрозу для систем захисту інформації [17, 19]. Алгоритми квантової наближеної оптимізації належать до класу квантово-класичних гібридних варіаційних алгоритмів методом відпалу. КК фірми D-Wave можуть обчислювати алгоритми лише з обмеженою глибиною квантової схеми, оскільки принцип роботи таких відпалювачів заснований на адіабатичній еволюції у часі квантової системи за обмежену кількість кроків. Основний квантовий стан обчислювача побудовано на моделі Ізінга – Гамільтона, яка використовується для розв'язування комбінаторних задач оптимізації. Оскільки задача Ізінга є NP-складною, вбудовування інших задач комбінаторної оптимізації у відповідну систему також може продемонструвати квантову перевагу.

Наближений алгоритм квантової оптимізації використовується для розв'язання задачі факторизації зі скінченною кількістю кроків адіабатичної еволюції і не гарантує, що отриманий розв'язок відповідає глобальному оптимальному розв'язку вихідної задачі. Так відбувається тому що в алгоритмі наближеної квантової оптимізації замість того, щоб поступово слідувати за еволюцією адіабатичного стану, алгоритм намагається вгадати його, використовуючи обмежену кількість кроків та евристики. З іншого боку, неточності в роботі наближених алгоритмів квантової оптимізації при більш високих значеннях кількості кроків в еволюції адіабатичного стану формують більше локальних мінімумів у енергетичному ландшафті розв'язку. Ця обставина ускладнює пошук мінімуму, тому необхідну кількість кроків слід підбирати за евристичним принципом та емпіричними підходами.

Список літератури

1. Moguel E., Rojo J., Valencia D. et al. Quantum service-oriented computing: current landscape and challenges. *Software Qual J*. 2022. https://doi.org/10.1007/s11219-022-09589-y
2. Wang Y., Liu H. Quantum Computing in a Statistical Context. *Annual Review of Statistics and Its Application*. 2022. Vol. 9:1. P. 479–504. https://doi.org/10.1146/annurev-statistics-042720-024040
3. Gill S.S., Kumar A., Singh H. Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*. 2022. **52** (1). P. 66–114. https://doi.org/10.1002/spe.3039
4. Корольов В.Ю., Ходзінський О.М. Розв'язування задач комбінаторної оптимізації на квантових комп'ютерах. *Cybernetics and Computer Technologies*. 2020. **2**. С. 5–13. https://doi.org/10.34229/2707-451X.20.2.1
5. What is Quantum Annealing? https://docs.dwavesys.com/docs/latest/c_gs_2.html (звернення: 08.09.2022)
6. QPU Solver Datasheet https://docs.dwavesys.com/docs/latest/doc_qpu.html (звернення: 08.09.2022)

7. Anschuetz E., Olson J., Aspuru-Guzik A., Cao Y. Variational Quantum Factoring. In: Feld, S., Linnhoff-Popien, C. (eds) *Quantum Technology and Optimization Problems. QTOP 2019. (Lecture Notes in Computer Science*). Vol. 11413. Springer, Cham. https://doi.org/10.1007/978-3-030-14082-3_7
8. Variational Quantum Factoring. https://github.com/mstechly/vqf (звернення: 08.09.2022)
9. D-Wave Examples. Factoring. https://github.com/dwave-examples/factoring (звернення: 08.09.2022)
10. Li Z.K., Dattani N.S., Chen X., Liu X. High-fidelity Adiabatic Quantum Computation Using the Intrinsic Hamiltonian of a Spin System: Application to the Experimental Factorization of 291311. *Quantum Physics.* 2017. P. 1–6. https://doi.org/10.48550/arXiv.1706.08061
11. Jiang S., Britt K.A., McCaskey A.J. et al. Quantum Annealing for Prime Factorization. *Scientific Report*. 2018. **8**. 17667. P. 1–9. https://doi.org/10.1038/s41598-018-36058-z
12. Gidney C. Factoring with N+2 Clean Qubits and N-1 Dirty Qubits. *Quantum Physics.* 2018. P. 1–14. https://doi.org/10.48550/arXiv.1706.07884
13. Kieu T.D. A factorisation algorithm in Adiabatic Quantum Computation. *Journal of Physics Communications*. **3**. 17667. 2019. https://doi.org/10.1088/2399-6528/ab060d
14. Baonan W., Feng H., Haonan Y., Chao W. Prime Factorization Algorithm Based on Parameter Optimization of Ising Model. *Scientific Report.* 2020. **10**. 7106. P. 1–10. https://doi.org/10.1038/s41598-020-62802-5
15. Peng W., Wang B., Hu F. et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. Science China Physics, Mechanics, Astronomy. 2019. **62** (6). 60311. https://doi.org/10.1007/s11433-018-9307-1
16. Warren R. H. Factoring on a Quantum Annealing Computer. *Quantum Information and Computation*. 2019. **19** (3–4). P. 252–261. https://doi.org/10.26421/qic19.3-4-5
17. Wang B., Yang X., Zhang D. Research on Quantum Annealing Integer Factorization Based on Different Columns. *Frontier Physics.* 2022. **10**. 914578. https://doi.org/10.3389/fphy.2022.914578
18. Factoring with Reverse Annealing. https://github.com/novice108/factorQuant/blob/main/factorRVS.py (звернення: 19.01.2023)
19. Корольов В.Ю., Огурцов М.І., Ходзінський О.М. Багаторівневе державне впізнавання об’єктів та аналіз застосовності пост-квантових криптографічних алгоритмів для захисту інформації. *Cybernetics and Computer Technologies*. 2020. **3**. С. 74–84. https://doi.org/10.34229/2707-451X.20.3.7

Одержано 17.02.2023

Корольов Вячеслав Юрійович,
кандидат технічних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0003-1143-5846

Ходзінський Олександр Миколайович,
кандидат фізико-математичних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ.
https://orcid.org/0000-0003-4574-3628
okhodz@gmail.com

УДК 519.6:511

В.Ю. Корольов, О.М. Ходзінський *

Дослідження впливу параметрів квантового відпалу на якість розв’язку задачі факторизації чисел

Інститут кібернетики імені В.М. Глушкова НАН України, Київ
** Листування: okhodz@gmail.com*

Вступ. Сучасні системи захисту інформації використовують методи асиметричної криптографії для передачі ключів шифрування, що ґрунтуються на високій обчислювальній складності факторизації вели-

ких чисел. Квантові комп'ютери (КК) теоретично дозволяють прискорити розв'язання задачі факторизації чисел порівняно з класичними комп'ютерами та створюють потенційну загрозу для систем захисту інформації. Втім, реальні КК мають обмежену кількість кубіті зв'язків між ними та проблеми з підтримкою стабільно низької температури, що знижує імовірність знайдення глобального мінімуму.

Сумісне використання КК з класичними комп'ютерами на базі гібридних хмарних сервісів є доцільним, коли пошук оптимального розв'язку прямими методами це складна проблема як в теоретичному сенсі, так і в сенсі необхідного обсягу розрахунків для задач з конкретними даними.

У статті запропоновано спосіб підвищення точності розв'язування задачі факторизації на основі багатократного пошуку мінімуму за методом апаратного зворотного квантового відпалу з варіацією його параметрів. Наведено результати чисельних експериментів для двох різних процесорів КК та гібридного квантово-класичного комп'ютера фірми D-Wave, показано, що максимальне число, що можна факторизувати за виключно прямим відпалом є 143, а за комбінацією прямого і зворотного відпалів – 255.

Мета роботи. Дослідження впливу параметрів відпалу і відповідних режимів для КК адіабатичного типу, побудованого фірмою D-Wave, на якість розв'язку задачі факторизації. Подати рекомендації до покращення точності розв'язку задачі факторизації та підвищення статистичної частоти появи правильних пар множників.

Результати. Чисельні експерименти показали, що для задачі факторизації чисел послідовне застосування прямого і зворотного відпалу дозволяє покращити імовірність отримання правильної пари множників та підвищити більш ніж у два рази статистичну частоту її появи.

Режими квантового відпалу: пауза і загартовування знижують імовірність отримання правильного розв'язку та погіршують статистичну частоту появи правильних пар множників.

Висновки. Використання прямого і зворотного відпалу дозволяє підвищити імовірність отримання правильного розв'язку задачі факторизації для адіабатичного КК фірми D-Wave. Збільшення часу обчислення задачі виправдано, оскільки дозволяє підвищити імовірність правильного розв'язку. Використання гібридних квантово-класичних обчислень та хмарних сервісів дозволяє виконувати факторизацію для чисел з розрядністю до двадцяти двох біт.

Ключові слова: квантовий відпал, факторизація натуральних чисел, асиметричні шифри, загартовування, зворотній відпал, комбінаторна оптимізація.

MSC 11A51

Vyacheslav Korolyov, Oleksandr Khodzinskyi *

A Research of the Influence of Quantum Annealing Parameters on the Quality of the Solution of the Number Factorization Problem

V.M. Glushkov institute of cybernetics of the NAS of Ukraine, Kyiv
* *Correspondence: okhodz@gmail.com*

Introduction. Modern information security systems use methods of asymmetric cryptography to transfer encryption keys, which are based on the high computational complexity of factorization of large numbers. Quantum computers (QCs) theoretically make it possible to accelerate the solution of the problem of factorization of numbers in comparison with classical computers and pose a potential threat to information security systems. However, real QCs have a limited number of connections between them and problems with preserving a stable low temperature, which reduces the probability of detecting a global minimum.

The joint use of QCs with classical computers based on hybrid cloud services is advisable when the search for the optimal solution by direct methods is a complex problem both in the theoretical sense and in the sense of the required amount of calculations for tasks with specific data.

The article proposes a method for improving the accuracy of solving the factorization problem based on multiple minimum search by the method of hardware reverse quantum annealing with a variation of its parameters. The results of numerical experiments for two different QC processors and a hybrid quantum-classical computer by D-Wave are presented, it is shown that the maximum number that can be factorized exclusively by direct annealing is 143, and with a combination of direct and reverse annealing 255.

The purpose. Examination of the influence of the parameters of quantum annealing and the corresponding solutions for the adiabatic CC, developed by D-Wave, on the quality of the solution of the factorization problem. To give recommendations for improving the accuracy of solving the factorization problem and increasing the statistical frequency of the appearance of correct pairs of multipliers.

Results. Numerical experiments have shown that for the problem of factorization of numbers, the successive application of direct and reverse annealing makes it possible to improve the probability of obtaining the correct pair of multipliers and to more than double the statistical frequency of its occurrence.

Quantum annealing modes: pause and quenching reduce the probability of obtaining the correct solution and worsen the statistical frequency of the appearance of correct pairs of multipliers.

Conclusions. The use of direct and reverse annealing makes it possible to increase the probability of obtaining the correct solution of the factorization problem for the adiabatic QC of D-Wave. Increasing the calculation time of the problem is justified, since it allows increasing the probability of a correct solution. The use of hybrid quantum-classical computing and cloud services allows factorization for numbers with a bit depth of up to twenty-two bits.

Keywords: quantum annealing, factorization of natural numbers, asymmetric shifts, hardening, reverse annealing, combinatorial optimization.