УДК 519.2:519.7: 003.026

Ю.І. ГОРБЕНКО, канд. техн. наук, Є.Ю. КАПТЬОЛ

СУТНІСТЬ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МЕТОДУ ГРОВЕРА НА КЛАСИЧНОМУ КОМП'ЮТЕРІ ДЛЯ СИМЕТРИЧНОГО КРИПТОАНАЛІЗУ

Вступ

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 досягнуто в частині розроблення, стандартизації та застосування симетричного криптоперетворення [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). Підтвердженням цьому є прийняття та застосування міжнародних ДСТУ ISO/IEC 18033-3, 18034-4, ДСТУ 7624:2014, ДСТУ 7564:2014, FIPS – 197, FIPS – 202 тощо. При цьому, великий інтерес до задач криптоаналізу проявляють як безпосередньо криптоаналітики так і розробники стандартизованих симетричних та асиметричних криптосистем.

Зрозуміло, що криптоаналітики направляють свої зусилля на безпосередній злам відповідних криптосистем, а розробники та ті, що застосовують криптографічні перетворення, – на перевірку їх криптографічних властивостей. Якщо раніше для спроб вирішення задач криптоаналізу застосовувались класичні спеціалізовані комп'ютерні системи, засоби та класична математика, то нині розробляються квантові комп'ютери та практично розроблені відповідні квантові математичні методи [1 – 3]. Але освоєння та застосування квантових систем та квантових математичних методів, а також програмування носить як методологічний аспект, так і психологічний – складність сприйняття.

Дослідження, що проведені, дозволяють прогнозувати використання для симетричного криптоаналізу квантового методу, що отримав назву методу Гровера [3, 4].

Метою цієї статі є деталізація, освоєння для застосування, перевірка криптоаналітичних властивостей та демонстрація застосування методу Гровера при криптоаналізі СБП, в тому числі і з методичними цілями освоєння методу при навчанні з використанням прикладів, але поки що на класичному комп'ютері.

Сутність особливості методу гровера

У загальній постановці сутність метода Гровера полягає в проведенні вичерпного пошуку специфічного (унікального) елементу у несортованій базі даних, що складається з $N = 2^n$ елементів, де n – довжина квантового регістру (кількість кубітів) [4]. Для криптоаналізу СБП специфічність елементу може зводитись до сеансового чи довгострокового ключа, сінхропослідовності тощо. Особливістю, наприклад, ключа є те, що при його застосуванні зашифровані дані можуть бути розшифрованими за поліноміальний час.

У порівнянні з найкращими класичними методами метод Гровера передбачає проведення пошуку з квадратичним прискоренням, замість $O(N)$ всього за $O(\sqrt{N})$ групових операцій. Для отримання такого прискорення використовується квантова суперпозиція станів. Причому, як показує аналіз, основним застосуванням методу Гровера є реалізований на його основі алгоритм криптоаналізу СБП Гровера. Зрозуміло, чому метод носить узагальнений зміст, так метод може бути реалізований у вигляді алгоритму криптоаналізу СП, ФГ, асиметричного шифру в кільці поліномів тощо [3, 4].

Наше обґрунтування методу Гровера ґрунтуються на його потенційних можливостях. Так, в табл. 1 наведено результати розрахунку стійкості СБП проти квантового криптоаналізу [4]. Наведені в табл. 1 дані дозволяють зробити висновок, що при розробленні

та введенні в експлуатацію хоча б одного квантового комп'ютера, значне число симетричних криптоперетворень буде зламаними, а деякі будуть під суттєвою підозрою.

Таблиця 1

Стійкість симетричних криптосистем проти квантового криптоаналізу на основі методу Гровера [3, 4]

№ п/п	Шифр	Параметри		Стійкість при атаці на	
		Розмір блока, біт	Розмір ключа, біт	блок повідомлення	ключ
1	AES-128	128	128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
2	AES-256	128	256	2^{64} ($10^{19,2}$)	2^{128} ($10^{38,4}$)
3	DES	64	56	2^{32} ($10^{9,6}$)	2^{28} ($10^{8,4}$)
4	TDES	64	168	2^{32} ($10^{9,6}$)	2^{134} ($10^{40,2}$)
5	ГОСТ-28147	64	256	2^{32} ($10^{9,6}$)	2^{128} ($10^{38,4}$)
6	Калина-128	128	128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
7	Blowfish	64	448	2^{32} ($10^{9,6}$)	2^{224} ($10^{67,2}$)

Спочатку розглянемо сутність та зробимо відповідний аналіз методу Гровера та етапів його виконання.

1. На першому кроці квантовий регістр з n кубітів, необхідних для представлення пошукового простору розміру $N = 2^n$, встановлюється у стан $|0\rangle$ у вигляді

$$|0\rangle^{\otimes n} = |0\rangle \tag{1}$$

Після цього квантова система встановлюється в стан рівної суперпозиції станів. Для цього над квантовим регістром з n кубітами виконується перетворення Адамара $H^{\otimes n}$, що складається з використання n звичайних гейтів (вентилів) Адамара 3]:

$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{2}$$

2. На другому кроці $\frac{\pi}{4}\sqrt{2^n}$ разів застосовуються ітерації Гровера. Така кількість застосування ітерації Гровера зумовлюється необхідністю отримання реальної оптимальної ймовірності того, що отриманий стан системи буде саме тим, який шукається, а також необхідністю того, що необхідний стан матиме загальне зміщення фази не більше $\frac{\pi}{4}$ радіани [4]. Причому, кожна ітерація Гровера проводить амплітудне підсилення ймовірності знаходження елементу бази, що шукається. Кожна ітерація Гровера складається із застосування квантового оракула O та застосування оператора дифузії.

Спочатку йде виклик квантового оракула O, що модифікує систему в залежності від того, чи знаходиться система в необхідному стані. Оракул характеризується тим, що може аналізувати та модифікувати систему без зведення її до класичного стану, тобто продовжує знаходиться в квантовому стані. Конкретна реалізація квантового оракула залежить від кожного окремого випадку та задачі. Наприклад , у випадку криптоаналізу СБП оракул виконує розшифрування на ключі та повертає результат – успіх чи ні. Спільним для кожного оракула є те, що він розпізнає, чи знаходиться система в правильному стані та, якщо система знаходиться в правильному стані, оракул повертає фазу на π радіани, в іншому ж випадку він не робитиме нічого, позначивши правильний стан для подальших модифікацій наступними операціями. Причому, через зсув фаз можлива ситуація, коли правильний стан залишається тим самим, хоча його амплітуда матиме протилежний знак.

Ефект реакції оракула на систему (x) можна відобразити як

$$|x\rangle \xrightarrow{\text{O}} (-1)^{f(x)}|x\rangle, \tag{3}$$

де $f(x)=1$, якщо система знаходиться в правильному стані (успішному) та $f(x)=0$ – в іншому випадку. Точна реалізація оракула залежить від $f(x)$, а $f(x)$ залежить від задачі пошуку. Як уже зазначалось, у випадку криптоаналізу СБП, $f(x)=1$, якщо розшифрування на даному ключі оракулом є успішним.

Наступна частина ітерації Гровера називається оператором дифузії. Оператор дифузії проводить інверсію щодо середнього. Амплітуда кожного стану перетворюється так, щоб вона була набагато вищою за середнє настільки, наскільки вона була нижчою за середнє значення, та навпаки.

Оператор дифузії складається з трьох послідовних операцій: застосування перетворення Адамара $H^{\otimes n}$, умовного фазового зсуву, котрий зсуває кожен стан, окрім $|0\rangle$, на -1, та ще одного застосування перетворення Адамара $H^{\otimes n}$. Умовний фазовий зсув відображається унітарним оператором $2|0\rangle\langle 0|-I$ [5]:

$$\begin{aligned}\left[2|0\rangle\langle 0|-I\right]|0\rangle &= 2|0\rangle\langle 0|0\rangle - I = |0\rangle \\ \left[2|0\rangle\langle 0|-I\right]|x\rangle &= 2|0\rangle\langle 0|x\rangle - I = -|x\rangle\end{aligned} \tag{4}$$

Згідно з нотацією (2) стосовно $|\psi\rangle$ та за врахування (4) отримуємо оператор дифузії як

$$H^{\otimes n}\left[2|0\rangle\langle 0|-I\right]H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\psi\rangle\langle\psi| - I \tag{5}$$

З урахуванням оракула O (3) та оператора дифузії (5), повну ітерацію Гровера можна подати у вигляді

$$\left[2|\psi\rangle\langle\psi|-I\right]\text{O}\,. \tag{6}$$

Аналіз показує, що основною вимогою до ітерації Гровера є вимога мінімізації її складності (часу виконання). Слід відмітити, що складність і відповідно точний час виконання оракула залежить від конкретних задач і реалізацій. Тому виклик оракула звичайно розглядається як одна елементарна операція.

Загальна складність (час виконання) однієї ітерації Гровера становить $O(2n)$, що пояснюється необхідністю виконання двох перетворень Адамара, а також складності застосування $O(n)$ вентилів при виконанні умовного фазового зсуву зі складністю $O(n)$. У цілому складність виконання всього алгоритму Гровера можна оцінити як $O(\sqrt{N}) = O(\sqrt{2^n}) = O(2^{\frac{n}{2}})$ ітерацій, кожна зі складністю $O(n)$.

Схематичне зображення алгоритму Гровера з додатковим кубітом для оракула згідно з [3] наведено на рис. 1.

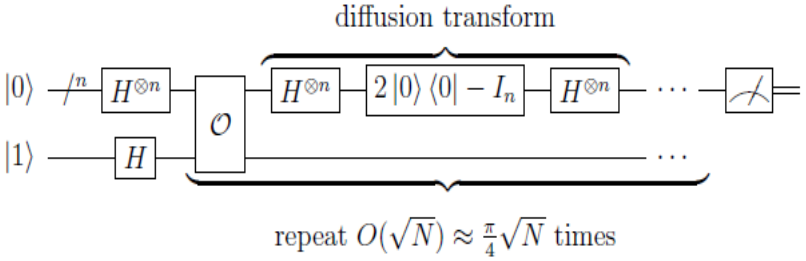


Рис.1. Алгоритм Гровера з додатковим кубітом для оракула

Для визначення результату виконання ітерації Гровера виконуються класичні вимірювання, причому результат буде правильним з достатньо високою ймовірністю. На цьому виконання алгоритму Гровера завершується, його складність становить $O(1)$ [4, 5].

Необхідно відмітити, що алгоритм Гровера є квантовим алгоритмом і вимагає застосування квантового комп'ютера та квантової математики. По суті квантова математика методу Гровера наведена вище, формули (1) – (6) та на рис. 1. Квантовий комп'ютер ще недоступний. Проте його можна реалізувати на класичному комп'ютері. Але слід зауважити, що реалізація його на класичному комп'ютері, що не підтримує квантові властивості, не є прийнятною передусім з точки зору складності (часу) виконання. Так, на квантовому комп'ютері, завдяки квантовим властивостям, наприклад можливість обстежувати весь регістр одразу без розгляду кожного окремого елемента, оракул розглядається як одна елементарна операція, а її виконання займає набагато менше потужності (часу), ніж це потребує на класичному комп'ютері. Тобто, виконання алгоритму Гровера на класичному комп'ютері є суттєво складнішим. Так, по суті лише реалізація оракула замість $\sqrt{N}$ звертань потребуватиме $N\sqrt{N}$ звертань. Відповідно час застосування алгоритму зростає настільки, що використання методу Гровера буде повільнішим, навіть у порівнянні зі складністю пошуку ключа СБП методом «грубої сили» тощо.

З метою демонстрації практичної реалізації методу Гровера розглянемо його на прикладі алгоритму пошуку унікального елементу при симетричному перетворенні.

Приклад 1. Припустимо, що система складається з $N = 16 = 2^4$ станів, і стан, який ми шукаємо, x_0, має індекс 7 та представлений бітовою строчкою $|7\rangle = |0111\rangle$. Розглянемо алгоритм Гровера пошуку данного «унікального» елемента по кроках.

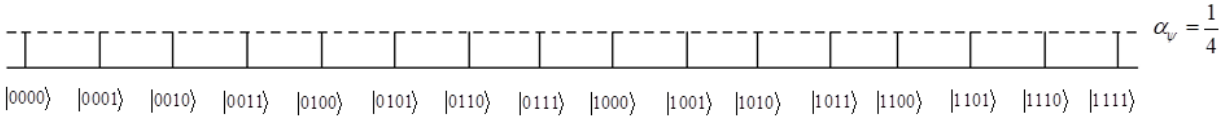
1. Для того щоб описати цю систему, потрібно $n = 4$ кубіти. У відповідності до алгоритму Гровера зробимо ініціалізацію квантового регістру з $n = 4$ кубітів, що необхідне для представлення пошукового простору розміру $N = 2^4$, встановивши регістр у початковий стан:

$$|\psi_0\rangle = |0000\rangle$$

2. Проведемо перетворення Адамара, що дозволяє отримати значення амплітуди, що пов'язана з кожним станом з рівною ймовірністю перебування в кожному з 16 можливих станів:

$$|\psi\rangle = H^{\otimes 4}|0000\rangle = (H|0\rangle)^{\otimes 4} = \frac{1}{4}\sum_{i=0}^{15}|i\rangle$$

Геометрично це можна зобразити як



3. За вказаних даних оптимальним для отримання рішення є виконання ітерацій Гровера, кількість яких визначається таким чином:

$$\frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{16} = \frac{4\pi}{4} = \pi \approx 3.14$$

В подальшому для використання округлимо число ітерацій до трьох. В кожній ітерації першим кроком є виклик квантового оракула O, потім проводиться інверсія середнього, або ж оператор дифузії.

4. При пошуку елементу з індексом 7 оракул дає такі значення [3, 4]:

$$U_f(|0111\rangle|-\rangle) = -|0111\rangle|-\rangle; \qquad U_f(|i\rangle|-\rangle) = |i\rangle|-\rangle, \text{ if } i \neq 7;$$

5. Далі визначимо $|u\rangle$ використовуючи (2), в результаті маємо

$$|u\rangle = \frac{1}{\sqrt{15}}\sum_{\substack{i=0\\ i\neq 7}}^{15}|i\rangle = \frac{\begin{array}{c}|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle+|0101\rangle+|0110\rangle+|1000\rangle+|1001\rangle+|1010\rangle\\ +|1011\rangle+|1100\rangle+|1101\rangle+|1110\rangle+|1111\rangle\end{array}}{\sqrt{15}}$$

Також аналогічно (2) маємо, що $|\psi\rangle = \frac{\sqrt{15}}{4}|u\rangle + \frac{1}{4}|0111\rangle$

6. Наступним кроком знайдемо

$$|\psi_1\rangle|-\rangle = U_f(|\psi\rangle|-\rangle) = \left(\frac{\begin{array}{c}|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle+|0101\rangle+|0110\rangle-|0111\rangle+|1000\rangle+\\ |1001\rangle+|1010\rangle+|1011\rangle+|1100\rangle+|1101\rangle+|1110\rangle+|1111\rangle\end{array}}{4}\right)|-\rangle$$

Зазначимо, що $|0111\rangle$ є єдиним елементом, що має стан зі знаком "$-$".

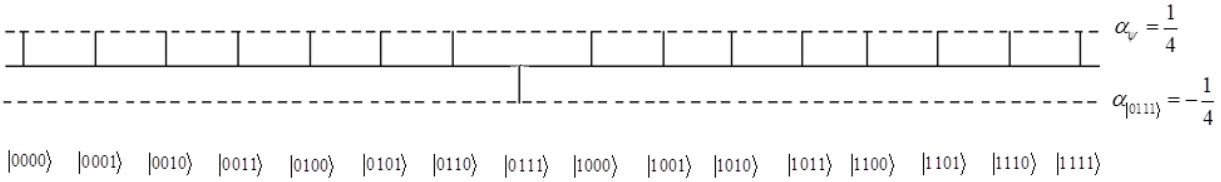
Запишемо $|\psi_1\rangle$ у вигляді

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{2}|0111\rangle \ ,$$

або у вигляді

$$|\psi_1\rangle = \frac{\sqrt{15}}{4}|u\rangle - \frac{1}{4}|0111\rangle$$

Геометрично подамо отримані значення у вигляді позитивних та негативних:



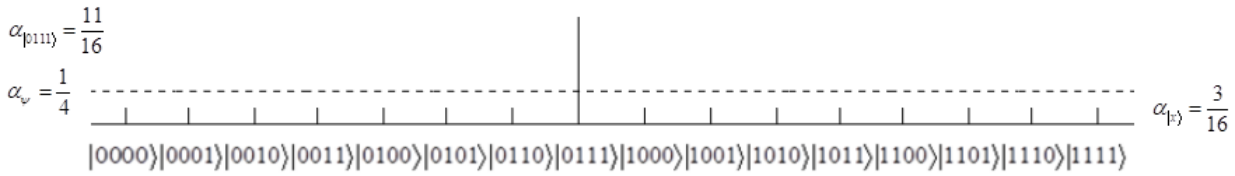
7. Далі ми обчислюємо

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle; \qquad |\psi_2\rangle = \frac{3}{4}|\psi\rangle + \frac{1}{2}|0111\rangle;$$

$$|\psi_2\rangle = \frac{3\sqrt{15}}{16}|u\rangle + \frac{4}{16}|0111\rangle = \frac{3\sqrt{15}}{16}|u\rangle + \frac{1}{4}|0111\rangle$$

Слід відмітити, що $\langle\psi|\psi\rangle = 16\frac{1}{4}\left[\frac{1}{4}\right] = 1$. На додаток до цього, так як $|0111\rangle$ є одним з базисних векторів, можемо використати відповідність $\langle\psi|0111\rangle = \langle 0111|\psi\rangle = \frac{1}{4}$.

В результаті геометрично можна подати як

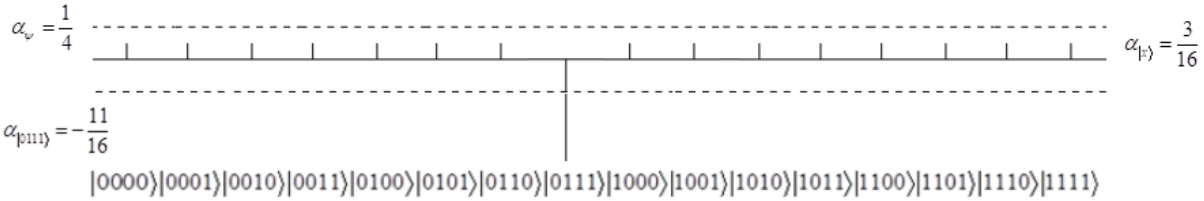


Наведеним результатом завершується перша ітерація G, залишилося ще дві.
Далі отримуємо, що

$$|\psi_3\rangle=\frac{3}{4}|\psi\rangle-\frac{7}{8}|0111\rangle$$

$$|\psi_3\rangle=\frac{3\sqrt{15}}{16}|u\rangle-\frac{11}{16}|0111\rangle$$

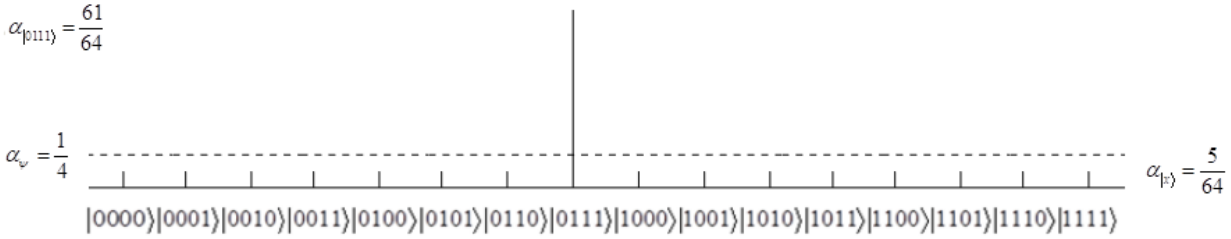
Геометрично результат подаємо як



$$|\psi_4\rangle=(2|\psi\rangle\langle\psi|-I)|\psi_3\rangle=\frac{5}{16}|\psi\rangle+\frac{7}{8}|0111\rangle$$

$$|\psi_4\rangle=\frac{5\sqrt{15}}{64}|u\rangle+\frac{61}{64}|0111\rangle$$

Геометрично результат другої ітерації подаємо як

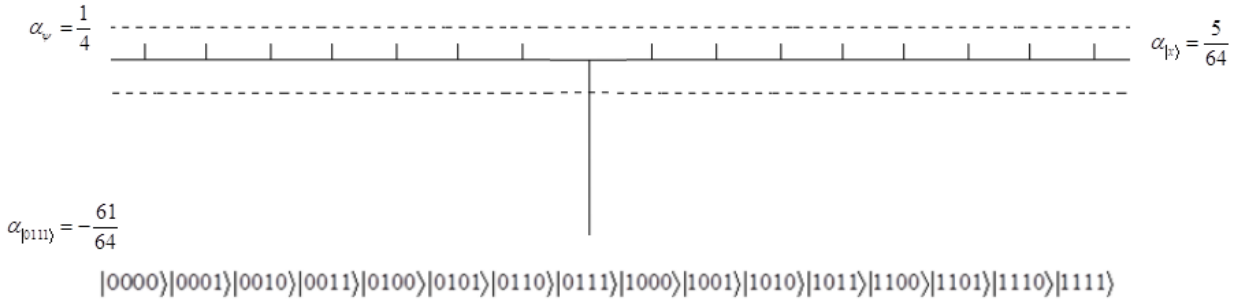


Отриманим значенням завершується друга ітерація, залишається ще одна G ітерація. При її виконанні маємо:

$$|\psi_5\rangle=\frac{5}{16}|\psi\rangle-\frac{33}{32}|0111\rangle$$

$$|\psi_5\rangle=\frac{5\sqrt{15}}{64}|u\rangle-\frac{61}{64}|0111\rangle$$

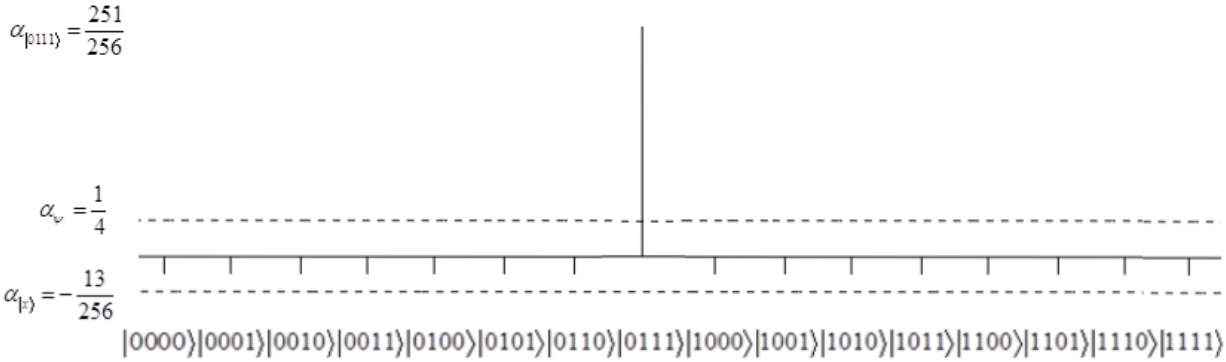
Геометрично результат третьої ітерації подаємо як



$$|\psi_6\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_5\rangle = -\frac{13}{64}|\psi\rangle + \frac{33}{32}|0111\rangle$$

$$|\psi_6\rangle = -\frac{13\sqrt{15}}{256}|u\rangle + \frac{251}{256}|0111\rangle$$

На завершення третьої ітерації маємо



Наведеним завершується виконання третьої ітерації G.

Вимірювання стану $|\psi_6\rangle$ дасть результат у вигляді стану $|0111\rangle$ з ймовірністю, що становить:

$$P = \left|\frac{251}{256}\right|^2 \approx 0{,}961$$

Таким чином, шанс отримання результату $|0111\rangle$, який має індекс 7, близько 96,1 %. Ймовірність отримання невірного стану становить близько 3,9 %. Хоча метод Гровера є ймовірнісним, зі зростанням N похибка стає незначною.

Приклад 2. Припустимо, що система складається з $N = 256 = 2^8$ станів, і стан, який ми шукаємо, x_0, має індекс 15 та представлений бітовою строчкою

$$|x\rangle = |15\rangle = |0000000000001111\rangle$$

1. Розглянемо алгоритм Гровера пошуку данного «унікального» елемента.

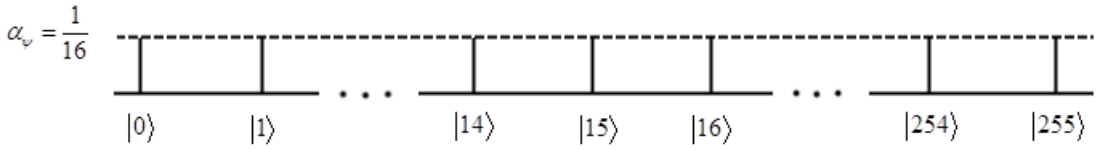
Для того щоб описати цю систему, потрібно $n = 8$ кубіти. У відповідності до алгоритму Гровера зробимо ініціалізацію квантового регістру з $n = 8$ кубітів, що необхідне для представлення пошукового простору розміру $N = 2^8$, встановивши регістр у початковий стан:

$$|\psi_0\rangle = |00000000\rangle$$

2. Проведемо перетворення Адамара, що дозволяє отримати значення амплітуди, що пов’язана з кожним станом з рівною ймовірністю перебування в кожному з 16 можливих станів:

$$|\psi\rangle = \frac{1}{16}\sum_{i=0}^{255}|i\rangle$$

Геометрично отримаємо результат



3. По аналогії з прикладом 1 маємо

$$\frac{\pi}{4}\sqrt{256} = \frac{16\pi}{4} = 4\pi \approx 12,56 \approx 13$$

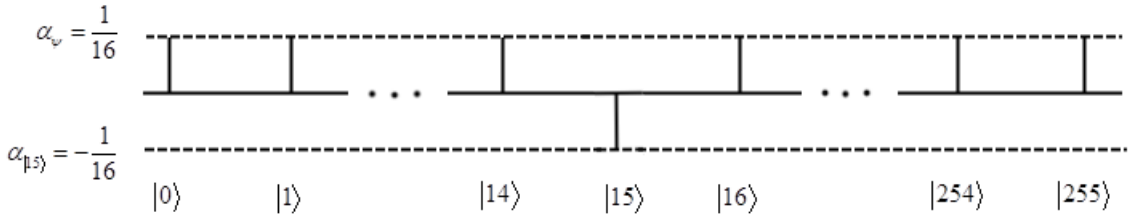
$$|u\rangle = \frac{1}{\sqrt{255}}\sum_{\substack{i=0\\ i\neq 15}}^{255}|i\rangle$$

$$|\psi\rangle = \frac{\sqrt{255}}{16}|u\rangle + \frac{1}{16}|x\rangle$$

4. Для першої ітерації маємо

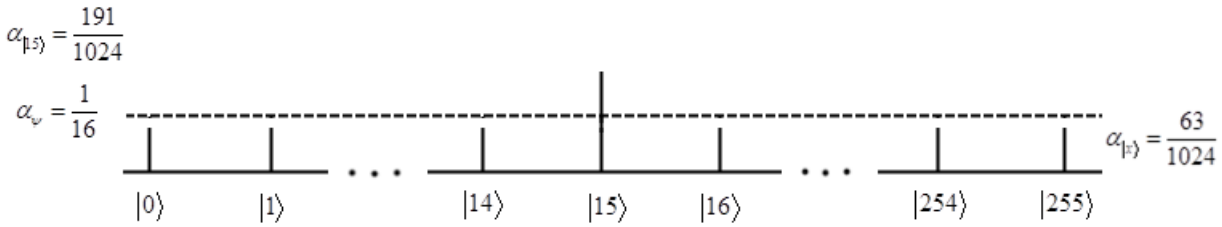
$$|\psi_1\rangle = |\psi\rangle - \frac{1}{8}|x\rangle$$

$$P = 0.00390625$$



$$|\psi_2\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_1\rangle = \frac{63}{64}|\psi\rangle + \frac{1}{8}|x\rangle$$

$$P = 0.03479099$$

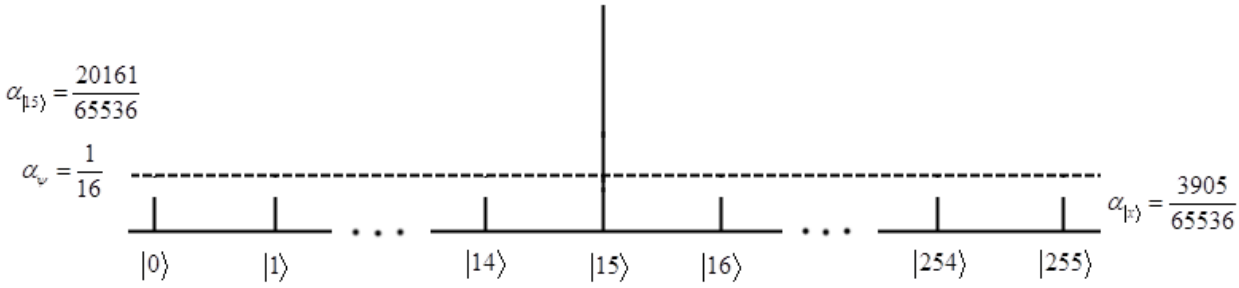


5. Друга ітерація

$$|\psi_3\rangle = \frac{63}{64}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{1}{8}|x\rangle = \frac{63}{64}|\psi\rangle - \frac{127}{512}|x\rangle$$

$$|\psi_4\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_3\rangle = \frac{3905}{4096}|\psi\rangle + \frac{127}{512}|x\rangle$$

$$P = 0.094637722$$



6. Третя ітерація

$$|\psi_5\rangle = \frac{3905}{4096}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{127}{512}|x\rangle = \frac{3905}{4096}|\psi\rangle - \frac{12033}{32768}|x\rangle$$

$$|\psi_6\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_5\rangle = \frac{237887}{262144}|\psi\rangle + \frac{12033}{32768}|x\rangle$$

$$P = 0.17972063$$

7. Четверта ітерація

$$|\psi_7\rangle = \frac{237887}{262144}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{12033}{32768}|x\rangle = \frac{237887}{262144}|\psi\rangle - \frac{1007999}{2097152}|x\rangle$$

$$|\psi_8\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_7\rangle = \frac{14216769}{16777216}|\psi\rangle + \frac{1007999}{2097152}|x\rangle$$

8. П’ята ітерації

$$|\psi_9\rangle = \frac{14216769}{16777216}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{1007999}{2097152}|x\rangle = \frac{14216769}{16777216}|\psi\rangle - \frac{78728705}{134217728}|x\rangle$$

$$|\psi_{10}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_9\rangle = \frac{831144511}{1073741824}|\psi\rangle + \frac{78728305}{134217728}|x\rangle$$

9. Шоста ітерація

$$|\psi_{11}\rangle = \frac{831144511}{1073741824}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{78728305}{134217728}|x\rangle = \frac{831144511}{1073741824}|\psi\rangle - \frac{5869756031}{8589934592}|x\rangle$$

$$|\psi_{12}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{11}\rangle = \frac{47323492673}{68719476736}|\psi\rangle + \frac{5869756031}{8589934592}|x\rangle$$

10. Сьома ітерація

$$|\psi_{13}\rangle = \frac{47323492673}{68719476736}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{5869756031}{8589934592}|x\rangle = \frac{47323492673}{68719476736}|\psi\rangle - \frac{422987878657}{549755813888}|x\rangle$$

$$|\psi_{14}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{13}\rangle = \frac{2605715652415}{4398046511104}|\psi\rangle + \frac{422987878657}{549755813888}|x\rangle$$

11. Восьма ітерація

$$|\psi_{15}\rangle = \frac{2605715652415}{4398046511104}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{422987878657}{549755813888}|x\rangle = \frac{2605715652415}{4398046511104}|\psi\rangle - \frac{29676939886463}{35184372088832}|x\rangle$$

$$|\psi_{16}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{15}\rangle = \frac{137088861868097}{281474976710656}|\psi\rangle - \frac{29676939886463}{35184372088832}|x\rangle$$

12. Дев’ята ітерація

$$|\psi_{17}\rangle = \frac{137088861868097}{281474976710656}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{29676939886463}{35184372088832}|x\rangle =$$

$$= \frac{137088861868097}{281474976710656}|\psi\rangle - \frac{2036413014601729}{2251799813685248}|x\rangle$$

$$|\psi_{18}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{17}\rangle =$$

$$= \frac{6737274144956479}{18014398509481984}|\psi\rangle + \frac{2036413014601729}{2251799813685248}|x\rangle$$

13. Десята ітерація

$$|\psi_{19}\rangle = \frac{6737274144956479}{18014398509481984}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{2036413014601729}{2251799813685248}|x\rangle =$$

$$= \frac{6737274144956479}{18014398509481984}|\psi\rangle - \frac{137067707079467135}{144115188075855872}|x\rangle$$

$$|\psi_{20}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{19}\rangle =$$

$$= \frac{294117838197747521}{1152921504606846976}|\psi\rangle + \frac{137067707079467135}{144115188075855872}|x\rangle$$

14. Одинадцята ітерація

$$|\psi_{21}\rangle = \frac{294117838197747521}{1152921504606846976}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{137067707079467135}{144115188075855872}|x\rangle =$$

$$= \frac{294117838197747521}{1152921504606846976}|\psi\rangle - \frac{9066451091283644161}{9223372036854775808}|x\rangle$$

$$|\psi_{22}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{21}\rangle =$$

$$= \frac{9757090553372197183}{73786976294838206464}|\psi\rangle + \frac{9066451091283644161}{9223372036854775808}|x\rangle$$

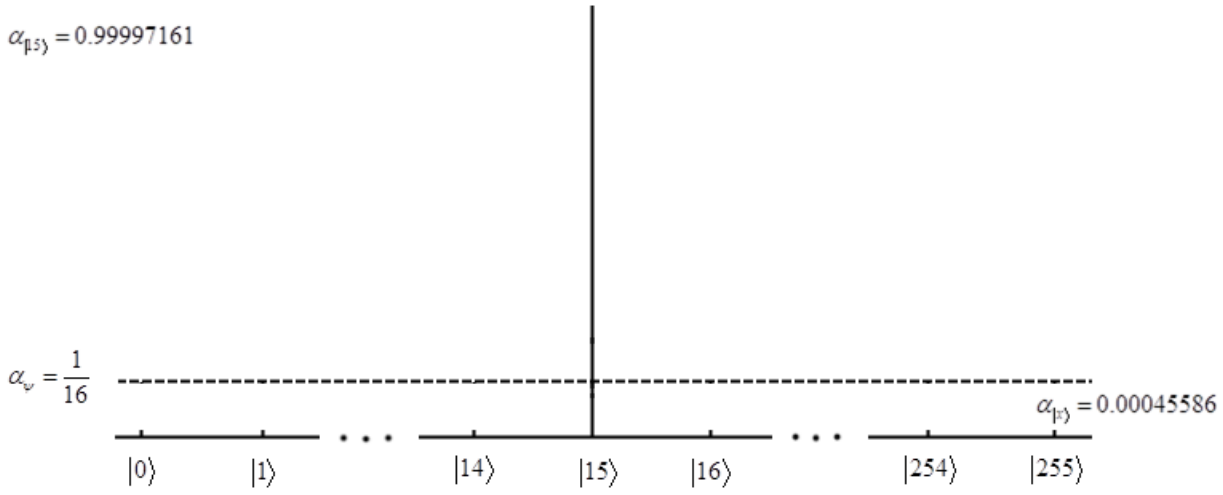
15. Дванадцята ітерація

$$|\psi_{23}\rangle = \frac{9757090553372197183}{73786976294838206464}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{9066451091283644161}{9223372036854775808}|x\rangle =$$

$$= \frac{9757090553372197183}{73786976294838206464}|\psi\rangle - \frac{590009960395525423487}{590295810358705651712}|x\rangle$$

$$|\psi_{24}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{23}\rangle =$$

$$= \frac{34443835020295196225}{472236648286964521 3696}|\psi\rangle + \frac{590009960395525423487}{590295810358705651712}|x\rangle$$



$$P = \left|0.99997161\right|^2 \approx 0.99994322 \approx 99.994322\%$$

16. Тринадцята ітерація

$$\left|\psi_{25}\right\rangle = \frac{34443835020295196225}{4722366482869645213696}\left(\left|\psi\right\rangle - \frac{1}{8}\left|x\right\rangle\right) - \frac{590009960395525423487}{590295810358705651712}\left|x\right\rangle =$$

$$= \frac{34443835020295196225}{4722366482869645213696}\left|\psi\right\rangle - \frac{3779508130033392229939 3}{3777893186295716170956 8}\left|x\right\rangle$$

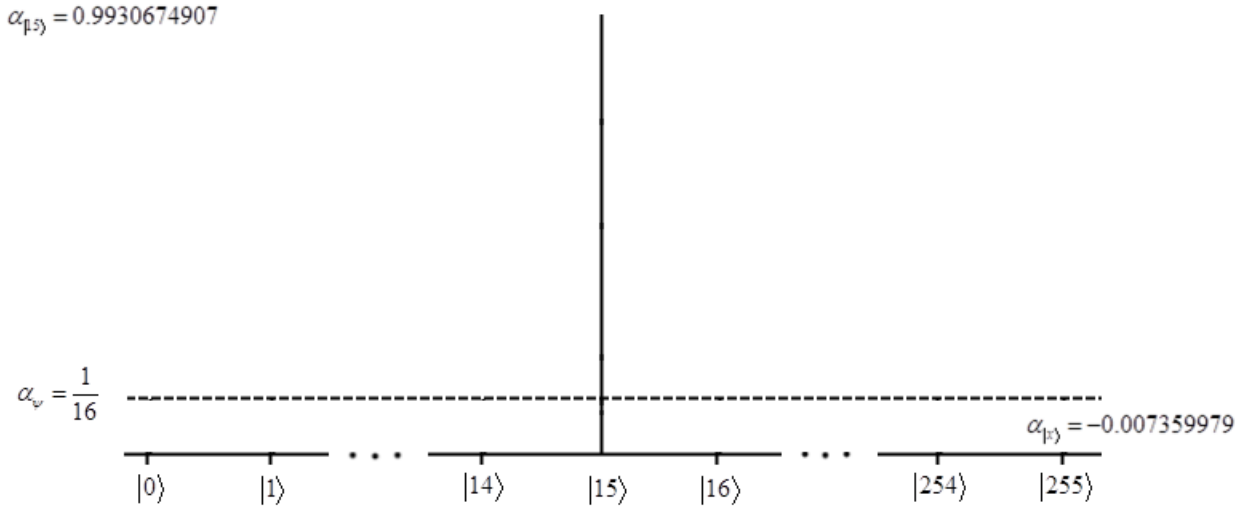
$$\left|\psi_{26}\right\rangle = \left(2\left|\psi\right\rangle\left\langle\psi\right| - I\right)\left|\psi_{25}\right\rangle =$$

$$= -\frac{35590675859035029740993}{3022314549036572936765 44}\left|\psi\right\rangle + \frac{3779508130033392229939 3}{3777893186295716170956 8}\left|x\right\rangle$$

$$\left|\psi\right\rangle = \frac{\sqrt{255}}{16}\left|u\right\rangle + \frac{1}{16}\left|x\right\rangle$$

$$\left|\psi_{26}\right\rangle = -\frac{35590675859035029740993\sqrt{255}}{4835703278458516698824704}\left|u\right\rangle + \frac{4802179730583707024581311}{4835703278458516698824704}\left|x\right\rangle$$

Наприкінці отримуємо значення ймовірності правильного визначення елемента 15.



$$P = \left| \frac{48021797305837070245813 11}{48357032784585166988247 04} \right|^2 \approx 0,98618305$$

З прикладу 2 можна зробити висновок, що для досягнення найкращого результату кількість ітерацій Гровера потрібно округляти до меншого.

Висновки

1. Суттєві результати досягнуто в частині розроблення, стандартизації та застосування симетричного криптоперетворення. 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). Одним із основних є метод Гровера.

2. Освоєння та застосування квантових систем та квантових математичних методів, а також відповідне їх програмування має як методологічний, так і психологічний аспект – складність сприйняття.

3. Метод Гровера полягає в проведенні вичерпного пошуку специфічного (унікального) елементу у несортованій базі даних, що складається з $N = 2^n$ елементів, де n довжина квантового регістру (кількість кубітів).

4. Для криптоаналізу СБП специфічність елементу може зводитись до сеансового чи довгострокового ключа, сінхропослідовності тощо. Особливістю ключа є те, що при його застосуванні зашифровані дані можуть бути розшифрованими за поліноміальний час.

5. У порівнянні з найкращими класичними методамии метод Гровера передбачає проведення пошуку з квадратичним прискоренням. Для отримання такого прискорення використовується квантова суперпозиція станів.

6. Конкретна реалізація квантового оракула залежить від кожного окремого випадку та задачі. Наприклад, у випадку криптоаналізу СБП, оракул виконує розшифрування на ключі та вертає результат – успіх чи ні.

Метод Гровера може бути застосований як на класичному, так і квантовому комп'ютері, хоча реалізація на класичному комп'ютері не є рентабельною.

7. Наведені 1 та 2 приклади підтвердили ефективність методу Гровера стосовно пошуку в несортованій базі: для: 4-бітного числа з ймовірністю близько 96,1 % зі складністю в три раунди; для 8-бітного числа з ймовірністю близько 99 % зі складністю в 13 раундів (силова атака вимагає 256 раундів).

8. Таким чином, застосування методу Гровера для пошуку специфічного елементу в несортованій базі дійсно дозволяє досягти квадратичне прискорення пошуку, вимагає $\sqrt{N}$ раундів у порівнянні з N «грубої сили».

Список 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. – Харків : Форт, 2016. – 959 с.

4. Lov K. Grover. A fast quantum mechanical algorithm for database search. 3C-404A, Bell Labs 600 Mountain Avenue Murray Hill NJ 07974. https://arxiv.org/pdf/quant-ph/9605043.pdf.

5. Emma Strubell. An Introduction to Quantum Algorithms. COS498 – Chawathe. https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf.

АТ «Інститут інформаційних технологій», Харків;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 06.11.2018