УДК 004.056.5 DOI:10.31673/25187678.2022.021014

Кожухівський А.Д., д.т.н.; **Гайдур Г.І.,** д.т.н.; **Кожухівська О.А.,** д.т.н.

КВАНТОВИЙ АЛГОРИТМ ПОШУКУ В НЕСТРУКТУРОВАНІЙ БАЗІ ДАНИХ

Kozhukhivskyi A.D., Haydur G.I., Kozhukhivska O.A. Quantum search algorithm in unstructured database. Grover's quantum algorithm was developed to solve the problem of searching an unstructured database for a certain unique element. In general, this problem can be formulated as follows: an unstructured database consists of elements and contains one unique element that has a certain property that can be tested with polynomial complexity, and which must be found with minimal time and complexity. Classical methods require querying the database to find the desired element, while Grover's algorithm allows you to perform only approximately steps, which are iterations of the procedure, to the database and be sure that the resulting element will be exactly the desired element with a probability close to 1. As in quantum algorithms aimed at cryptanalysis of symmetric transformations, Grover's algorithm repeats the procedure (Grover's iteration) to increase the probability of obtaining the correct result. Similarly to such algorithms in Grover's method, when iterations are continued after reaching the required number of iterations, the probability of obtaining the correct result decreases. This is due to the fact that during the execution of Grover's iteration, a rotation is performed in the complex space. Thus, each iteration, making a turn, brings the register closer and closer to the desired state, but at a certain point a maximum closeness is reached, at which the continued use of iterations will lead to a turn past the desired state, which will move the state of the system away from the desired state. The database for this algorithm can be any search space consisting of a certain number of elements. So, for example, it can be applied to find a secret key for a symmetric cryptograms formation or to find a collision for a hashing function.

***Keywords*:** Grover's quantum algorithm, unstructured database, unique element, collision, hashing function.

Кожухівський А.Д., Гайдур Г.І., Кожухівська О.А. Квантовий алгоритм пошуку в неструктурованій базі даних. Квантовий алгоритм Гровера розроблено для вирішення задачі проведення пошуку в неструктурованій базі даних певного унікального елемента. В загальному вигляді ця проблема може бути сформульована так: неструктурована база даних складається з N елементів та містить один унікальний елемент, що має певну властивість з поліноміальною складністю, який потрібно знайти з мінімальними витратами часу та складністю. Як і в квантових алгоритмах, в алгоритмі Гровера здійснюється повтор процедури (ітерації Гровера).

Ключові слова: Квантовий алгоритм Гровера, неструктурована база даних, унікальний елемент, колізія, функція гешування.

Вступ

Постановка задачі. Нині в криптографічному загалі широко обговорюється та досліджуються проблема створення та стандартизації перспективних криптографічних перетворень, в першу чергу для постквантового періоду [1, 2]. Суттєві результати досягнені в частині розроблення, стандартизації та застосування симетричних криптоперетворень [3]. Разом з тим, продовжується розвиток та здійснюються спроби розробити більш ефективні методи криптоаналізу симетричних криптосистем – симетричних блокових перетворень (СБП), симетричних потокових перетворень (СПП) та функцій гешування (ФГ). При цьому на сучасному етапі розглядаються деталізація, освоєння для застосування, перевірка криптоаналітичних властивостей та демонстрація застосування методу Гровера при криптоаналізі СБП, в тому числі, з методичним освоєнням методу при навчанні з використанням прикладів, але поки що на класичному комп'ютері.

Аналіз літературних джерел. Алгоритм Гровера будується з використанням методу Гровера, він є квантовим алгоритмом, що призначений для проведення вичерпного пошуку унікального елемента в несортованій базі даних, що містить $N = 2^n$ елементів, де $\boldsymbol{n}$ позначає довжину задіяного для представлення пошукового простору квантового регістра (кількість кубітів в ньому), а $\boldsymbol{N}$ є розміром пошукового простору [4, 5].

Невирішені питання. На основі аналізу літературних джерел можна зробити наступні висновки. Застосування методу Гровера для пошуку специфічного елемента в неструктурованій базі дійсно дозволяє досягти квадратичне прискорення пошуку, вимагає $\sqrt{N}$ раундів у порівнянні з N раундів грубої сили.

Мета та задачі дослідження. Метою роботи є дослідження алгоритму Гровера при пошуку унікального елемента в неструктурованій базі даних. Для досягнення мети дослідження розв'язуються такі наукові задачі: дослідження квантової схеми оракула; розробка блок-схеми алгоритму пошуку в неструктурованій базі даних.

Виклад основного матеріалу дослідження.

Одним з добре відомих класичних алгоритмів є алгоритм пошуку деякого обраного елемента з великого набору N елементів. Цей алгоритм входить в якості підпрограми у велетенське число різноманітних програм. З фізичної точки зору це відповідає пошуку білої кулі серед N - 1 чорних куль, що лежать в урні. Зрозуміло, не можна підглядати, а можна тільки виймати кулі по черзі і тоді розглядати їх, визначаючи, чи вийняли потрібну кулю або ні. Біла куля буде знайдена класичним алгоритмом з вірогідністю 1/2 після N/2 спроб. Чи існує алгоритм пошуку, що дозволяє знайти потрібний елемент за менше число спроб? Несподівано виявилось, що такий алгоритм існує. Саме такий, але вже квантовий алгоритм пошуку був запропонований Гровером. Важливість існування такого алгоритму в тому, що він демонструє переваги квантових обчислень над класичними. Тому обговоримо цей алгоритм детальніше.

Нехай серед N = $\boldsymbol{2^n}$ елементів треба вибрати один. Розпочнемо з того, що кожному елементу $\boldsymbol{x_i}$ зіставимо певний стан $\boldsymbol{n}$ кубітів виду $|\dots, \mathbf{0}, \mathbf{0}, \dots, \mathbf{1}, \mathbf{0}, \mathbf{1}, \dots, \mathbf{1}\rangle$. Таких станів рівно N = $\boldsymbol{2^n}$. Тому одному елементу можна зіставити рівно один стан. Тоді завдання зводиться до пошуку одного стану, що відповідає шуканому елементу серед $\boldsymbol{2^n}$ станів. Для того, щоб можна було виділити шуканий елемент від інших елементів $\boldsymbol{x_i}$, і $\neq 0$, він повинен відрізнятися від них. Іншими словами, шуканий елемент повинен мати властивість, що відрізняє його від інших елементів. У фізичному прикладі це був колір кулі.

З формальної точки зору існування такої властивості означає існування функції C (x), такої, що C ($\boldsymbol{x_0}$) = 1, а C ($\boldsymbol{x_i}$) = 0, якщо і ≠ 0. Тоді можна припустити, що можна побудувати квантову схему, яка в стані розрізняти шуканий стан кубітів від інших станів. Якщо не вдаватися до внутрішнього устрою такої схеми, то її дію можна зображувати, як на рис. 1. Важливо відмітити, що дія цієї схеми оборотна і, отже, такий унітарний оператор може бути побудований. Часто така схема називається оракулом.

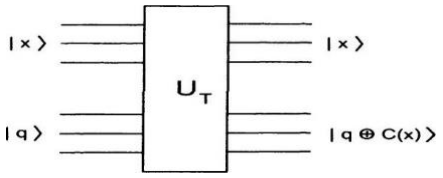

Рис. 1. Квантова схема, яка здатна відрізнити шуканий стан від інших станів

Таким чином, дія цієї квантової схеми на базисні стани описується як $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}|\boldsymbol{x}\rangle|\boldsymbol{q}\rangle = |\boldsymbol{x}\rangle|\boldsymbol{q}\oplus\boldsymbol{C}(\boldsymbol{x})\rangle$, де $|\boldsymbol{x}\rangle$ стан "верхніх" кубітів, а $|\boldsymbol{q}\rangle$ – стан кубітів схеми, що перевіряє. Символ | 〉 уведений Діраком [6]. Знак ⊕, як і раніше, означає складання за модулем 2. Легко помітити, що якщо подіяти схемою $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}$ на стан $|\boldsymbol{x_0}\rangle\,|\mathbf{0}\rangle$, то схема переведе кубіт оракула в стан $|\mathbf{1}\rangle$. Проте дію оракула можна привести до простішої і зручнішої форми. Для цього розглянемо дію цієї схеми, якщо кубіт оракула знаходиться в стані суперпозиції виду $\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}$ ($|\mathbf{0}\rangle - |\mathbf{1}\rangle$). Дія $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}$ на такий стан кубітів зводиться до наступного виразу:

$\widehat{\boldsymbol{U}}_{\boldsymbol{T}}|\boldsymbol{x}\rangle\left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle-|\mathbf{1}\rangle)\right)=(-\mathbf{1})^{\boldsymbol{C}(\boldsymbol{x})}|\boldsymbol{x}\rangle\left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle-|\mathbf{1}\rangle)\right)$. Найважливіше спостереження з цього рівняння, що стан кубітів оракула не міняється при функціонуванні цієї схеми. Це означає, що можна не стежити за станами кубітів оракула і звести дію цієї схеми до наступної:

$\widehat{\boldsymbol{U}}_{\boldsymbol{T}}|\boldsymbol{x}\rangle=(-\mathbf{1})^{\boldsymbol{C}(\boldsymbol{x})}|\boldsymbol{x}\rangle$. Слід підкреслити, що ця схема не здійснює пошук як такий. Її роль зводиться тільки до розпізнавання властивостей станів кубітів, що пред'являються їй. Якщо повернутися до класичного прикладу з кулями, то її роль зводиться до можливості відрізнити чорний колір кулі від білого. Тепер приведемо блок-схему алгоритму Гровера, що здійснює пошук потрібного елемента в неструктурованій базі даних (рис. 2).

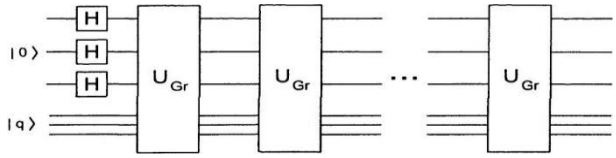

Рис. 2. Блок- схема Гровера квантового алгоритму пошуку

На вхід цієї схеми подаються кубіти в нульових станах $|\mathbf{0}\rangle$. Подальша дія на них операторів Адамара $\boldsymbol{H}^{\otimes\boldsymbol{n}}$ приводить їх стан в стан однорідної суперпозиції $|\boldsymbol{\varphi}\rangle=\frac{\mathbf{1}}{\sqrt{N}}\sum_{\mathbf{0}}^{\boldsymbol{N}-\mathbf{1}}|\boldsymbol{x}\rangle$. Залишається розглянути облаштування квантової схеми, що відповідає дії унітарного оператора $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}$. Ця квантова схема приведена на рис. 3.

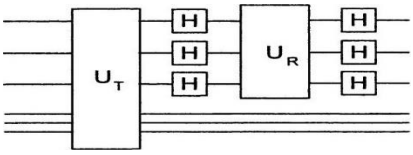

Рис. 3. Квантова схема, що пояснює "мікроскопічний" пристрій оператора Гровера $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}$

Опишемо дію унітарного оператора $\widehat{\boldsymbol{U}}_{\boldsymbol{R}}$, що входить в цю схему. Його дія зводиться до зсуву фази відповідно до правил $\widehat{\boldsymbol{U}}_{\boldsymbol{R}}|\mathbf{0}\rangle=|\mathbf{0}\rangle$, $\widehat{\boldsymbol{U}}_{\boldsymbol{R}}|\boldsymbol{x}\rangle=-|\boldsymbol{x}\rangle$, якщо x ≠ 0. Цей оператор легко записати в термінах проєкційних операторів як $\widehat{\boldsymbol{U}}_{\boldsymbol{R}}=\mathbf{2}|\mathbf{0}\rangle\langle\mathbf{0}|-\boldsymbol{I}$, де $\boldsymbol{I}$ – одиничний оператор, що не міняє стан. Таким чином, схема оператора Гровера влаштована досить просто. Легко зрозуміти, що її можна також записати, використовуючи формалізм проекційних операторів у виді $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}=(\mathbf{2}|\boldsymbol{\varphi}\rangle\langle\boldsymbol{\varphi}|-\boldsymbol{I})\,\widehat{\boldsymbol{U}}_{\boldsymbol{T}}$. Тепер розглянемо процес здійснення пошуку квантовим алгоритмом. Припустимо для простоти, що шуканий стан тільки один - $|\boldsymbol{x}_{\mathbf{0}}\rangle$. Для розуміння дії алгоритму зручно перейти до простих геометричних представлень.

Для цього представимо стан $|\boldsymbol{\varphi}\rangle$ у вигляді суми двох одиничних векторів. Вектора $|\boldsymbol{\alpha}\rangle=\frac{\mathbf{1}}{\sqrt{\boldsymbol{N}-\mathbf{1}}}\sum_{\boldsymbol{x}\neq\boldsymbol{x}_{\mathbf{0}}}|\boldsymbol{x}\rangle$, де підсумовування виконується по усіх станах, за винятком шуканого стану при пошуку. Другий вектор, в нашому випадку, це шуканий вектор $|\boldsymbol{\beta}\rangle=|\boldsymbol{x}_{\mathbf{0}}\rangle$. У більш загальному випадку, якщо шукається декілька векторів, то вектор $\boldsymbol{\beta}$ вибирається у вигляді однорідної суперпозиції шуканих станів. Таким чином,

$$|\boldsymbol{\varphi}\rangle=\frac{\sqrt{\boldsymbol{N}-\mathbf{1}}}{\sqrt{\boldsymbol{N}}}|\boldsymbol{\alpha}\rangle+\frac{\mathbf{1}}{\sqrt{\boldsymbol{N}}}|\boldsymbol{\beta}\rangle. \quad (1)$$

У такому представленні вектор $|\boldsymbol{\varphi}\rangle$ розташований в площині, "натягнутій" на вектори $|\boldsymbol{\alpha}\rangle$ і $|\boldsymbol{\beta}\rangle$. Амплітуди при цих векторах можна записати в термінах кута між вектором $|\boldsymbol{\varphi}\rangle$ і напрямом, наприклад, вектора $|\boldsymbol{\alpha}\rangle$ (див. Рис. 4) $|\boldsymbol{\varphi}\rangle=\mathbf{cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\alpha}\rangle+\sin\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\beta}\rangle$.

Для аналізу дії оператора $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}$ розглянемо спочатку дію оракула на стан (1). Легко зрозуміти, що $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}|\boldsymbol{\varphi}\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|\boldsymbol{\alpha}\rangle - \frac{1}{\sqrt{N}}|\boldsymbol{\beta}\rangle$. У такій дії оператора легко узнати відображення вектора $|\boldsymbol{\varphi}\rangle$ відносно осі $|\boldsymbol{\alpha}\rangle$. В термінах кута результат дії $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}$: $\widehat{\boldsymbol{U}}_{\boldsymbol{T}}|\boldsymbol{\varphi}\rangle = \mathbf{cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right), |\boldsymbol{\alpha}\rangle = \sin\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right), |\boldsymbol{\beta}\rangle$ зводиться до заміни $\boldsymbol{\theta} \rightarrow -\boldsymbol{\theta}$. Тепер подіємо на отриманий стан кубітів оператором $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}} = (\mathbf{2}|\boldsymbol{\varphi}\rangle\langle\boldsymbol{\varphi}| - \boldsymbol{I})$. Дія цього оператора на довільний вектор зводиться до його відображення відносно осі, що задається вектором станів $|\boldsymbol{\varphi}\rangle$ [7].

$$(\mathbf{2}|\boldsymbol{\varphi}\rangle\langle\boldsymbol{\varphi}| - \boldsymbol{I})\left(\mathbf{cos}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\alpha}\rangle - \mathbf{sin}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\beta}\rangle\right) = \left(\mathbf{cos}\left(\frac{\mathbf{3}\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\alpha}\rangle + \mathbf{sin}\left(\frac{\mathbf{3}\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\beta}\rangle\right).$$

Це означає, що $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}|\boldsymbol{\varphi}\rangle = \left(\mathbf{cos}\left(\frac{\mathbf{3}\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\alpha}\rangle + \mathbf{sin}\left(\frac{\mathbf{3}\boldsymbol{\theta}}{\mathbf{2}}\right)|\boldsymbol{\beta}\rangle\right)$.

Таким чином, в площині, "натягнутій" на вектори $|\boldsymbol{\alpha}\rangle$ і $|\boldsymbol{\beta}\rangle$, дія оператора Гровера на вектор однорідної суперпозиції $|\boldsymbol{\varphi}\rangle$ зводиться до повороту його на кут $\boldsymbol{\theta}$ у напрямі осі $|\boldsymbol{\beta}\rangle$ (рис. 4) [7].

Рис. 4. Символічно показані зміни амплітуд базисних станів, що входять у вигляді рівноправної суперпозиції, під впливом оператора $\widehat{\boldsymbol{U}}_{\boldsymbol{gr}}$

Враховуючи, що в задачі пошуку інтерес представляє ситуація, коли $\boldsymbol{N} \gg \mathbf{1}$, тому вектор спрямований практично уздовж осі $|\boldsymbol{\alpha}\rangle$. Це означає малу величину кута $\boldsymbol{\theta} \ll 1$ і для оцінки використовуємо $\mathbf{sin}\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right) \approx \frac{\boldsymbol{\theta}}{\mathbf{2}} = \frac{\mathbf{1}}{\sqrt{N}}$. Отже, можна знайти значення *m*, при якому кут $\frac{\mathbf{2}\boldsymbol{m}+\mathbf{1}}{\mathbf{2}}\boldsymbol{\theta}$ стане порядку $\frac{\boldsymbol{\pi}}{\mathbf{2}}$ і результуючий вектор стану буде спрямований уздовж осі $|\boldsymbol{\beta}\rangle$. Прирівнюючи $\frac{\mathbf{2}\boldsymbol{m}+\mathbf{1}}{\mathbf{2}}\boldsymbol{\theta} \approx \frac{\boldsymbol{\pi}}{\mathbf{2}}$, і підставивши значення $\boldsymbol{\theta}$, отримаємо $\frac{\mathbf{2}\boldsymbol{m}+\mathbf{1}}{\mathbf{2}}\mathbf{2} \approx \frac{\boldsymbol{\pi}\sqrt{\boldsymbol{N}}}{\mathbf{2}}$.

Після проведення елементарних перетворень і нехтуючи одиницею в порівнянні з 2*m*, знайдемо m $\approx \frac{\boldsymbol{\pi}\sqrt{\boldsymbol{N}}}{\mathbf{4}}$. Це означає, що після приблизно $\frac{\boldsymbol{\pi}\sqrt{\boldsymbol{N}}}{\mathbf{4}}$ застосувань оператора Гровера амплітуда стану $|\boldsymbol{\beta}\rangle = |\boldsymbol{x}_{\mathbf{0}}\rangle$ стане близькою до одиниці, а амплітуди при інших базисних станах стануть дуже малі (рис. 5).

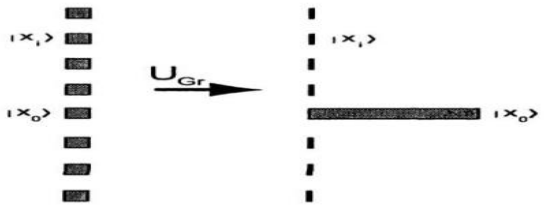

Рис. 5. Символічно показані зміни амлітуд базисних станів при $\frac{\boldsymbol{\pi}\sqrt{\boldsymbol{N}}}{\mathbf{4}}$ - кратному застосуванні оператора Гровера

Висновки

Використовуючи чудовий квантовий алгоритм Гровера, можна знайти елемент $|\boldsymbol{x}_{\mathbf{0}}\rangle$ з набору N елементів за $\sqrt{\boldsymbol{N}}$ кроків. В порівнянні з класичним алгоритмом пошуку, приблизно за N/2 кроків, перевага досить помітна.

Список використаної літератури

1. Neal Koblitz and Alfred J. Menezes A Riddle wrapped in an Enigma. Department of Mathematics, Box 353.350, University of Washington, Seattle, WA 98195 U.S.A. – Access mode: https://eprint.iacr.org/2015/1018.pdf.

2. Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // – Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

3. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія. / Ю. І. Горбенко. Х. : Форт, 2016. – 959 с.

4. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Round 3 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

5. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І. Горбенко, Є. Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. Вип. 195. – С. 89-100.

6. Дирак П., Принципы квантовой механики / П. Дирак.- М.: Наука, 1979.- 480 с.

7. D.Aharonov, Quantum computation, In D.Stauffer, editor, Annual Reviews of computational Physics VI., World Scientific, Singapore, 1999.

Автори статті

Кожухівський Андрій Дмитрович – доктор технічних наук, професор, професор кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Гайдур Галина Іванівна - доктор технічних наук, професор, зав. кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Кожухівська Ольга Андріївна - доктор технічних наук, доцент кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Kozhukhivskyi Andrii Dmytrovych – Doctor of Science (technic), Professor, Professor of Information and Cybernetic security of State University of Telecommunications, Kyiv, Ukraine.

Haydur Halyna Ivanivna - Doctor of Science (technic), Professor, chief Department of Information and Cybernetic Security, State University of Telecommunications, Kyiv, Ukraine.

Kozhukhivska Olga Andriivna - Doctor of Science (technic), Associate Professor Department of Information and Cybernetic Security, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 10.01.2022 р. Рецензент: д.т.н., проф. В.А. Савченко