A Quantum Algorithm for Solving Unstructured Search Problems

Dr. Hasan Albustani*
Yana Ghanim**

(Received 2 / 7 / 2019. Accepted 15 / 10 / 2019)

□ ABSTRACT □

Grover algorithm is a quantum algorithm for solving search problems in unstructured databases which means that finding that one of the elements in the search space isn't a solution can't help us to avoid looking at other elements,this case is the most difficult, as to find the owner of a given telephone number in a phonebook arranged by names whereas the easiest case is to search in a structured search space,such as to search for a phone number for a given person in a phonebook arranged by names.

This paper discusses the formation of this algorithm- which provides a polynominal (quadratic) acceleration compared to classical search algorithm- using quantum gates and its implementation in a 16-elements search space to search for different numbers and values of solutions.

Keywords: Quantum computing -Quantum computing algorithms - Grover algorithm.

*Assistant Professor, Faculty of information and communication Technology, Tartus University, Tartus, Syria.

**Master Student , Faculty of Information and Communication Technology, Tartus University, Tartus, Syria.

خوارزمية كمومية لحل مشاكل البحث في فضاءات البحث غير البنيوية

د.حسن البستاني *

يانا غانم **

(تاريخ الإيداع 2 / 7 / 2019. قُبِل للنشر في 15/ 10 / 2019)

□ ملخّص □

إنّ خوارزمية كروفر هي خوارزمية كمومية لحل مسائل البحث في فضاءات البحث غير البنيوية، ويقصد بفضاء البحث الذي ليس له بنية أنّ اكتشاف أنّ أحد الاحتمالات الواردة في فضاء البحث لا يمثّل حلاً لا يمكننا من تجنب البحث في احتمالات أخرى(أي لا يمكن توجيه البحث لاحتمالات معينة بهدف تسريعه)، وهذه الحالة هي الأصعب كمحاولة البحث عن اسم صاحب رقم هاتفي معطى في دليل هاتفي مرتّب بالأسماء، أما الحالة الأسهل فهي البحث في فضاء بحث ذي بنية، مثل البحث عن رقم هاتف لشخص معطى اسمه في دليل هاتفي مرتّب بالأسماء.

تناقش ورقة البحث تشكيل هذه الخوارزمية – التي تؤمن تسريعاً تربيعياً بالمقارنة مع خوارزميات البحث التقليدية– باستخدام البوابات الكمومية وتنفيذها في فضاء بحث من 16 عنصر للبحث عن أعداد وقيم مختلفة من الحلول.

الكلمات المفتاحية: الحوسبة كمومية – خوارزميات البحث الكمومي –خوارزمية كروفر.

* **مدرّس– كلية هندسة تكنولوجيا المعلومات والاتصالات– جامعة طرطوس – طرطوس– سورية.**

** **طالبة ماجستير– كلية هندسة تكنولوجيا المعلومات والاتصالات– جامعة طرطوس – طرطوس– سورية.**

مقدمة:

تعتمد الحوسبة الكمومية على مبدأ التراكب الكمومي(quantum superposition) ، ففي الأجسام الضخمة مقارنة بحجم الذرة لا يمكن لشيء أن يكون في حالتين مختلفتين في الوقت نفسه، لكن التراكب الكمومي يفترض أن الجسيمات دون الذرية تكون في جميع الحالات الممكنة لها في الوقت نفسه، وتأخذ قيمة معينة فقط عندما نقوم بقياس حالتها [1].

إن اعتماد مبدأ التراكب الكمومي في الحوسبة يفسح المجال أمام التنفيذ المتوازي للعمليات الحاسوبية أي معالجة الحالات المتعددة في الوقت نفسه، مما يعطي القدرة لحل بعض التحديات التي تواجه الحواسيب التقليدية كعمليات البحث الضخمة وخوارزميات التشفير وفك التشفير المعقدة.

انطلقت الأبحاث في مجال الحوسبة الكمومية بدءاً من ثمانينات القرن الماضي على يد الفيزيائي Richard Feynman الذي تساءل عن ماهية الحواسيب التي بإمكانها محاكاة الفيزياء، وتوصل إلى أننا بحاجة إلى حواسيب كمومية للقيام بذلك [2].

أكد العالم Paul Penioff من خلال بحثه في العام نفسه (1982) أنه من الممكن أن نستخدم علم الكم لنمذجة حواسيب كمومية تكافئ في الحد الأدنى فاعلية الحواسيب التقليدية[3] ، وتوصل العالم David Deutsh عام(1985) إلى أن الحواسيب الكمومية المفترضة ستتمكن من القيام بأشياء تفوق قدرة الحواسيب التقليدية[4].

في عام 1996توصل العالم الهندي- الأمريكي Lov Grover إلى خوارزمية تعتمد على مبادئ علم الكم لتخفيض زمن البحث في قواعد البيانات وسميت الخوارزمية باسمه (Grover Search Algorithm)[5].

بدءاً من العام 1998 بدأت الأبحاث والتجارب العلمية لإنتاج حواسيب كمومية، وتم تطوير أول حاسوب كمومي في مختبرات LosAlamos باستخدام الأيونات المحجوزة[6]، ثم توال تطوير الحواسيب الكمومية بالاعتماد على مفاهيم وبنى فيزيائية مختلفة كالطنين المغناطيسي النووي(Nuclear Magnetic Resonance) و أمواج D(D-wave).

مع هذا التطور في مجال تصنيع الحواسيب الكمومية كان هناك العديد من التجارب والأبحاث لتنفيذ خوارزمية grover على حاسوب كمومي كان أبرزها في جامعة maryland university،حيث تم عام 2017 تنفيذ الخوارزمية بثلاث بيتات كمومية على حاسوب كمومي قابل للبرمجة مصنع باستخدام الأيونات المحجوزة [7].

على الرغم من أنّ تعقيد هذه الخوارزمية قريب من تعقيد الخوارزميات الكمومية الأخرى كخوارزمية Deutsch التي اقترحها العالم David Deutsh في منتصف الثمانينات من القرن الماضي[1] ، وخوارزمية Shor التي اقترحها العالم Peter Shor عام 1992 والتي تهتم بإيجاد عوامل عدد معطى [1] ، إلاّ أن أهمية هذه الخوارزمية تتمثل في اتساع مجال استخداماتها، حيث يمكن استخدامها كنواة لطيف واسع من التطبيقات الهامة كما في عمليات التشفير[8] ، وكسر التشفير[9]، ومعالجة الصورة [10]، وفي عمليات الأمثّلة (إيجاد القيمة الصغرى أو الكبرى)[11] .

أهمية البحث وأهدافه:

1- بناء نموذج الدارة الكمومية الممثلة لخوارزمية كروفر في الحالة العامة.

2- تنفيذ الخوارزمية في فضاء بحث من 16 عنصر.

طرائق البحث ومواده:

1- البوابات الكمومية:

سنبدأ بتعريف البوابات الكمومية التي سنستخدمها لاحقاً في تصميم الخوارزمية ، والتحويل الذي تقوم به كل بوابة من هذه البوابات[1],[12].

a.بوابة العكس (X-gate)

بفرض أن الحالة الابتدائية معرفة وفق العلاقة (1).

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \quad (1)$$

إن تطبيق بوابة X- gate يؤدي إلى التبديل بين احتماليتي الحالتين 0 و1 وتصبح الحالة الجديدة كالآتي:

$$X|\psi\rangle=\alpha|1\rangle+\beta|0\rangle \quad (2)$$

b. بوابة قلب الصفحة (Z - gate)

هذه البوابة لا تغير من الحالة $|0\rangle$ ولكنها تقلب صفحة الحالة $|1\rangle$ لتعطي $-|1\rangle$ كما في المعادلة(3).

$$Z|\psi\rangle=\alpha|0\rangle-\beta|1\rangle \quad (3)$$

c. بوابة هادامارد (Hadamard)

تحويل هادامارد (Hadamard) هو مثال على حالة معممة من تحويل فوريه، وهو يقوم بتجزئة شعاع الدخل إلى مركبات. وفق الطريقة التراجعية نعرف تحويل هادامارد1X1 والمسمى H_0 حيث $H_0=1$ ،ومن أجل $m>0$ فإن H_m تعطى كالآتي:

$$H_m=\frac{1}{\sqrt{2}}\begin{bmatrix}H_{m-1} & H_{m-1}\\ H_{m-1} & -H_{m-1}\end{bmatrix}$$

وبالتالي فإن H_1 تعطى كالآتي :

$$H_1=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

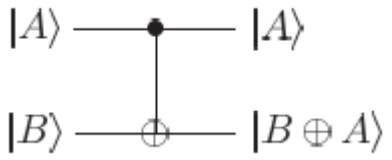
كما تعطى H_2 كالآتي:

$$H_2=\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

ويمكن استخدام الطريقة التراجعية للوصول إلى التحويل الذي تقوم به البوابة الكمومية من أجل أي عدد من البيتات الكمومية .

d. بوابة التحكم بالعكس (controlled-Not)

يعطى الرمز الكمومي للبوابة كما في الشكل (1) .



الشكل(1): رمز بوابة Controlled –Not.

تقوم هذه البوابة بعكس حالة البت الثاني عندما يكون البت الأول 1، وتعطى مصفوفة التحويل كالآتي:

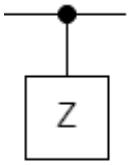
$$U_{CN}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

يمكن تعميم بوابة Controlled –Not من أجل أي عدد من البيتات الكمومية، حيث تتحكم عدد من البيتات بعكس حالة البت الأخير. من أجل ثلاث بيتات كمومية تسمى البوابة عندئذ بوابة toffoli، وتعطى مصفوفة التحويل لها على النحو الآتي:

$$\text{Toffoli}=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$

e. بوابة التحكم بقلب الصفحة (controlled-z)

يعطى الرمز الكمومي للبوابة كما في الشكل (2) .



الشكل(2): رمز بوابة Controlled-Z.

تقوم هذه البوابة بقلب صفحة الحالة 11، وتعطى مصفوفة التحويل كالآتي:

$$U_z=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

يمكن تعميم بوابة Controlled –Z من أجل أي عدد من البيتات الكمومية، حيث يتم قلب صفحة الحالة التي تكون فيها جميع البتات 1.

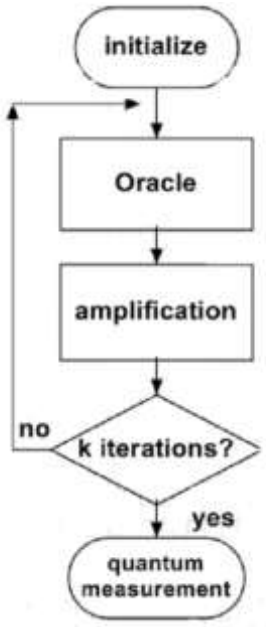
يجب أن تحقق جميع البوابات الكمومية خاصية الواحدية $U.U^t=1$ ،حيث U هي مصفوفة التحويل.

سنستعين بمحاكيQuirk وهو منصة على شبكة الانترنت من أجل بناء ومحاكاة الدارات الكمومية[13].

2- مراحل الخوارمية

يوضح الشكل (3) مخطط التدفق لهذه الخوارزمية التي تتضمن أربعة مراحل هي: مرحلة التهيئة، مرحلة التنبؤ، مرحلة التضخيم، مرحلة القياس الكمومي.

سنقوم بالتعريف بمراحل الخوارزمية والعلاقات الرياضية المعبرة عنها [1] ،] [7] ،[14].



الشكل(3): مخطط تدفق خوارزمية grover.

a.المرحلة الأولى:مرحلة التهيئة (initialization)

تقوم هذه المرحلة بتوليد فضاء البحث عن طريق تحويل هادامارد على كل مدخل من المداخل بعد تهيئتها بالقيمة |0> وفق التحويل الآتي:

$$H|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{X=0}^{N-1}|x\rangle \qquad (4)$$

حيث يشير الرمز $\langle\ |$ إلى ترميز الحالة الكمومية وفق تدوين برا–كيت [1]، وتمثل n عدد البيتات المستخدمة في تمثيل فضاء البحث، و الرمز $\otimes$ يشير إلى الجداء المباشر (direct product) و N هي عدد الحالات الكمومية الممثلة باستخدام n بت كمومي.

b .مرحلة التنبؤ (oracle)

يمكن التعبير عن مشكلة البحث بالتابع f(x)،حيث f(x)=1 إذا كان x هو حل للخوارزمية، و f(x)=0 في بقية الحالات، وبالتالي فإن تابع التنبؤ يقوم بالتحويل الآتي:

$$|x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle \qquad (5)$$

حيث x هو مسجل العنصر الذي نجري عليه عملية التحقق، و q هو بت كمومي يتعرض للعكس إذا كان f(x)=1 ولا يحدث له أي تغيير في بقية الحالات، و الرمز $\oplus$ يشير إلى عملية ال xor.

نطبق التنبؤ بحيث يكون بت التنبؤ مساويًا $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$، ونحصل عليه بتطبيق تحويل هادامارد على الحالة |1>، وبالتالي يكتب التحويل السابق في العلاقة (5) على النحو الآتي:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|x\rangle \qquad (6)$$

c. مرحلة التضخيم(amplification)

هدف مرحلة التضخيم هو زيادة مطال الحالة أو الحالات الصحيحة، وتخفيض مطال الحالات الخاطئة عن طريق التحويل الآتي:

$$\sum_{i=0}^{N-1} ai\left|xi\right\rangle \rightarrow \sum_{i=0}^{N-1}(2A-ai)\left|xi\right\rangle \qquad (7)$$

حيث A هو المطال المتوسط، ويعبر عنه بالعلاقة الآتية:

$$A=\frac{\sum_{I=0}^{N-1} a_i}{N} \qquad (8)$$

سبق أن توصلنا من مرحلة التنبؤ إلى أن مطال الحالة أو الحالات الصحيحة سيكون سالب، ومطال بقية الحالات سيكون موجباً، وبالتالي فإن تطبيق عملية التضخيم سيعطي النتيجة الآتية:

$$-ai\left|xi\right\rangle \rightarrow 2A+ai\left|xi\right\rangle \text{ when } xi = w \qquad (9)$$

$$ai\left|xi\right\rangle \rightarrow 2A-ai\left|xi\right\rangle \text{ when } xi \neq w \qquad (10)$$

حيث w هو الحل الصحيح (القيمة التي نبحث عنها).

d. مرحلة القياس الكمومي (quantum measurement)

يحول القياس الكمومي حالة كمومية وحيدة إلى بت منطقي وحيد(0 أو 1) بالاعتماد على الاحتمالية فإذا كانت الحالة:

$$\left|\Psi\right\rangle=\alpha\left|0\right\rangle+\beta\left|1\right\rangle \qquad (11)$$

فإن عملية القياس الكمومي ستنتج 0 باحتمالية $|\alpha|^2$ و 1 باحتمالية $|\beta|^2$ ($|\alpha|^2+|\beta|^2=1$).

تعطى عدد تكرارات الخوارزمية المطلوبة للوصول إلى الحل الصحيح على النحو الآتي:

$$\mathbf{k}=\frac{\pi}{4}\sqrt{\frac{N}{M}} \qquad (12)$$

حيث:

M: عدد العناصر الصحيحة المبحوث عنها، N: حجم فضاء البحث،K: عدد التكرارات (يجب أن يكون عدداً صحيحاً، إذا تضمن أجزاء يجري التقريب للقيمة الأصغر(Round down)).

3 – تشكيل الخوارزمية باستخدام البوابات الكمومية:

سنقوم باستنتاج البوابات الكمومية المستخدمة في تمثيل كل مرحلة من مراحل الخوارزمية:

a.المرحلة الأولى:مرحلة التهيئة (initialization)

نستخدم في هذه المرحلة بوابة هادامارد لإنجاز تحويل الهادامارد الذي تتطلبه هذه المرحلة، حيث يجري تطبيق هذا التحويل على كل بت من بيتات الدخل من أجل توليد كامل فضاء البحث.

b. مرحلة التنبؤ (oracle)

بما أن هدف مرحلة التنبؤ هو الإشارة إلى العناصر الصحيحة لذلك سيختلف تشكيلها باختلاف قيم العناصر التي نبحث عنها، ويمكن أن ننجز مرحلة التنبؤ بطريقتين:

1. التنبؤ الثنائي (Boolean-Oracle)

- يمكن تحقيق مرحلة التنبؤ باستخدام الحالة العامة من بوابات Controlled–Not، حيث يمثل التابع f(x)عندئذ قيم بيتات التحكم لبوابة التحكم بالعكس التي تتحكم بعكس بت التنبؤ، حيث يتم تشكيل هذه المرحلة بحيث ينتج f(x)=1 من أجل القيم التي نريد البحث عنها.
- نقوم بتهيئة بت التنبؤ بالقيمة 1 ونضع بوابة هادامارد على خط البت قبل مرحلة التنبؤ من أجل الوصول إلى قلب صفحة الحالات الصحيحة عندما يتعرض هذا البت للعكس(العلاقة(6))، كما نطبق بوابة هادامارد على بت التنبؤ بعد مرحلة التنبؤ لإلغاء التراكب وإعادته إلى قيمته الأصلية 1.
- في هذه الطريقة وعند البحث في فضاء بحث من N عنصر فإننا سنحتاج إلى $n=\log_2(N)$ لتمثيل فضاء البحث بالإضافة إلى بت الاختبار الذي سيتعرض للعكس، أي أننا سنحتاج إلى$\log_2(N)+1$بت كمومي عند استخدام هذه الطريقة.
- قد نحتاج إلى بوابات عكس عندما نريد أن تكون قيمة أحد البيتات المتحكمة 0.

2.التنبؤ بقلب الصفحة (Z-Oracle)

- يمكن أن نستخدام بوابات قلب الصفحة (Z–gate والحالة العامة من controlled–z) لتشكيل مرحلة التنبؤ، بحيث تؤدي سلسلة من عمليات القلب إلى قلب صفحة الحالات المطلوبة دون الحاجة لوجود بت التنبؤ.
- قد نحتاج إلى بوابات عكس في هذه الطريقة أيضاً عندما نريد أن تكون قيمة أحد البيتات المتحكمة 0.

c. مرحلة التضخيم (amplification)

يمكن التعبير عن عملية التحويل في مرحلة التضخيم بشكل مصفوفي على النحو الآتي [8]:

$$D=\begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \dots & \dots & \dots & \frac{2}{N} \\ \frac{2}{N} & \dots & \dots & \dots & \dots & \frac{2}{N} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{2}{N} & \dots & \dots & \dots & \dots & \frac{2}{N}-1 \end{bmatrix}$$

$$D_{i,j}=\begin{cases} \frac{2}{N} & if\ i \neq j \\ \frac{2}{N}-1 & if\ i=j \end{cases}$$ أو باختصار

حيث المصفوفة D هي مصفوفة بطول NxN وتسمى مصفوفة الانتشار Diffusion.

ومن الممكن كتابة المصفوفة D كجداء ثلاث مصفوفات :

$$D=-H^{\otimes n}.U_0.H^{\otimes n}=-H^{\otimes n}\begin{bmatrix}-1 & 0 & \dots & \dots & \dots & 0\\ 0 & 1 & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & 1 & \dots\\ 0 & \dots & \dots & \dots & \dots & 1\end{bmatrix}H^{\otimes n}$$

حيث المصفوفة U_0 هي مصفوفة بطول NxN .

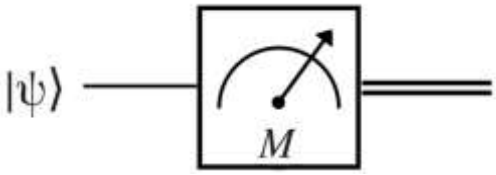
سنقوم بكتابة U_0 أيضاً كجداء ثلاث مصفوفات بطول NxN على النحو الآتي:

$$U_0=\begin{bmatrix}0 & 0 & \dots & \dots & \dots & 1\\ 0 & \dots & \dots & \dots & 1 & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & 1 & \dots & \dots & 0 & \dots\\ 1 & \dots & \dots & \dots & \dots & 0\end{bmatrix}\begin{bmatrix}1 & 0 & \dots & \dots & \dots & 0\\ 0 & 1 & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & 1 & \dots\\ 0 & \dots & \dots & \dots & \dots & -1\end{bmatrix}\begin{bmatrix}0 & 0 & \dots & \dots & \dots & 1\\ 0 & \dots & \dots & \dots & 1 & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots & \dots\\ \dots & 1 & \dots & \dots & 0 & \dots\\ 1 & \dots & \dots & \dots & \dots & 0\end{bmatrix}$$

تمثل المصفوفتان الأولى والاخيرة التحويل المصفوفي ل n من بوابات العكس، بينما تمثل المصفوفة الوسطى التحويل المصفوفي لبوابة تحكم بقلب الصفحة مكونة من $n-1$ بت تحكم.سنقوم بإهمال الإشارة السالبة في العلاقة المعبرة عن D (أي سنمثل D– باستخدام البوابات الكمومية) وهذا سيجعل عملية التضخيم تتم في الاتجاه السالب، ولكن هذا لا يؤثر أبداً على الاحتمالية التي هي مربع المطال، نستنتج مما سبق أن بناء مرحلة التضخيم يكون باستخدام بوابات هادامارد والعكس والتحكم بقلب الصفحة.

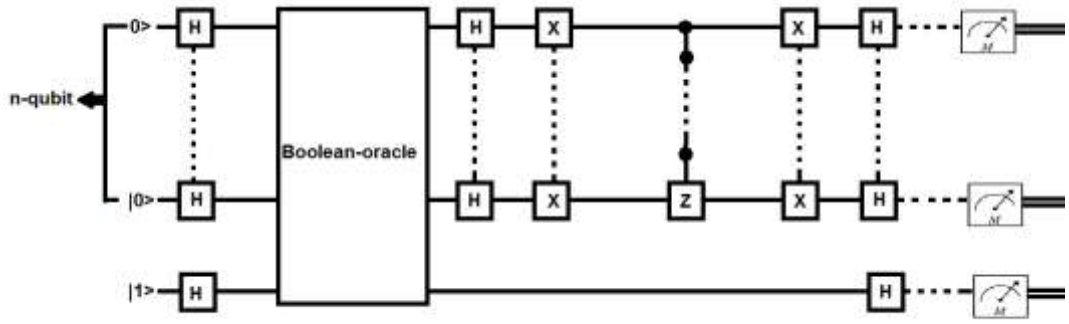
d. المرحلة الرابعة مرحلة القياس الكمومي (quantum measurement)

يمثل الشكل(4) البوابة الكمومية التي تقوم بعملية القياس الكمومي، حيث تحول البت الكمومي المكون من مركبتين إلى بت ثنائي 0 أو 1 وفقاً للمنطق التقليدي (كل منهما باحتمالية معينة).

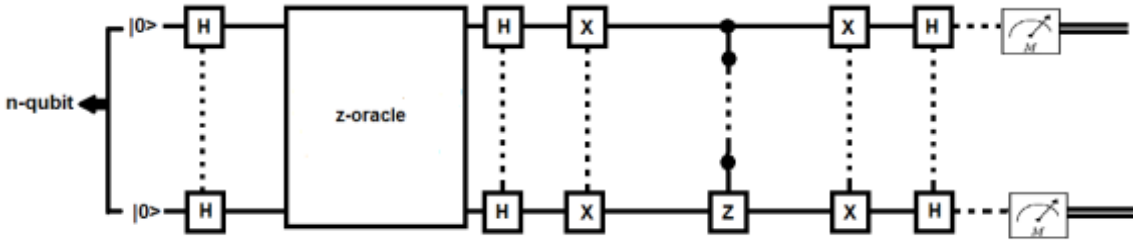


الشكل(4): رمز بوابة القياس الكمومي.

للوصول إلى نموذج الدارة الكلية نقوم باستبدال التحويلات المصفوفية السابقة بالبوابات التي تمثلها وبنفس الترتيب، يمثل الشكلان(5) و(6) نموذجي الدارة باستخدام طريقتي التنبؤ.



الشكل(5): نموذج دارة grover في الحالة العامة باستخدام التنبؤ الثنائي.

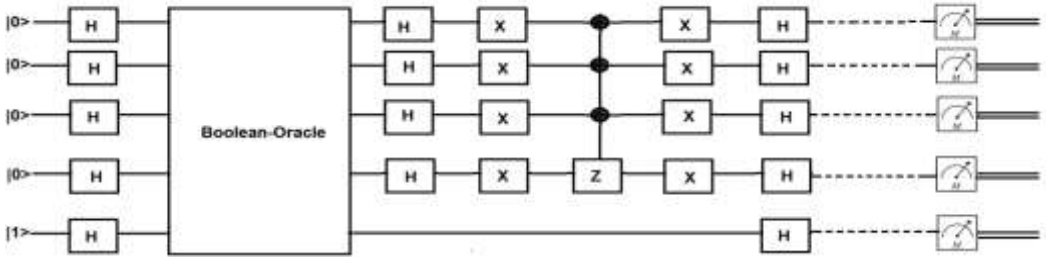


الشكل(6): نموذج دارة grover في الحالة العامة باستخدام التنبؤ بقلب الصفحة.

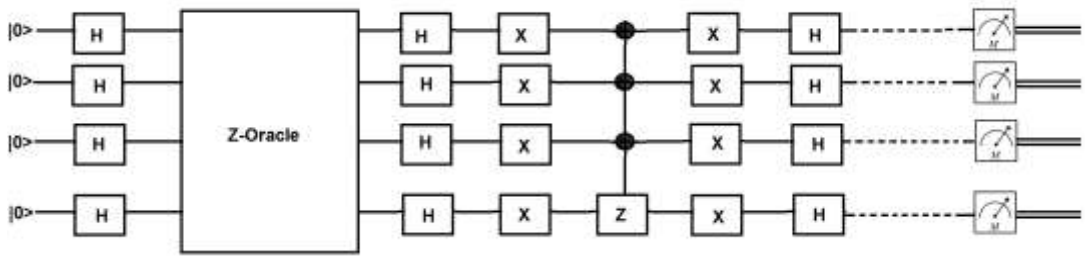
4.تنفيذ الخوارزمية في فضاء بحث من 16 عنصر:

توصلنا من خلال المناقشة السابقة إلى أن تشكيل مرحلة التنبؤ يختلف باختلاف عدد وقيم العناصر التي نبحث عنها، وللوصول إلى فهم آلية استنتاج مرحلة التنبؤ سنقوم انطلاقاً من النموذج العام للدارة الذي توصلنا إليه بتصميم الدارة الكمومية الممثلة للخوارزمية من أجل البحث عن أعداد وقيم مختلفة من الحلول في فضاء بحث من 16عنصر.

عند البحث في فضاء من 16عنصر فإننا نحتاج إلى أربع بيتات كمومية لتمثيل فضاء البحث $n=\log_2(16)=4$، ويصبح نموذجا الدارة من أجل هذا الحجم لفضاء البحث باستخدام طريقتي التنبؤ كما في الشكلين (7) و(8).



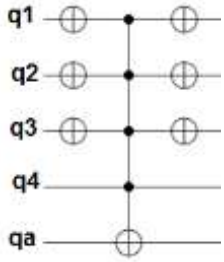
الشكل(7): نموذج دارة grover في فضاء بحث من 16 عنصر باستخدام التنبؤ الثنائي.



الشكل(8): نموذج دارة grover في فضاء بحث من 16 عنصر باستخدام التنبؤ بقلب الصفحة.

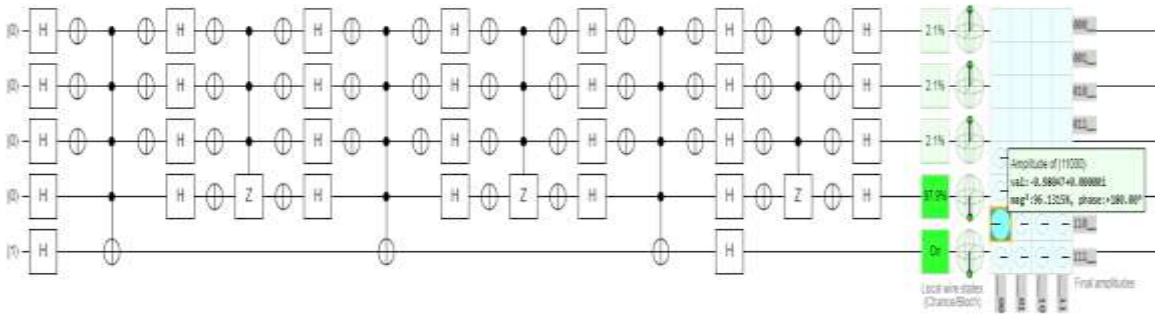
a.البحث عن حل وحيد:

عند البحث عن حل وحيد بطريقة التنبؤ الثنائي نحتاج إلى بوابة تحكم بالعكس وحيدة (بأربع بيتات تحكم) حيث تتحكم البيتات الأربعة الأولى بعكس حالة البت الأخير(بت التنبؤ)، يوضح الشكل(9) دارة التنبؤ الثنائي للبحث عن الحل q1q2q3q4=0001، حيث نضع بوابة عكس على خطوط البيتات الثلاثة الأولى قبل بوابة التحكم بالعكس بحيث يتم عكس بت التنبؤ عندما تكون قيمة هذه البيتات 0 وقيمة البت الرابع 1، حيث يمثل التابع f(x) في هذه الحالة قيم بيتات التحكم لبوابة التحكم بالعكس التي تؤدي إلى عكس البت المتحكم به(بت التنبؤ). عندما f(x)=1 سيجري عكس بت التنبؤ مما يؤدي إلى قلب صفحة الحالة الكمومية الموافقة (q1q2q3q4= 0001). تم وضع بوابتي عكس على خطوط البيتات الثلاثة الأولى بعد بوابة التحكم بالعكس لإعادة قيم البيتات الكمومية إلى ما كانت عليه قبل مرحلة التنبؤ لأن هدف عملية العكس ليس تغيير قيم هذه البيتات بل التأثير على بت التنبؤ(qa).



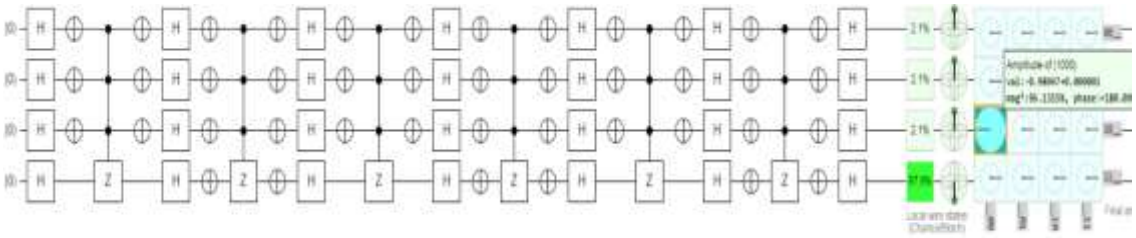
الشكل(9): دارة التنبؤ الثنائي للبحث عن q1q2q3q4=0001.

الشكل(10) يمثل الدارة الكمومية الكلية للبحث عن العنصر q1q2q3q4=0001 بطريقة التنبؤ الثنائي، حيث نحتاج إلى ثلاثة تكرارات للوصول إلى الحل الصحيح (تحسب التكرارات من العلاقة (12))، احتمالية الحالة الصحيحة الوحيدة (%96.13) .



الشكل (10): تنفيذ الخوارزمية من أجل البحث عن الحل q1q2q3q4=0001 بطريقة التنبؤ الثنائي.

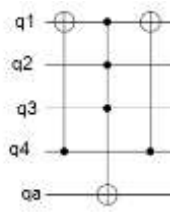
وبالآلية نفسها يتم تشكيل دارة التنبؤ بقلب الصفحة للبحث عن عنصر واحد في قاعدة البيانات، يمثل الشكل (11) الدارة الكمومية الكلية للبحث عن العنصر q1q2q3q4=0001 بطريقة التنبؤ بقلب الصفحة حيث نستخدم بوابة تحكم بقلب الصفحة وحيدة (بأربع بيتات تحكم) في مرحلة التنبؤ ولا نحتاج إلى بت التنبؤ.



الشكل (11): تنفيذ الخوارزمية أجل البحث عن الحل q1q2q3q4=0001 بطريقة التنبؤ بقلب الصفحة.

b.البحث عن حلين:

مثلاً عند البحث عن الحلين 1110,0111 نلاحظ أن قيمة البيتين الثاني والثالث مشتركة بين الحلين وتساوي 1، و قيمة البيتين الأول والرابع مختلفة بين الحلين وفيما بينهما في نفس الحل (01 ،10)، لذلك نشكل دارة التنبؤ كما في الشكل(12)، حيث تُطبق بوابة تحكم بالعكس بين البيتين الأول والرابع (لا يهم أي من البيتين هو المتحكم) بحيث يكون خرجها مساوياً للواحد عندما يكون هاذان البيتان متعاكسين، وفي المرحلة الثانية تُطبق بوابة تحكم بالعكس بثلاث بيتات تحكم(خرج بوابة التحكم الأولى والبيتين الثاني والثالث)حيث تتحكم هذه البيتات الثلاثة بعكس حالة بت التنبؤ، يبين الجدول (1) نتيجة f(x) بعد تطبيق هاتين المرحلتين حيث يكون f(x)=1 من أجل القيمتين المطلوبتين.

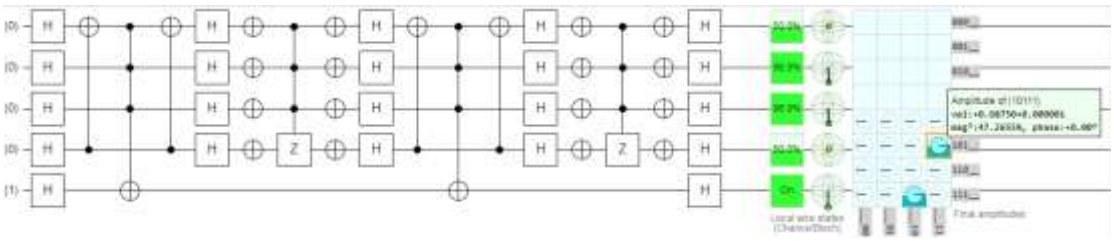


الشكل (12): دارة التنبؤ الثنائي للبحث عن الحلين q1q2q3q4=1110,0111.

ويوضح الشكل (13) الدارة الكمومية الكلية المطلوبة للبحث عن هذين الحلين بطريقة التنبؤ الثنائي، حيث توصلنا إلى الحلين بتطبيق تكرارين فقط، واحتمالية كل من الحلين47.26%.

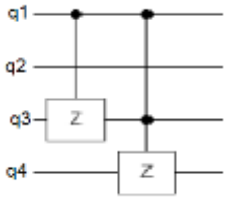
الجدول (1): مراحل تنفيذ دارة التنبؤ الثنائي للبحث عن q1q2q3q4=1110,0111.

q1	$q2$	q3	q4	M = q_4 controlled q_1	f(x)=q_2 and q_3 and M
0	0	0	0	0	0
1	0	0	0	1	0
0	1	0	0	0	0
1	1	0	0	1	0
0	0	1	0	0	0
1	0	1	0	1	0
0	1	1	0	0	0
1	**1**	**1**	**0**	**1**	**1**
0	0	0	1	1	0
1	0	0	1	0	0
0	1	0	1	1	0
1	1	0	1	0	0
0	0	1	1	1	0
1	0	1	1	0	0
0	**1**	**1**	**1**	**1**	**1**
1	1	1	1	0	0



الشكل (13): تنفيذ الخوارزمية في حالة البحث عن عنصرين q1q2q3q4=1110,0111 بطريقة التنبؤ الثنائي.

أيضاً عند البحث عن حلين باستخدام التنبؤ بقلب الصفحة تؤدي سلسلة من عمليات القلب إلى قلب صفحة الحالتين المطلوبتين، يوضح الشكل (14) دارة التنبؤ المطلوبة للبحث عن الحلين q1q2q3q4=1010,1110 حيث تتضمن الدارة مرحلتي قلب، في المرحلة الأولى يجري قلب صفحة الحالات التي يكون فيها البتين الأول و الثالث مساويان للواحد، وفي المرحلة الثانية يجري قلب صفحة الحالات التي تكون فيها البتات الأول والثالث والرابع مساوية للواحد . ويبين الجدول (2) النتيجة بعد كل عملية قلب ،حيث ينتج عن عملية القلب الأولى قلب صفحة الحالات 1010,1110,1011,1111 بينما يتم في المرحلة الثانية إعادة قلب صفحتي الحالتين 1011,1111 وبالتالي الوصول إلى النتيجة المطلوبة.

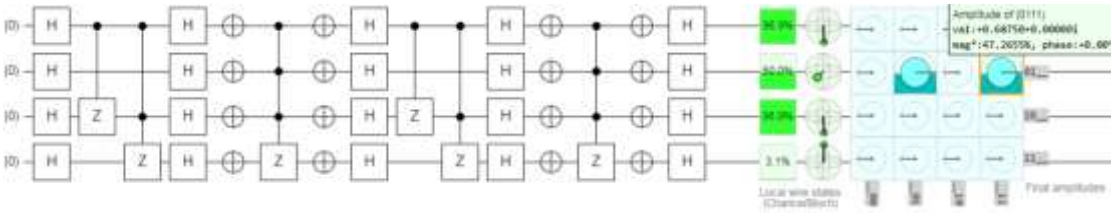


الشكل(14): دارة التنبؤ الثنائي للبحث عن الحلين q1q2q3q4=1110,1010 .

الجدول (2): مراحل تنفيذ دارة التنبؤ بقلب الصفحة للبحث عن الحلين1110 ,q1q2q3q4=1010.

q1	$q2$	q3	q4	q1 controlled-zq3	Output $_{oracle}$= (q1 and q3) controlled-z (q4)
0	0	0	0	1	1
1	0	0	0	1	1
0	1	0	0	1	1
1	1	0	0	1	1
0	0	1	0	1	1
1	**0**	**1**	**0**	**-1**	**-1**
0	1	1	0	1	1
1	**1**	**1**	**0**	**-1**	**-1**
0	0	0	1	1	1
1	0	0	1	1	1
0	1	0	1	1	1
1	1	0	1	1	1
0	0	1	1	1	1
1	0	1	1	-1	1
0	1	1	1	1	1
1	1	1	1	-1	1

يوضح الشكل(15) الدارة الكلية المطلوبة للبحث عن العنصرين1010,1110=q1q2q3q4 وفق طريقة التنبؤ بقلب الصفحة، حيث احتجنا إلى تكرارين للوصول إلى الحلين الصحيحين، واحتمالية كل من الحلين 47.26%.



الشكل (15): تنفيذ الخوارزمية في حالة البحث عن العنصرين 1010,1110=(q1q2q3q4) بطريقة التنبؤ بقلب الصفحة.

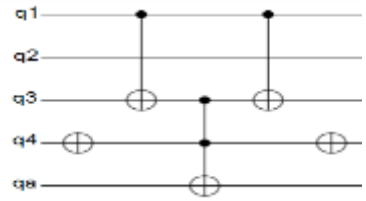
c.البحث عن أربعة حلول:

للبحث عن أربعة حلول نخفض الشروط في مرحلة التنبؤ بحيث ينتج f(x)=1 من أجل أربعة حلول، مثلاً عند تشكيل دارة التنبؤ للبحث عن الحلول q1q2q3q4=1000,1100,0110,0010 نلاحظ ما يلي:

- قيمة البت الرابع صفر في الحلول الأربعة.
- قيمة البيتين الأول والثالث مختلفة بين الحلول وفيما بينهما في الحل نفسه، حيث يأخذ هذين البيتين أحد القيمتين 01 أو 10.
- قيمة البت الثاني مختلفة بين الحلول (0 أو 1).

وبالتالي تكون دارة التنبؤ كما في الشكل(16)، ففي المرحلة الأولى تُطبق بوابة تحكم بالعكس بين البيتين الأول والثالث بحيث يكون خرجها 1 عندما البيتين متعاكسين، وفي المرحلة الثانية تُطبق بوابة تحكم بالعكس ببيتي تحكم (خرج المرحلة الأولى والبت الرابع بعد عكسه) حيث يتحكم هذين البيتين بعكس حالة بت التنبؤ.

يوضح الجدول (3) نتيجة f(x) بعد تنفيذ هاتين المرحلتين، حيث نتوصل إلى أن f(x)=1 من أجل القيم الأربعة المطلوبة

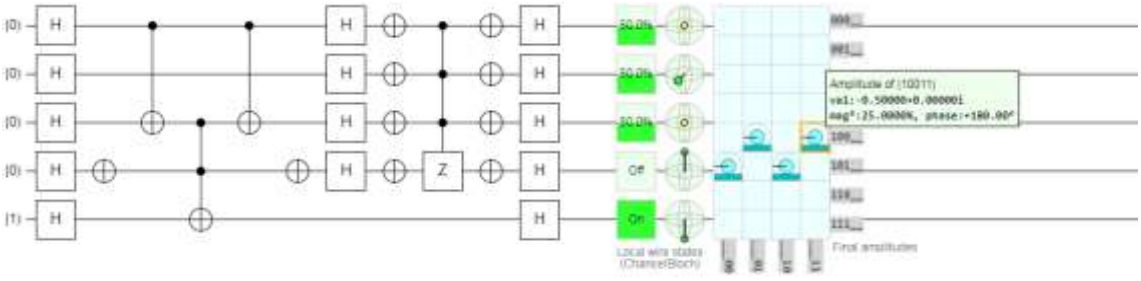


الشكل(16): دارة التنبؤ الثنائي للبحث عن الحلول q1q2q3q4=1000,1100,0110,0010.

الجدول (3): مراحل تنفيذ دارة التنبؤ الثنائي للبحث عن الحلول q1q2q3q4=1000,1100,0110,0010.

q1	$q2$	q3	q4	$\overline{q4}$	M = q1 controlled-Not q3	f(x)=$\overline{q4}$ and M
0	0	0	0	1	0	0
1	**0**	**0**	**0**	**1**	**1**	**1**
0	1	0	0	1	0	0
1	**1**	**0**	**0**	**1**	**1**	**1**
0	**0**	**1**	**0**	**1**	**1**	**1**
1	0	1	0	1	0	0
0	**1**	**1**	**0**	**1**	**1**	**1**
1	1	1	0	1	0	0
0	0	0	1	0	0	0
1	0	0	1	0	1	0
0	1	0	1	0	0	0
1	1	0	1	0	1	0
0	0	1	1	0	1	0
1	0	1	1	0	0	0
0	1	1	1	0	1	0
1	1	1	1	0	0	0

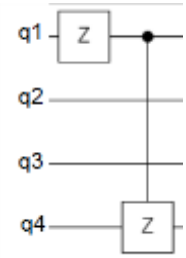
يوضح الشكل(17) الدارة الكلية المطلوبة للبحث عن الحلول q1q2q3q4=1000,0010,0110,1100 وفق طريقة التنبؤ بقلب الصفحة، حيث توصلنا إلى النتيجة بتنفيذ تكرار وحيد، واحتمالية كل حالة من الحالات الصحيحة 25%.



الشكل(17): تنفيذ الخوارزمية للبحث عن الحلول q1q2q3q4=1000,1100,0110,0010 بطريقة التنبؤ الثنائي

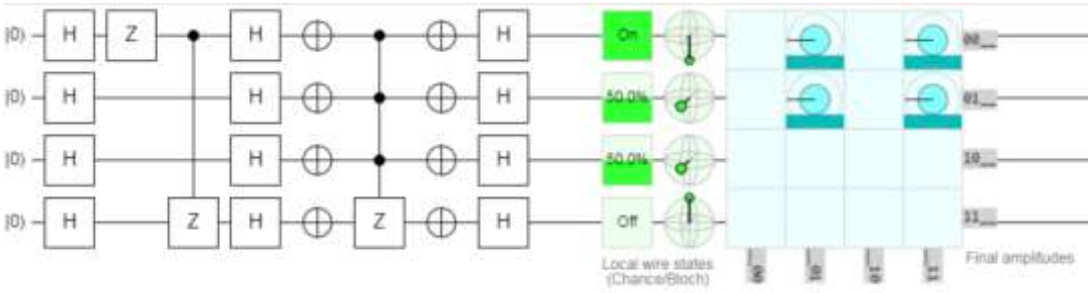
تستنتج دارة التنبؤ بقلب الصفحة للبحث عن أربعة حلول بنفس فلسفة استنتاج دارة البحث عن حلين، بفرض البحث عن الحلول q1q2q3q4=1000,1100,1010,1110 :

نلاحظ أن البت الأول في جميع الحلول مساو للواحد والبت الرابع مساو للصفر، لذلك نشكل دارة التنبؤ كما في الشكل(18)، حيث نضع بوابة قلب الصفحة على خط البت الأول بحيث يجري قلب صفحة الحالات التي يكون فيها البت الأول 1(ثماني حالات تتضمن الحلول الأربعة المطلوبة)، وفي المرحلة الثانية نطبق بوابة التحكم بقلب الصفحة بين خرج المرحلة السابقة (البت المتحكم) والبت الرابع بحيث يتم إعادة قلب صفحة الحالات الأربعة غير المطلوبة والتي تعرضت للقلب في المرحلة الأولى، حيث ينتج عن عملية القلب الأولى قلب صفحة الحالات 1000,1100,1010,1110,1001,1101,1011,1111، بينما يتم في المرحلة الثانية إعادة قلب صفحة الحالات 1001,1101,1011,1111، وبالتالي الوصول إلى النتيجة المطلوبة.



الشكل(18): دارة التنبؤ بقلب الصفحة للبحث عن الحلول q1q2q3q4=1000,1100,1110,1010.

يوضح الشكل(19) الدارة الكلية المطلوبة للبحث عن الحلول q1q2q3q4=1000,1100,1010,1110 وفق طريقة التنبؤ بقلب الصفحة، حيث توصلنا إلى النتيجة بتنفيذ تكرار وحيد.



الشكل (19): تنفيذ الخوارزمية في حالة البحث عن الحلول q1q2q3q4=1000,1100,1110,1010 بطريقة التنبؤ بقلب الصفحة.

الاستنتاجات والتوصيات:

1- اقتصرت الأبحاث السابقة على دراسة الخوارزمية من أجل أعداد محددة من البيتات الكمومية(غالباً ثلاث بيتات كمومية)، بينما قمنا ببناء نموذج خوارزمية كروفر في الحالة العامة باستخدام البوابات الكمومية حيث توصلنا إلى:

a. يتم بناء مراحل التهيئة والتضخيم والقياس الكمومي وفق تشكيل ثابت من بوابات هادامارد والعكس والتحكم بقلب الصفحة والقياس الكمومي.

b. يمكن بناء مرحلة التنبؤ بطريقتين تتضمن كل منهما مجموعة من البوابات الكمومية التي يختلف عددها وتشكيلها باختلاف عدد العناصر المبحوث عنها وقيمتها.

2- أعطى التنفيذ على المحاكي النتائج المتوقعة دون وجود ابتعاد عن الحلول المطلوبة أو ظهور نتائج خاطئة.

3- عند تنفيذ الخوارزمية في فضاء بحث من 16 عنصر توصلنا للنتيجة بعد تطبيق ثلاث تكرارات عند توافر حل وحيد وتكرارين عند توافر حلين وتكرار وحيد عند توافر أربعة حلول، إذ تنخفض عدد التكرارات بازدياد عدد القيم الصحيحة المتوفرة كما هو موضّح في الجدول(4) (حيث N=16 و M هو عدد الحلول).

الجدول (4): عدد التكرارات المطلوبة للبحث عن أعداد مختلفة من الحلول في فضاء بحث من 16 عنصر

	عدد التكرارات من العلاقة العامة لعدد التكرارات (العلاقة(12))	عدد التكرارات بعد التقريب للقيمة الأصغر (Round Down)
حل وحيد	$(\frac{\pi}{4}\sqrt{\frac{N}{M}})=(\frac{\pi}{4}\sqrt{\frac{16}{1}})=3.14$	3
حلّين	$(\frac{\pi}{4}\sqrt{\frac{N}{M}})=(\frac{\pi}{4}\sqrt{\frac{16}{2}})=2.22$	2
ثلاثة حلول	$(\frac{\pi}{4}\sqrt{\frac{N}{M}})=(\frac{\pi}{4}\sqrt{\frac{16}{3}})=1.1$	1

4- تكمن الثغرة الأساسية في هذه الخوارزمية في مشكلة توزع الاحتمالية على الحالات الصحيحة، اذا إن احتمالية ايجاد حل وحيد تكون قريبة من 100%، واحتمالية ايجاد حلين قريبة من 50% لكل منهما، ومن أجل أربعة حلول فإن الاحتمالية قريبة من 25% لكل حل من الحلول وبالتالي عند البحث عن عدد كبير من الحلول كمئة حل مثلاً ستصبح الاحتمالية أقل من 1% لكل من هذه الحلول (من أجل كل تنفيذ وحيد للخوارزمية)، وهذا يشكل صعوبة بالنسبة لعملية القياس، وتكمن المشكلة الثانية في أنه من غير الممكن في كثير من الحالات تحديد عدد الحلول الصحيحة بشكل مسبق قبل القيام بعملية البحث وبالتالي عدم القدرة على معرفة العدد الصحيح من التكرارات المطلوبة للوصول إلى النتيجة، لذلك فإن خوارزمية كروفر مثالية بالنسبة للتطبيقات التي تتطلب البحث عن قيمة وحيدة أو عدد محدود ومعروف من القيم حيث لا تكون الثغرات السابقة مؤثرة.

5- سيترافق تطور الحواسيب الكمومية مع تطور خوارزمية كروفر وزيادة تسريعها، إذ إن زيادة عدد الحالات الكمومية الأساسية المستخدمة في الحواسيب الكمومية يعني زيادة عدد العمليات التي تنفذ بشكل متوازي، وبالتالي زيادة تسريع الخوارزميات الكمومية، بالإضافة إلى الحاجة لعدد بيتات كمومية أقل لتمثيل نفس الحجم من فضاء البحث، فعلى سبيل المثال إنّ استخدام ثلاث حالات كمومية أساسية (0 و 1 و2) بدلاً من حالتين (0 و1) يسمح لنا بتمثيل فضاء بحث من 16 عنصر باستخدام ثلاث بيتات كمومية فقط [15].

المراجع:

- [1] CHUANG,I,L; NIELSEN,M,A.2010,*Quantum Computation and Quantum Information*.10th Anniversary Edition ,Gambridge University Press,U.K,710.
- [2]FEYNMAM,R.1982,*Simulating Physic with Computer. International Journal of Theoretical Physics.*U.S.A.Vol.21,No.6 -7,467- 488.
- [3] BENIOFF,B.1982,*Quantum Mechanical Models of Turning Machines That Dissipate No Energy. Physical Review Letters* .U.S.A. Vol.48 ,No.23,1581 – 1585.
- [4]Deutsh,D.1985,*Quantum Theory, the Church-Turning machine and the universal quantum computer. Proceeding of the Royal Society of London Series A* .U.K. Vol. 400,No.1818 ,97 – 117.
- [5]Grover,L**.**1996**,***A fast quantum mechanical for database search**.** Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*.U.S.A,212 – 219**.**
- [6] HOLZCHEITER.M;HUGHES.R;JAMES.D;GOMES.J;GULLEY.M; KWIAT.P;LAMOREAUX.S;PETERSON.C;SANDBERG.V;SCHAUER.M;SIMMONS;T HORBURN.C;TUPA.D;WANG.P;WHITE.A.1998,*The Los Alamos Trapped Ion Quantum Computer.Fortschritte der Physik.*GERMANY.Vol.46.No.4-5,329-361.
- [7] 04Dec.2017. https://www.nature.com/articles/s41467-017-01904-7.
- [8] DENISENKO,D;NIKITENKOVA,M.2019,*Application of Grover's Quantum algorithm for SDES key Searching. Journal of Experimental and Theoretical Physic.Russia*.vol.128,No.1,25-44;
- [9] Ziatdinov.M.2013,using *frequency analysis and Grover's algorithm to implement known ciphertext attack on symmetric ciphers.Labachevskii Journal of Mathematics.Russia.*Vol.34,No.4,313-315.
- [10] Dhara,S;Sen,D.2018.*Low light Image Enhancement using Grover's Algorithm on superposed luminance levels ,25th International Conference on Image Processing*.Greece,1113-1117.
- [11] Chakrabarty.I;Khan.S;Singh.V.2017,*Dynamic Grover search:application in recommendation system and optimization problems,Quantum Information Processing*.Netherland.Vol.16,No.6, 153.
- [12]Refianti.R;Mutiara.A.2010,*Simulation of Grover's Algorithm Quantum Search in a Classical Computer. International Journal of Computer Science and Information Security. U.S.A.* Vol.8,No.9 ,261-269.
- [13] 20Aug.2018. https://algassert.com/quirk.
- [14] POLAK,W,H; RIEFFEL,E,G,2011,*Quantum Computation A gentle introduction, Massaschusetts Institute of Technology*,England,389.
- [15] 19 Sep.2019. https://phys.org/news/2019-08-complex-quantum-teleportation.html.