

بناء دارات التنبؤ الكمومي انطلاقاً من جداول الحقيقة الكمومية وتوظيفها في تنفيذ الخوارزميات الكمومية (خوارزمية كروفنر)

م.رنيم الابراهيم *

(تاريخ الإيداع 2023/2/14 . قُبل للنشر في 2023/7/13)

□ ملخص □

تتطور التحديات التي تواجه الأجهزة الحاسوبية الحالية مع ازدياد درجة تعقيد العمليات الحاسوبية وقريباً ستصبح القدرة الحاسوبية المتوفرة بين أيدينا عاجزة عن مواجهة معظم هذه التحديات لذا تبرز أهمية إيجاد حل نوعي لمعالجة مشكلات الحواسيب الحالية عن طريق الاستعانة ببنى وتقنيات جديدة في الحوسبة. إن الخوارزميات الكمومية هي خوارزميات رياضية تستند إلى مبادئ علم الكم الفيزيائي وقد اقترحت في تسعينات القرن الماضي وأحدثت ثورة آنذاك نتيجة للتسريع الكبير الذي تقدمه بالمقارنة مع نظيراتها التقليدية. وقد عاد الاهتمام بها مؤخراً نتيجة للتطور التقني الكبير الذي سمح بإنتاج حواسيب كمومية (كما في شركة Ibm الأمريكية وشركة d-wave الكندية) وبالتالي تنفيذ الخوارزميات الكمومية على هذه الحواسيب. تعد مرحلة التنبؤ الكمومي مرحلة أساسية من معظم الخوارزميات الكمومية، ويقترح بحثنا منهجية لتشكيل توابع التنبؤ الكمومية وبناء دارات التنبؤ الكمومي بشكل مباشر من الجداول التي اطلقنا عليها اصطلاحاً "جداول الحقيقة الكمومية" مما يؤمن مرونة وسرعة وتقليصاً لعدد البتات والبوابات الكمومية. سنقوم -اعتماداً على المنهجية المقترحة- بتشكيل دارات التنبؤ الكمومي لتنفيذ خوارزمية كروفنر الكمومية في فضاء بحث مكون من 16 عنصر، وسناقش النتائج الناتجة عن تنفيذ الخوارزمية.

الكلمات المفتاحية: الحوسبة الكمومية- الخوارزميات الكمومية- دارات التنبؤ الكمومي- خوارزمية بحث كروفنر.

Building quantum oracle circuits from quantum truth table and using it in implementation quantum algorithms (Grover's algorithm)

Eng. Ranim Alibraheem*

(Received 14/2/2023 . Accepted 13/7/2023)

□ ABSTRACT

The challenges that facing today's computing devices are evolving with increasing complexity of computer operations. The computing power in our hand will soon be unable to meet most of these challenges ,Therefore it is important to find a qualitative solution to face the problems of current computers by using new technologies and structures in computing

Quantum algorithms are mathematical algorithms based on principles of quantum science, it was proposed in 1990s.it created a revolution at that time because of the great acceleration it offered in compared with traditional counterparts, interested in it has recently returned due to the great technical development that allowed for production of quantum computers (as in American ibm and Canadian d-wave).consequently ,implementing quantum algorithms on these computers.

The quantum oracle stage is an essential stage of most quantum algorithms,our research suggests how to build quantum oracle stage directly from the tables that we have termed "quantum truth tables", This ensures flexibility,speed,and reduction in the number of quantum bits and gates.

Depending on the proposed method, we will configure quantum oracle circuits to implement Grover's algorithm in a 16-element search space and discuss the results of implementing the algorithm.

Keywords: Nanotechnologies -Quantum dots- Sequential circuits ,Quantum computing.

*Academic Assistant- Faculty Of ICTE - Department of CESE - Tartus University -Syria .

1- مقدمة:

ميكانيك الكم هو أحد فروع الفيزياء الذي يدرس الكون على المستوى المتناهي في الصغر وقد حقق منذ بدايات القرن الماضي نتائج هامة في تفسير الكثير من الظواهر الطبيعية كالضوء والكهرباء والمغناطيسية. تستند الحوسبة الكمومية إلى مبدئين أساسيين هما مبدأ التراكب الكمومي (quantum superposition) ومبدأ التشابك الكمومي (quantum entanglement). ينص مبدأ التراكب الكمومي على حقيقة أن الجسيمات دون الذرية تكون في جميع الحالات الممكنة لها في الوقت نفسه، وتأخذ قيمة محددة فقط عند إجراء عملية القياس، وإن توظيف هذا المبدأ في الحوسبة يسمح بالتنفيذ المتوازي للعمليات الحاسوبية، وبالتالي حل المشاكل المتعلقة بازدياد تعقيد العمليات الحاسوبية [1]. أما مبدأ التشابك الكمومي فإنه يستند إلى حقيقة أن قياس حالة أحد الجسيمات المترابطة كمومياً يمكننا من معرفة حالة الجسيم الآخر مباشرة من دون إجراء عملية القياس، وإن توظيف هذا المبدأ الكمومي سيحدث ثورة في مجال الاتصالات اللاسلكية ونقل المعلومات بشكل آني وكذلك في تقنيات تشفير المعلومات [2]. تعد مرحلة التنبؤ الكمومي جزءاً أساسياً من الخوارزميات الكمومية المقترحة حتى الوقت الحالي كخوارزمية كروفنر Grover's algorithm [3] [15]. وخوارزمية دوتش Deutsch algorithm [4]، وتتلخص وظيفة مرحلة التنبؤ في قلب صفحة (تغيير إشارة) قيمة معينة أو مجموعة قيم في فضاء القيم مقارنةً مع بقية القيم. إن أهمية التوصل إلى منهجية لاستنتاج مرحلة التنبؤ يتجلى في أهمية التطبيقات التي من الممكن تحقيقها من خلالها، إذ يمكن استخدام مرحلة التنبؤ في خوارزمية كروفنر لحل المعادلات الرياضية المعقدة [5] أو مثلاً تحديد المفتاح الذي يحقق العلاقة بين كلمة غير مشفرة وناتج تشفيرها، وبالتالي كسر تشفير خوارزميات التشفير [6] مستفيدين بذلك من التسريع الأسّي الذي تؤمنه خوارزمية كروفنر بالمقارنة مع خوارزميات البحث التقليدي.

2- أهداف البحث:

- تمثيل الوظائف المنطقية الأساسية (and, or, not, xor) باستخدام البوابات الكمومية.
- اختزال توابع التنبؤ الكمومي بالاعتماد على قوانين الجبر البوليني من أجل تقليص واختصار البوابات المشكلة لدارات التنبؤ الكمومي.
- بناء دارات التنبؤ الكمومية لتمييز قيم مختلفة في فضاء من 16 قيمة بالاعتماد على الوظائف الأساسية المستنتجة
- توظيف النتائج التي توصلنا إليها في تنفيذ خوارزمية بحث كروفنر وذلك في فضاء بحث من 16 عنصر.

3 - الدراسات السابقة

3-1 الدراسة الأولى [7]: تمت في جامعة Maryland في الولايات المتحدة الأمريكية عام 2017، حيث تم دراسة تنفيذ خوارزمية كروفر في فضاء بحث من ثمانية عناصر على حاسوب كمومي فعلي، يتقاطع هذا البحث مع بحثنا المنجز في دراسة تشكيل دارات التنبؤ الكمومي لتنفيذ الخوارزمية، حيث تم في هذه الدراسة تشكيل جدولين يتضمنان دارات التنبؤ الثنائي والتنبؤ بقلب الصفحة من أجل جميع احتمالات البحث عن حل أو حلين في فضاء بحث من ثمانية عناصر، واعتمد استنتاج مرحلة التنبؤ على قيمة الحل أو الحلين في كل حالة، حيث تم استخدام بوابات العكس والتحكم بالعكس فقط للتنبؤ الثنائي، في حين تم استخدام بوابات العكس والتحكم بقلب الصفحة لإيجاد حل وحيد باستخدام طريقة التنبؤ بقلب الصفحة، وتم استخدام بوابات قلب الصفحة والتحكم بقلب الصفحة فقط للبحث عن حلين بطريقة قلب الصفحة، و تضمن الجدولان ثمان حالات للبحث عن حل وحيد وثمان وعشرين حالة للبحث عن حلين.

3-2 الدراسة الثانية [8]: تمت الدراسة عام 2020 حيث تم دراسة كيفية اختصار الدارات الكمومية بالاعتماد على جداول كارنو بشكل مشابه للحوسبة التقليدية ولكنها لم تتناول تمثيل التوابع الأساسية أو المختصرة باستخدام الوظائف الأساسية الممثلة باستخدام البوابات الكمومية، حيث اعتمدت الدراسة بشكل أساسي على تجزئة بوابة توفولي بأربع وخمس بيئات إلى بوابات جزئية S, H, T, T^+ ومن ثم اختصار البوابات الجزئية معاً.

3-3 الدراسة الثالثة [9] بعنوان (Automatic generation of Grover quantum oracles for arbitrary data structure) تمت عام 2023 وهدفت إلى تمثيل قواعد البيانات غير البنوية باستخدام متبئات (oracles) بحيث يمكن لخوارزمية كروفر أن تبحث في قاعدة البيانات هذه بفعالية.

4- طرائق البحث ومواده:

4-1 البوابات الكمومية

في الدارات الكمومية يجب أن نأخذ بعين الاعتبار النقاط التالية التي تميزها عن الدارات التقليدية [10]:

- لا تحتوي الدارات الكمومية على حلقات أو تغذية عكسية.
- لا يمكن إنجاز تفرع الأسلاك لأن الحالات الكمومية العشوائية (غير المحددة) لا يمكن معرفتها من دون عملية القياس.
- على الرغم من أن عمل الدارة يمكن تحليله باستخدام الحالات التقليدية إلا أن مفهوم التراكب هو ما يعطي الحوسبة الكمومية القوة الحسابية.

خلافاً للحوسبة التقليدية فإن البت الكمومي يتكون من تراكب حالتين كموميتين (0,1) حيث لكل منهما احتمالية ومجموع احتماليتهما يساوي 1، بفرض أن الحالة الكمومية الابتدائية للكيوبت معرفة وفق العلاقة الآتية:

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

عندئذ يتم حساب احتمالية كل من الحالتين عن طريق المعاملين α و β حيث احتمالية الحالة 0 هي $|\alpha|^2$ واحتمالية الحالة 1 هي $|\beta|^2$ ومجموع احتماليتهما هو $|\alpha|^2 + |\beta|^2 = 1$

سنقوم بتعريف بعض البوابات الكمومية الأساسية المستخدمة في بناء الدارات الكمومية، بعض هذه البوابات وحيدة الكيوبت (single qubit)، وبعضها الآخر متعدد الكيوبتات (multiple qubits) [1,10,11].

• بوابة العكس (X-Gate):

إن تطبيق بوابة العكس يؤدي إلى التبدل بين احتماليتي الحالتين 0,1 وتصبح الحالة الجديدة كالآتي:

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

• بوابة قلب الصفحة (Z-Gate):

هذه البوابة لا تغير من الحالة $|0\rangle$ ولكنها تقلب صفحة الحالة $|1\rangle$ لتصبح $-|1\rangle$ كما في المعادلة الآتية:

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

• بوابة هادامارد (Hadamard-Gate):

إن تحويل هادامارد هو مثال على حالة معممة من تحويل فورييه، وهو يقوم بتجزئة شعاع الدخل إلى مركبات وفق الطريقة التراجعية نعرف تحويل هادامارد 1×1 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:

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

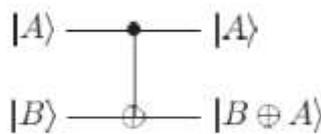
كما تعطى H_2 كالآتي:

$$H_1 \otimes H_1 = H_2 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

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

• بوابة التحكم بالعكس (controlled-Not Gate):

يعطى الرمز الكمومي للبوابة كما في الشكل (1):



الشكل(1): رمز بوابة التحكم بالعكس الكمومية

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

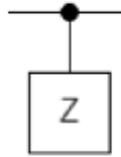
$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

كما يمكن تعميم بوابة التحكم بالعكس من أجل أي عدد من البتات الكمومية حيث تتحكم عدد من البتات بعكس حالة البت الأخير. من أجل ثلاث بيتات كمومية تسمى البوابة عندئذ بوابة توفولي (Toffoli Gate) أو بوابة التحكم المضاعف بالعكس (controlled-controlled-not) وتكون مصفوفة التحويل لها على النحو التالي:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

• بوابة التحكم بقلب الصفحة (controlled-Z Gate):

يعطى الرمز الكمومي لهذه البوابة كما في الشكل (2):



الشكل(2): رمز بوابة التحكم بقلب الصفحة الكمومية

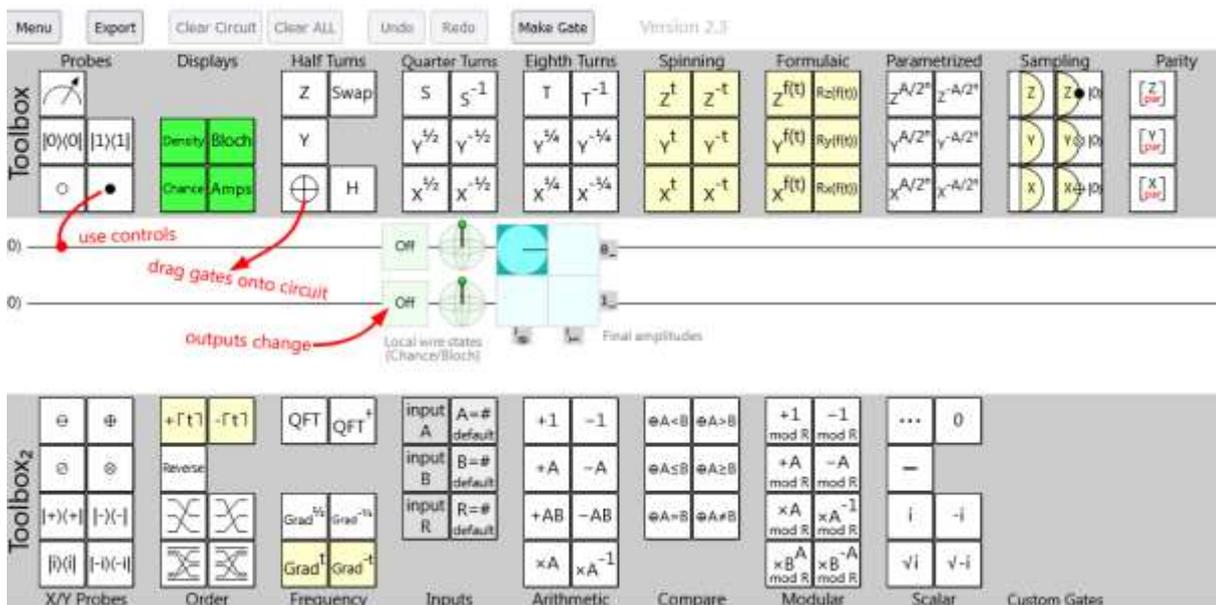
وتقوم هذه البوابة بقلب صفحة الحالة 11 وتعطى مصفوفة التحويل كآتي:

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

يمكن تعميم بوابة التحكم بقلب الصفحة من أجل أي عدد من البتات الكمومية حيث يتم قلب صفحة الحالة التي تكون فيها جميع البتات الكمومية 1.

يجب أن تحقق جميع البوابات الكمومية خاصية الواحدية حيث $U \cdot U^\dagger = 1$ حيث U هي مصفوفة التحويل، و U^\dagger هو المرافق المنقول لهذه المصفوفة.

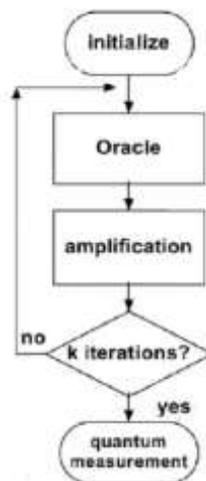
سنستعين بمحاكي quirk وهو منصة على شبكة الانترنت تسمح ببناء ومحاكاة الدارات الكمومية [12].



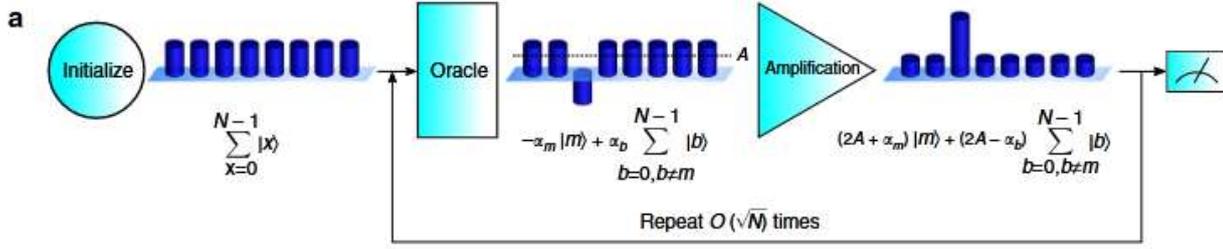
الشكل(3): واجهة محاكي quirk

2-4 خوارزمية كروفنر (Grover's algorithm)

خوارزمية كروفنر هي خوارزمية كمومية موجهة للبحث في قواعد البيانات غير البنيوية (unstructured databases). اقترحها العالم الهندي الأمريكي (Lov Grover) عام 1996 وهي تؤمن تسريعاً أسياً بالمقارنة مع نظيراتها التقليدية، يوضح الشكل(4) مخطط التدفق لهذه الخوارزمية ويوضح الشكل(5) مراحل الخوارزمية الأربعة وهي:مرحلة التهيئة ومرحلة التنبؤ ومرحلة التضخيم ومرحلة القياس الكومومي [3,13,14].



الشكل(4): مخطط تدفق خوارزمية كروفنر.



الشكل (5): مراحل خوارزمية كروفنر

1-2-4 المرحلة الأولى: مرحلة التهيئة (Initialization):

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

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

حيث تمثل n عدد البيتات المستخدمة في تمثيل فضاء البحث، والرمز \otimes يشير إلى الجداء التنسوري (Tensor Product) و N هي عدد الحالات الكمومية الممثلة باستخدام n بت كمومي.

2-2-4 المرحلة الثانية: 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:

$$|x\rangle |q\rangle \rightarrow |x\rangle |q \otimes f(x)\rangle \quad (5)$$

حيث x هو مسجل العنصر الذي نجري عليه عملية التحقق، و q هو بت كمومي ينقلب إذا كان $f(x)=1$ ، ولا يحدث له أي تغيير في بقية الحالات، والرمز \otimes يشير إلى عملية XOR.

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

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

3-2-4 المرحلة الثالثة : مرحلة التضخيم (Amplification)

إن الهدف من مرحلة التضخيم هو زيادة مطال الحالة أو الحالات الصحيحة، وتخفيض مطالات الحالات الخاطئة عن طريق التحويل الآتي:

$$\sum_{i=0}^{N-1} a_i |x_i\rangle \rightarrow \sum_{i=0}^{N-1} (2A - a_i) |x_i\rangle \quad (7)$$

حيث A هو المطال المتوسط، ويعبر عنه بالعلاقة الآتية:

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

بما أنه في نهاية مرحلة التنبؤ يصبح مطال الحالات الصحيحة سالب ، ومطال الحالات الخاطئة موجب، فإن تطبيق عملية التضخيم سيعطي النتيجة التالية:

$$-a_i|x_i \rangle \rightarrow 2A + a_i|x_i \rangle \text{ when } x_i = w \quad (9)$$

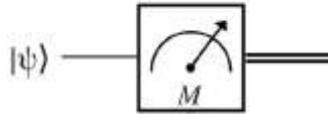
$$a_i|x_i \rangle \rightarrow 2A - a_i|x_i \rangle \text{ when } x_i \neq w \quad (10)$$

4-2-4 المرحلة الرابعة: مرحلة القياس الكمومي (Quantum Measurement):

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

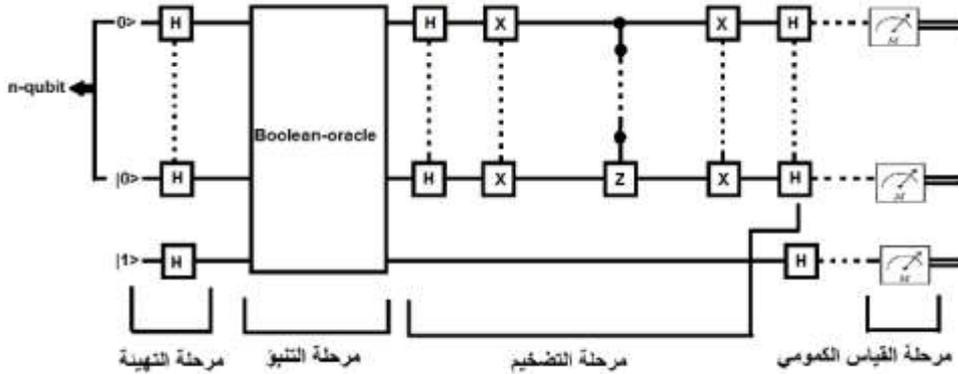
$$|\Psi \rangle = \alpha|0 \rangle + \beta|1 \rangle \quad (11)$$

فإن عملية القياس الكمومي ستنتج 0 باحتمالية $|a|^2$ وتنتج 1 باحتمالية $|\beta|^2$ حيث $1 = |\beta|^2 + |a|^2$ ، ويوضّح الشكل (6) رمز بوابة القياس الكمومي

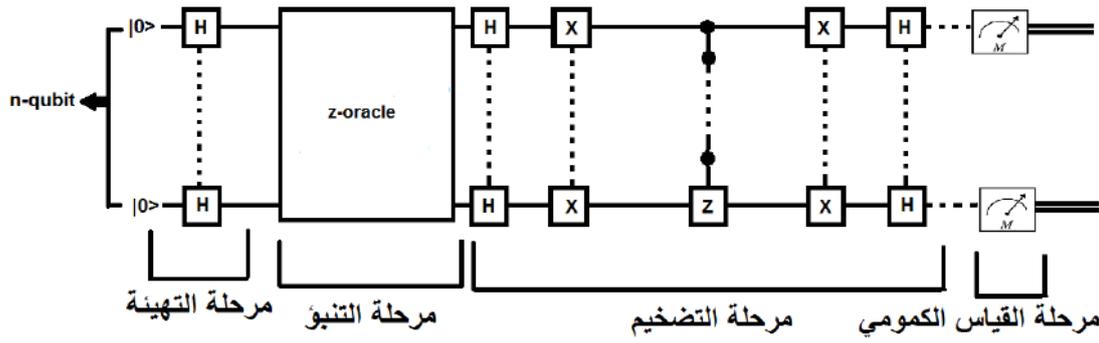


الشكل(6): رمز بوابة القياس الكمومي

إن للتنبؤ الكمومي طريقتان، هما التنبؤ الثنائي والتنبؤ بقلب الصفحة [13]، في التنبؤ الثنائي نحتاج إلى بت التنبؤ لقلب صفحة الحالة أو الحالات الصحيحة، أما في التنبؤ بقلب الصفحة فإن قلب صفحة الحالات الصحيحة لا يحتاج لوجود بت تنبؤ، ويوضح الشكلان (7)، (8) نموذجا دائرة كروفرف في الحالة العامة باستخدام طريقتي التنبؤ.



الشكل(7): نموذج دائرة كروفرف في الحالة العامة (N حالة) باستخدام التنبؤ الثنائي



الشكل (8): نموذج دائرة كروففر في الحالة العامة (N حالة) باستخدام التنبؤ بقلب الصفحة

يتم تكرار مرحلتي التنبؤ والتضخيم حتى الوصول إلى النتيجة المطلوبة، وتعطى العلاقة المعبرة عن عدد التكرارات المطلوبة على النحو التالي :

$$K = \frac{\pi}{4} \sqrt{\frac{M}{N} - \frac{1}{2}} \quad (12)$$

3-4 التنبؤ الثنائي: تمثيل الوظائف المنطقية الأساسية باستخدام البوابات الكومبية

1-3-4 تمثيل وظيفة xor باستخدام البوابات الكومبية:

ليكن لدينا التابع $f_1(x)$:

$$f_1(x) = x_1 \otimes x_2 \quad (13)$$

لتمثيل وظيفة xor يتم الاستعانة ببوابة التحكم بالعكس، حيث إن تحكم البت الأول بالبت الثاني ينتج لدينا جدول الحقيقة (1) والموافق لجدول الحقيقة المنطقي لبوابة xor .

الجدول (1): جدول الحقيقة الكومبي للتابع f_1

x_1	x_2	$f_1(x)$
0	0	0
0	1	1
1	0	1
1	1	0

2-3-4 تمثيل الوظيفة and باستخدام البوابات الكومبية

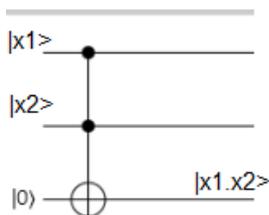
ليكن لدينا التابع $f_2(x)$:

$$f_2(x) = x_1 \cdot x_2 \quad (14)$$

لتشكيل وظيفة and سنستخدم بوابة التحكم بالعكس أيضاً ولكن سنلجأ إلى إضافة بت كومبي وتشبيته على القيمة 0 من أجل الحصول على الوظيفة المنطقية لبوابة and كما في الشكل (9) حيث نحتاج إلى ثلاث مداخل أحدها ثابت ومخرج ويوضح الجدول (2) جدول الحقيقة الكومبي لهذا التابع.

الجدول(2): جدول الحقيقة الكومبي للتابع $f_2(x)$

X_1	X_2	X_3	$f_2(x)$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	1



الشكل(9): تمثيل الوظيفة and باستخدام البوابات الكومبية CCNOT في التنبؤ الثنائي.

3-3-4 تمثيل الوظيفة or باستخدام البوابات الكومبية:

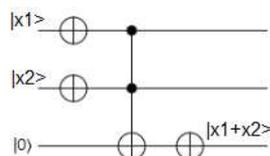
ليكن لدينا التابع $f_3(x)$:

$$f_3(x) = x_1 + x_2 \quad (15)$$

إن أقرب بوابة منطقية تعطينا خرج قريب لخرج بوابة or هي بوابة التحكم بالعكس، ومع ذلك فإننا لم نتمكن من إيجاد طريقة مباشرة للحصول على الخرج المطلوب كإضافة مدخل وتثبيت قيمته على 0 أو 1، وللحصول على وظيفة بوابة or سنلجأ إلى طريقة غير مباشرة بالاستعانة بقوانين الجبر البوليني(قانون دمورغان) والتمثيل الكومبي لوظيفة and على النحو التالي:

$$f_4(x) = \overline{\overline{x_1} \cdot \overline{x_2}} = \overline{\overline{x_1}} + \overline{\overline{x_2}} = x_1 + x_2 \quad (16)$$

أي أنه وللحصول على وظيفة or سنستخدم وظيفة and مع عكس المداخل والنتيجة كما في الشكل (10)



الشكل(10): تمثيل الوظيفة or باستخدام البوابات الكومبية CCNOT في التنبؤ الثنائي.

4-3-4 تمثيل الوظيفة not باستخدام البوابات الكومبية:

لتمثيل الوظيفة not نستخدم بوابة التحكم بالعكس الكومبية:

$$f_5(x) = \bar{x} \quad (17)$$

حيث من الجدير بالإشارة أن بوابة توفولي هي حالة معمة من بوابة التحكم بالعكس عندما عدد الببتات المتحكممة 2 أو أكثر.

5-3-4 بناء دارة التنبؤ الكومبي الثنائي لتمييز قيمة واحدة انطلاقاً من جدول الحقيقة

بفرض نريد تشكيل دارة التنبؤ الكومبي لتمييز القيمة 0111 وكخطوة أولى نقوم ببناء جدول الحقيقة الكومبي لتابع التنبؤ على النحو التالي:

الجدول(3): جدول الحقيقة الكومبي لاستنتاج التابع الكومبي لتمييز القيمة

$$0111q_4q_3q_2q_1 =$$

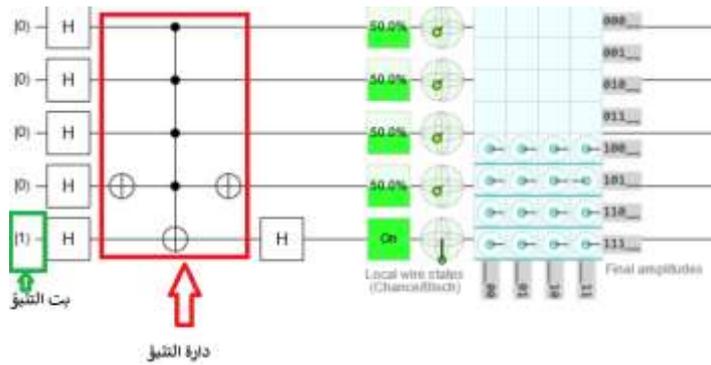
q_1	q_2	q_3	q_4	$f_5(q)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	1
1	1	1	1	0

حيث أن البت الكومبي الأخير q_5 يمكن تهيئته على الواحد ثم تطبيق بوابة الهادامار عليه في المرحلة التالية لينتج عكس صفحة الحالة الكومبية المطلوبة (كما يمكن تهيئتها على القيمة 0 وإضافة بوابة العكس).

يمكن كتابة تابع التنبؤ لتمييز هذه القيمة بدلالة وظيفتي and و not على النحو التالي:

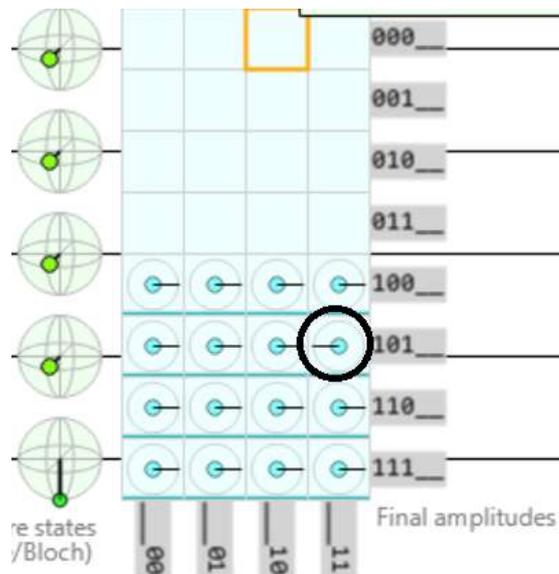
$$f_6(q) = q_1 q_2 q_3 \bar{q}_4 \quad (18)$$

أي أننا نحتاج لبوابة تحكم بالعكس بخمسة مداخل وخرج وبوابة عكس لتمثيل هذا التابع كما في الشكل (11) حيث طبقنا بوابة عكس على البت q_4 لأننا نريد أن تعكس بوابة التحكم قيمة بت التنبؤ عندما هذا البت 0 وباقي البتات 1.



الشكل(11): دائرة التنبؤ الكمومي الثنائي لتمييز القيمة $0111q_4q_3q_2q_1$.

يمثل الشكل(12) الجزء الخاص بالنتيجة للدائرة السابقة(مرحلة القياس الكمومي) حيث إن إشارة جميع الحالات الكمومية موجبة (نحو اليمين) أما إشارة الحالة الكمومية الموافقة للدخل $0111q_4q_3q_2q_1$ هي سالبة (نحو اليسار)



الشكل(12):مرحلة القياس الكمومي دائرة التنبؤ الكمومي الثنائي لتمييز القيمة $0111q_4q_3q_2q_1$.

حيث إن وجود بوابات الهادامار يؤدي إلى خلق تراكب كمومي من البيئات الأربعة (6 حالة متراكبة) كما ويجري عكس الحالة التي يكون خرج تابع التنبؤ فيها يساوي 1 كما هو موضح في العلاقة التالية:

$$\begin{aligned} |\Psi\rangle = & \frac{1}{16} |0000\rangle + \frac{1}{16} |1000\rangle + \frac{1}{16} |0100\rangle + \frac{1}{16} |1100\rangle + \frac{1}{16} |0010\rangle \\ & + \frac{1}{16} |1010\rangle + \frac{1}{16} |0110\rangle + \frac{1}{16} |1110\rangle + \frac{1}{16} |0001\rangle + \frac{1}{16} |1001\rangle + \frac{1}{16} |0101\rangle \\ & + \frac{1}{16} |1101\rangle + \frac{1}{16} |0011\rangle + \frac{1}{16} |1011\rangle - \frac{1}{16} |0111\rangle + \frac{1}{16} |1111\rangle \quad (19) \end{aligned}$$

4-3-6 بناء دارة التنبؤ الكومبي لتمييز عدة قيم انطلاقاً من جدول الحقيقة الكومبي

بفرض نريد تشكيل دارة التنبؤ الكومبي لتمييز القيم 1000,0010,0110 وكخطوة أولى نقوم ببناء جدول الحقيقة الكومبي لتابع التنبؤ على النحو التالي:

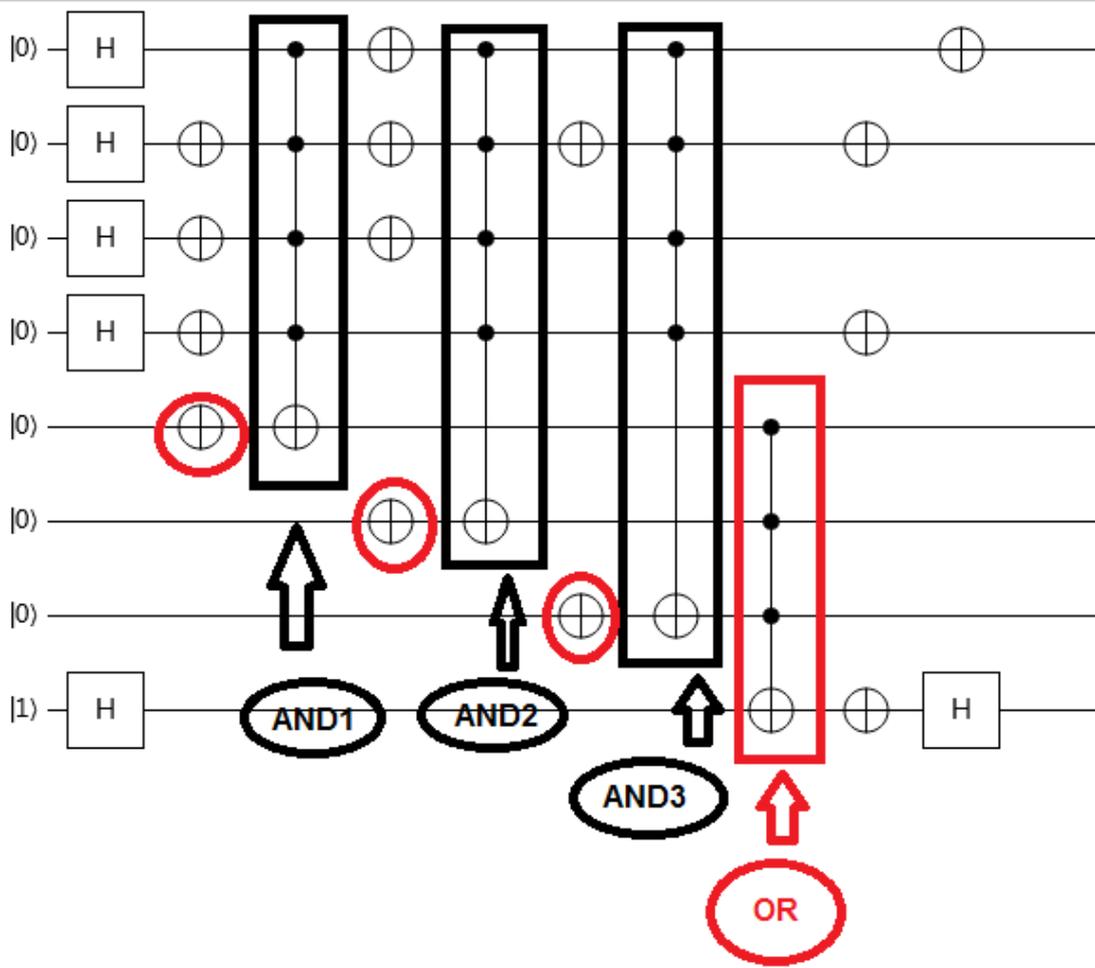
الجدول (4): جدول الحقيقة الكومبي لاستنتاج التابع الكومبي لتمييز القيم 1000,0010,0110

q_1	q_2	q_3	q_4	$f_7(q)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0
1	1	1	1	0

يمكن كتابة تابع التنبؤ لتمييز هذه القيم الثلاث على النحو التالي:

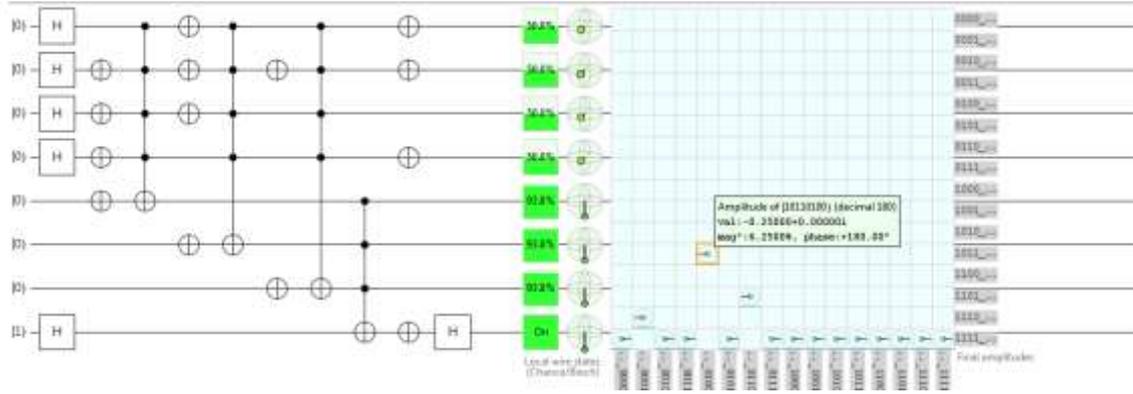
$$f_7(q) = q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 + \bar{q}_1 q_2 q_3 \bar{q}_4 + \bar{q}_1 \bar{q}_2 q_3 \bar{q}_4 \quad (20)$$

لتمثيل تابع التنبؤ السابق باستخدام البوابات الكمومية قمنا باستخدام ثلاث بوابات توفولي من أجل استخلاص المضاريب الثلاثة ثم طبقنا بوابة OR وفق لجمعهم وذلك وفق الطريقة التي تم استنتاجها سابقاً لبناء بوابة OR كما في الشكل (13). حيث البتات 5 و 6 و 7 هي بتات مساعدة لا تهمنا عن إجراء عملية القياس، كما أننا لم نقم بتوليد تراكب كمومي من هذه البتات باستخدام بوابات هادامارد. كما أن البتات الأربعة الأولى التي يشكل تراكبها فضاء البحث ينبغي إعادتها إلى الحالة الابتدائية باستخدام بوابات العكس.



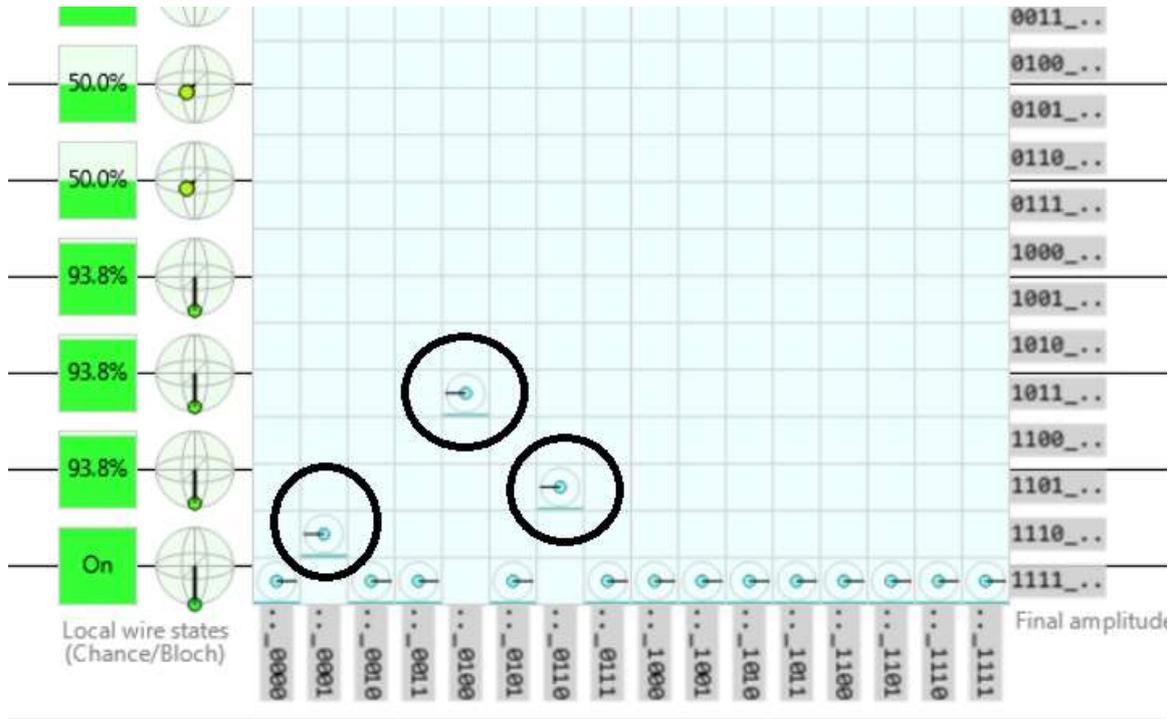
الشكل (13): دائرة التنبؤ الكمومي الثنائي لتمييز القيم 1000,0010,0110

وبالتالي تكون الدارة الكلية بعد إضافة مرحلة القياس كما هو موضح في الشكل (14)



الشكل(14): دائرة التنبؤ الكمومي الثنائي لتمييز القيم 1000,0010,0110

يمثل الشكل(15) الجزء الخاص بالنتيجة للدائرة السابقة(مرحلة القياس الكمومي) حيث إن إشارة جميع الحالات الكمومية موجبة (نحو اليمين) أما إشارة الحالة الكمومية الموافقة للدخل $q_1 \overline{q_2} \overline{q_3} \overline{q_4} + \overline{q_1} q_2 q_3 \overline{q_4} + \overline{q_1} \overline{q_2} q_3 \overline{q_4} + \overline{q_1} \overline{q_2} q_3 q_4$ هي سالبة (نحو اليسار).



الشكل(15):مرحلة القياس الكمومي دائرة التنبؤ الكمومي الثنائي لتمييز القيم 1000,0010,0110.

حيث إن وجود بوابات الهادامار يؤدي إلى خلق تراكب كمومي من البيتات الأربعة (16 حالة متراكبة) كما ويجري عكس الحالة التي يكون خرج تابع التنبؤ فيها يساوي 1 كما هو موضح في العلاقة التالية(حيث يعرض المحاكى النتيجة بحيث البت الأقل أهمية في اليمين):

$$\begin{aligned} |\Psi\rangle = & \frac{1}{16}|0000\rangle + \frac{1}{16}|1000\rangle - \frac{1}{16}|0100\rangle + \frac{1}{16}|1100\rangle + \frac{1}{16}|0010\rangle \\ & + \frac{1}{16}|1010\rangle - \frac{1}{16}|0110\rangle + \frac{1}{16}|1110\rangle - \frac{1}{16}|0001\rangle + \frac{1}{16}|1001\rangle + \frac{1}{16}|0101\rangle \\ & + \frac{1}{16}|1101\rangle + \frac{1}{16}|0011\rangle + \frac{1}{16}|1011\rangle + \frac{1}{16}|0111\rangle + \frac{1}{16}|1111\rangle \quad (21) \end{aligned}$$

حيث المحاكي المتوفر يسمح بقياس جميع بيئات الدارة ولكننا نهتم بخرج البيئات الأربعة الأولى فقط. هذا ويمكن استخدام هذه الطريقة من أجل تمييز أي عدد من القيم في فضاء القيم.

كما هو ملاحظ فإن استخدام and و or الأساسيتين في بناء توابع التنبؤ الكومبي بدون أي اختزال يتطلب عدد كبير من البوابات والبيئات الكومبية التي يزداد عددها بازدياد عدد القيم التي نريد تمييزها كما هو موضح في الجدول (5)

الجدول (5): عدد البوابات الكومبية المطلوبة لتشكيل دارات التنبؤ في كل حالة

عدد البوابات الكومبية المطلوبة في دارة التنبؤ الكومبي	عدد القيم المطلوب تمييزها
5	1
15	2
20	3

سنلجأ إلى قوانين الجبر البوليني من أجل اختزال توابع التنبؤ الكومبي ومحاولة تخفيض عدد البوابات

الكومبية، وكما هو واضح فإن تابع التنبؤ الكومبي لتمييز قيمة وحيدة لا يحتاج أي اختزال.

4-3-7 اختزال تابع التنبؤ الكومبي الثنائي واختصار دارة التنبؤ الكومبي لتمييز عدة قيم

ليكن لدينا التابع الذي يمثل تابع التنبؤ لتمييز القيم $q_1 q_2 q_3 q_4 = 0010, 0110, 1000$:

$$\begin{aligned} f_3(q) = & q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 + \bar{q}_1 q_2 q_3 \bar{q}_4 + \bar{q}_1 \bar{q}_2 q_3 \bar{q}_4 = \bar{q}_1 q_3 \bar{q}_4 (q_2 + \bar{q}_2) + q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 = \\ & \bar{q}_1 q_3 \bar{q}_4 + q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 = \bar{q}_4 (\bar{q}_1 q_3 + q_1 \bar{q}_2 \bar{q}_3) = \bar{q}_4 \bar{q}_1 q_3 + \bar{q}_4 q_1 \bar{q}_2 \bar{q}_3 \quad (22) \end{aligned}$$

يتضمن التابع المختزل ثلاث جداءات ومجموعين، ولتخفيض عدد العمليات وبالتالي عدد البوابات سنلغي

القوسين (توزيع الضرب على الجمع) لتخفيض عدد البوابات من 4 إلى 3 فيصبح التابع كثير حدود من حدين

ويكون لدينا عمليتي جداء و عملية مجموع، والدارة الكومبية لتمثيله موضحة في الشكل (16).

إن فضاء هيلبرت (Hilbert space) الذي تمثل فيه الحالات الكومبية يتمتع بجميع خواص الفضاءات

الرياضية الأخرى - كالفضاء الخطي (linear space) والفضاء القياسي (Normed space) - ومنها خاصية

توزيع الضرب على الجمع بالإضافة إلى خواص إضافية يتمتع بها هذا الفضاء بشكل خاص [14].

إن البيئات الأربعة الأولى لم نعلم بتغيير قيمتها بل استخدمناها لتوليد فضاء البحث وتمييز القيم المطلوبة

و تم تطبيق عدد زوجي من بوابات العكس بحيث تحافظ على قيمتها كما وقمنا بتطبيق بوابة الهادامارد على كل

منها مرة واحدة لنحافظ على حالة التراكب الكومبي المطلوبة لتوليد فضاء البحث.

إن عملية اختزال تابع التنبؤ يجب أن تعطي التابع الناتج القيمة 1 فقط من أجل المركبات التي نريد قلب

صفحتها وهذا ما يحققه التابع المختزل حيث إن عمل بوابة controlled-not هو تمرير الحالة الكومبية عندما أحد

البيئات المتحكم لا يساوي 1 وعكس صفحة الحالة الكومبية عندما جميع البيئات المتحكممة 1 وكما هو موضح في

الشكل (16) فقد تمت تهيئة بت التنبؤ على القيمة 1. وبالتالي عندما جميع بيئات التحكم (1) (عندما الحالة المدخلة

هي الحالة التي نريد تمييزها) يمكن حساب خرج مرحلة التنبؤ (بت التنبؤ) بالاعتماد على مصفوفات التحويل (عندما بيتات التحكم 1) :

$$[0 \ 1] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} [0 \ -2] = [0 \ -1]$$

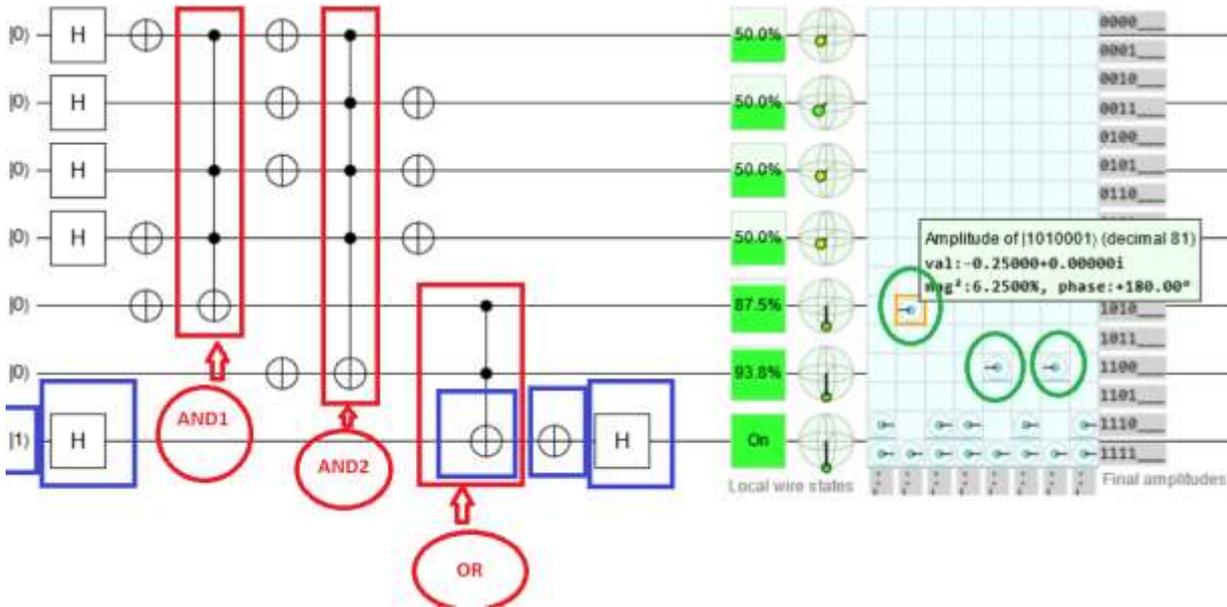
أي أن قيمة الخرج -1- باحتمالية 100%.

ويمكن حساب خرج بت التنبؤ بالاعتماد على مصفوفات التحويل (عندما أحد بيتات التحكم 0) :

$$[0 \ 1] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} [0 \ 2] = [0 \ 1]$$

حيث البت الأخير هو بت التنبؤ، أما البيتين الخامس والسادس فهما بيتان مساعدان لانجاز وظيفة Or التي نحن بحاجة إليها لبناء تابع التنبؤ لذلك لم نقم بتوليد تراكب كمومي من هذين البيتين كما لم نهتم بإعادتهما إلى الحالة الابتدائية ويمكن إهمالهما عند إجراء عملية القياس.

وكما هو يظهر لدينا في الشكل (16) فإن احتمالية كل حالة من الحالات هو $6.25\% = \left(\frac{1}{16}\right)^2$



الشكل (16): دارة التنبؤ الكمومي الثنائي لتمثيل التابع f_8

4-4 التنبؤ بقلب الصفحة: تمثيل الوظائف المنطقية الأساسية باستخدام البوابات الكمومية:

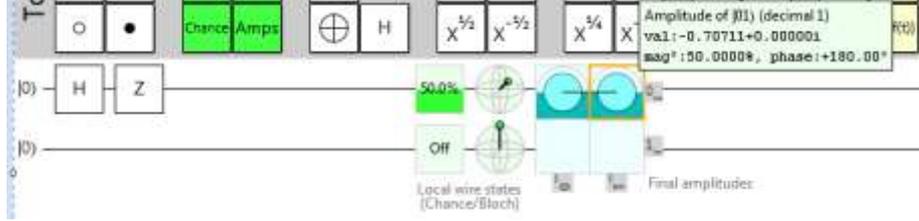
4-4-1 تمثيل وظيفة قلب الصفحة باستخدام البوابات الكمومية:

بفرض لدينا التابع المعبر عن عملية قلب صفحة حالة البت الكمومي q_1 :

$$f_9(q_1) = -q_1 \quad (23)$$

للحصول على وظيفة قلب الصفحة نستخدم البوابة Z فعلى سبيل المثال تكون الدارة الكمومية المطلوبة لتنفيذ التابع أعلاه كما في الشكل (17) حيث يتم قلب الصفحة عندما البت 1.

ملاحظة: يسمح المحاكى الكومى الذي نستخدمه بإدراج بيتين كموميين كحد أدنى و16 بيتاً كحد أقصى



الشكل (17): دارة التنبؤ الكومى بقلب الصفحة لتمثيل التابع f_9

2-4-4 تمثيل وظيفة العكس مع قلب الصفحة باستخدام البوابات الكمومية:

ليكن لدينا التابع f_{10} المعبر عن عملية قلب صفحة وعكس حالة البت الكومى q_1

$$f_{10}(q_1) = \bar{q}_1 \quad (24)$$

لتمثيل عملية العكس سنستخدم بوابة العكس وقلب الصفحة معاً، وعليه تكون الدارة الكمومية لتنفيذ التابع السابق كما في الشكل (18) حيث يتم قلب صفحة الحالة $|0\rangle$ ، حيث ينتج عن استخدام بوابة الهادامارد توليد بت كومى متراكب من حالتين كموميتين أساسيتين كما في العلاقة التالية:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (25)$$

في المرحلة التالية يتم تطبيق بوابة قلب الصفحة Z على الحالة الكمومية السابقة فتصبح الحالة الكمومية السابقة كما هو موضح في العلاقة (26):

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad (26)$$

وأخيراً يجري تطبيق بوابة العكس مما يؤدي إلى عكس كل من الحالتين الكموميتين الأساسيتين المكونين للحالة الكمومية السابقة كما هو موضح في العلاقة (27):

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle \quad (27)$$

حيث أنّ الحالة الكمومية الناتجة (النهائية) قد تم فيها قلب صفحة الحالة $|0\rangle$ وهذه هي وظيفة التابع f_{10} ،

كما يمكن التبديل بين موقعي بوابة العكس وقلب الصفحة والحصول على نفس النتيجة السابقة.



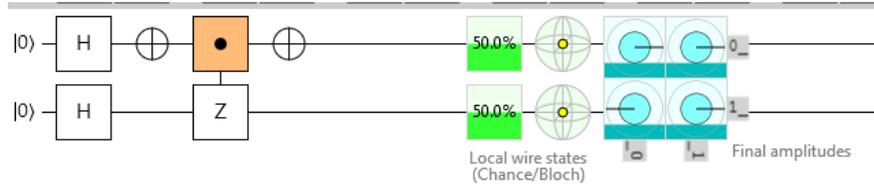
الشكل (18): دارة التنبؤ الكومى بقلب الصفحة لتمثيل التابع f_{10}

3-4-4 تمثيل وظيفة and بمدخلين مع قلب الصفحة باستخدام البوابات الكمومية:

بفرض لدينا التابع المعبر عن قلب صفحة الحالة الناتجة عن عملية and بين الحالة $|0\rangle$ للبت الكمومي q_1 والحالة $|1\rangle$ للبت q_2 .

$$f_{11}(q) = \bar{q}_1 q_2 \quad (28)$$

لتمثيل وظيفة and سنستخدم بوابة التحكم بقلب الصفحة حيث أنه وكما هو واضح من مناقشة البوابة وتابع التحويل، لها فإن حالة البيتين معاً تتحكم بعملية قلب الصفحة، وعليه تكون الدارة الكمومية لتنفيذ التابع أعلاه كما في الشكل (19).



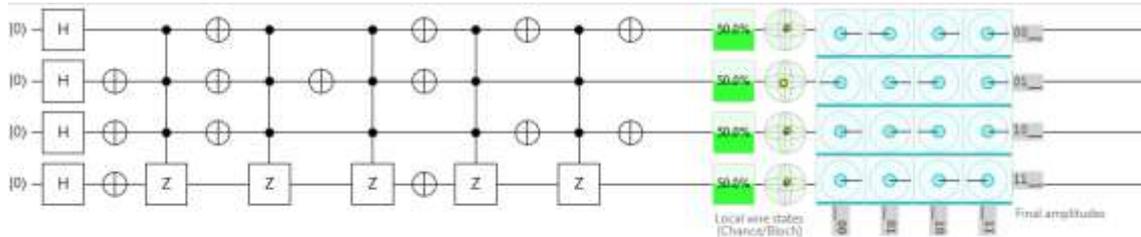
الشكل(19): دارة التنبؤ الكمومي بقلب الصفحة لتمثيل التابع f_{11}

4-4-4 تمثيل وظيفة or بمدخلين مع عكس الصفحة باستخدام البوابات الكمومية

إن تمثيل وظيفة or باستخدام بوابة قلب الصفحة Z مشابه للتمثيل باستخدام بوابات ccNOT المستنتج سابقاً مع اختلاف وحيد هو أن عملية قلب الصفحة تتم عن طريق استبدال البت المتحكم به ببوابة قلب الصفحة لنحصل على بوابة (Controlled-controlled-Z) بحيث أنه عندما تكون جميع البيئات المتحكممة 1 فإن البوابة ستعطي -1 وليس 1 أي أن خرج جميع الحالات الصحيحة لبوابة or يكون -1، بفرض لدينا التابع التالي المكوّن من خمسة حدود والذي يحتاج تمثيله إلى استخدام وظيفة or ووظيفة قلب الصفحة :

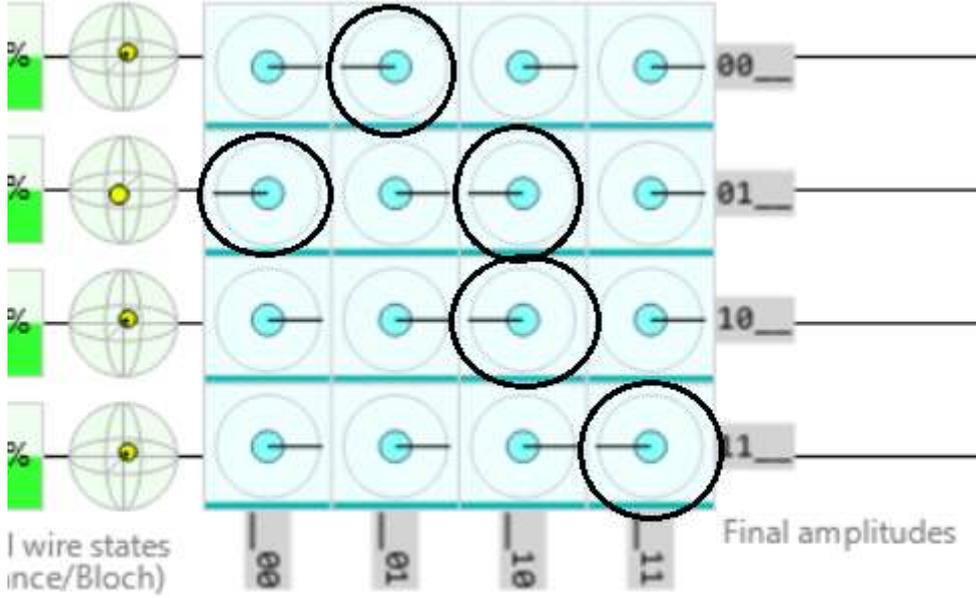
$$f_{12}(q) = q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 - \bar{q}_1 q_2 q_3 \bar{q}_4 - \bar{q}_1 \bar{q}_2 q_3 \bar{q}_4 - q_1 q_2 q_3 q_4 - q_1 \bar{q}_2 q_3 \bar{q}_4 \quad (29)$$

حيث سنلجأ إلى استخدام بوابة التحكم بقلب الصفحة في كل مرة لقلب صفحة حالة وحيدة ودون التأثير على بقية الحالات بما يشبه عمل المرشح حيث قد تؤثر عدة معالجات على الإشارة ولكن كل منها ضمن تردد معين يحدده المرشح، فعلى سبيل المثال ولتمثيل التابع أعلاه نحتاج إلى خمس بوابات تحكم بقلب الصفحة تستخدم كل واحدة منها لقلب صفحة حالة وحيدة فقط وبالنتيجة يتم قلب صفحة الحالات الخمس المطلوبة فقط وهذا ما يوضّحه الشكل(20).



الشكل(20): دارة التنبؤ الكمومي الثنائي لتمثيل التابع f_{12}

يمثل الشكل (21) الجزء الخاص بالنتيجة للدائرة السابقة (مرحلة القياس الكومومي) حيث إن إشارة جميع الحالات الكومومية موجبة (نحو اليمين) أما إشارة الحالة الكومومية الموافقة للتابع f_{13} هي سالبة (نحو اليسار).



الشكل(21):مرحلة القياس الكومومي لدائرة التنبؤ الكومومي الثنائي لتمثيل التابع f_{12}

5-4-4 تمثيل وظيفة xor بمدخلين مع عكس الصفحة باستخدام البوابات الكومومية:

تكتب وظيفة xor كتاب على النحو التالي:

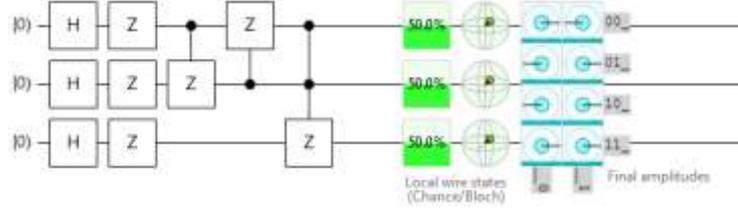
$$f_{13}(q) = -\bar{q}_1q_2 - \bar{q}_2q_1 \quad (30)$$

يهدف تمثيل وظيفة ال xor باستخدام بوابة قلب الصفحة إلى تمييز الخرج الصحيح عن طريق قلب الصفحة عندما قيمتي البيتان الكوموميان مختلفان مثلاً كما الحالتان الكوموميتان $|01\rangle$ أو $|10\rangle$ ، حيث إن إضافة بوابة الهادامارد على الدخل يسمح بتوليد جميع الحالات المحتملة ولكننا نهدف لبناء الدارة الكومومية التالية لبوابة الهادامارد التي تسمح لنا بقلب الصفحة عندما الحالتين مختلفتين فقط حيث تمثل بوابة xor ثنائية المداخل انطلاقاً من وظيفتي and والعكس المستنتجة مسبقاً كما في الشكل(22).

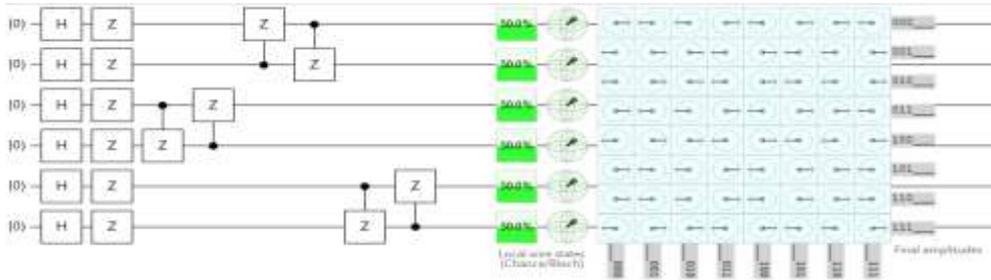


الشكل(22): دارة التنبؤ الكومومي الثنائي لتمثيل التابع f_{13}

تعتمد منهجية استنتاج وظيفة XOR على كون عدد البيتات زوجي أو فردي، حيث عندما يكون عدد البيتات زوجي نطبق بوابة XOR بمدخلين بين كل بيتين متجاورين، وعندما يكون عدد البيتات فردي نطبق عملية XOR إضافية بين نتيجة البيتات الزوجية والبت الإضافي كما هو موضح في الشكلين (23)، (24).

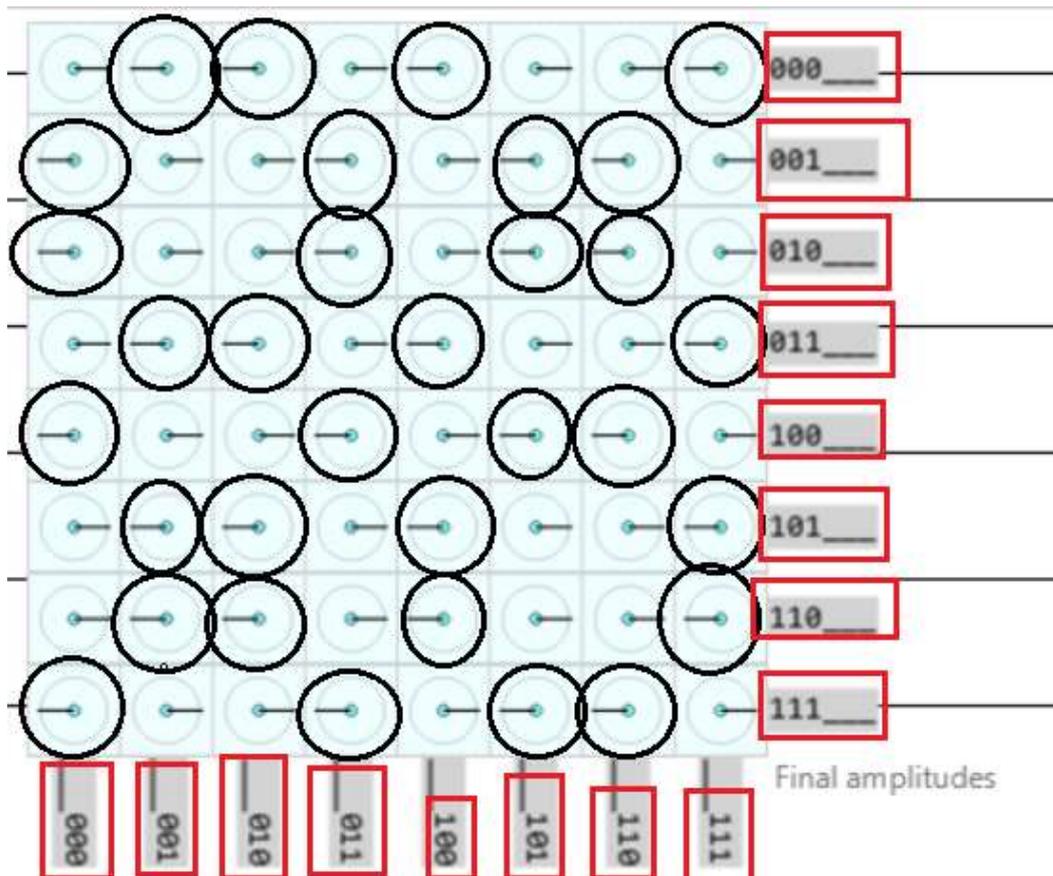


الشكل (23): دارة التنبؤ الكمومي الثنائي لتمثيل التابع $-q_1 \otimes q_2 \otimes q_3$



الشكل (24): دارة التنبؤ الكمومي الثنائي لتمثيل التابع $-q_1 \otimes q_2 \otimes q_3 \otimes q_4 \otimes q_5 \otimes q_6$

يوضح الشكل التالي مرحلة القياس الكمومي للدارة السابقة حيث إنه تم قلب صفحة جميع الحالات التي مجموع البيتات الستة فيها فردي (وظيفة XOR) مثلاً الحالة الكمومية $|010110\rangle$ قد تم عكس صفحاتها.



الشكل (25): مرحلة القياس الكمومي للدائرة الكمومية لتمثيل التابع $-q_1 \otimes q_2 \otimes q_3 \otimes q_4 \otimes q_5 \otimes q_6$

4-4-6 اختزال تابع التنبؤ الكمومي واختصار دائرة التنبؤ الكمومي بقلب الصفحة لتمييز عدة قيم

بفرض أننا نريد تمييز القيم 1000,0110,0010، أولاً نقوم ببناء جدول الحقيقة الكمومي:

الجدول (6): جدول الحقيقة الكمومي لتمييز القيم 0010,0110,1000

q_1	q_2	q_3	q_4	$f_{14}(q)$
0	0	0	0	1
0	0	0	1	1
0	0	1	0	-1
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	-1
0	1	1	1	1
1	0	0	0	-1
1	0	0	1	1
1	0	1	0	1

1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1
1	1	1	1	1

وعليه يمكن كتابة تابع التنبؤ الكمومي على النحو التالي:

$$f_{14}(q) = -q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 - \bar{q}_1 q_2 q_3 \bar{q}_4 - \bar{q}_1 \bar{q}_2 q_3 \bar{q}_4 = -\bar{q}_1 q_3 \bar{q}_4 (q_2 + \bar{q}_2) - q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 = -\bar{q}_1 q_3 \bar{q}_4 - q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4 \quad (31)$$

يتضمن التابع الناتج ثلاث جداءات وعملية قلب صفحة، ولتخفيض عدد العمليات وبالتالي عدد البوابات نبقى التابع على شكل SOP ($-\bar{q}_1 q_3 \bar{q}_4 - q_1 \bar{q}_2 \bar{q}_3 \bar{q}_4$) لأنه يتطلب عدد بوابات أقل، فيكون التابع كثير حدود من حدين ويكون لدينا عمليتي قلب للصفحة، والدارة الكمومية لتمثيله موضحة في الشكل (26).



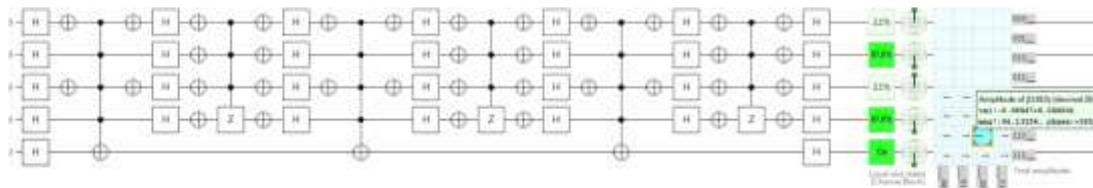
الشكل(26): دارة التنبؤ الكمومي بقلب الصفحة لتمييز القيم 0010,0110,1000

4-5 تنفيذ خوارزمية كروفر في فضاء بحث من 16 عنصر

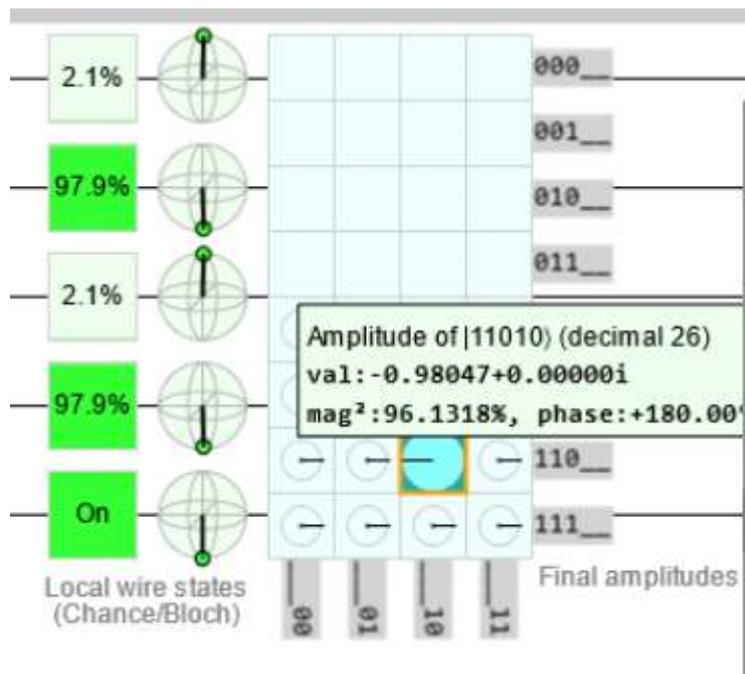
سنقوم بتنفيذ خوارزمية كروفر في فضاء بحث من 16 عنصر حيث سنقوم باستبدال مرحلة التنبؤ في المخطط العام لخوارزمية كروفر بتتابع التنبؤ المستنتجة.

4-5-1 البحث عن حل وحيد باستخدام طريقة التنبؤ الثنائي

عند البحث عن حل وحيد فإننا نحتاج إلى ثلاث تكرارات للوصول إلى النتيجة، ونستنتج ذلك من العلاقة العامة المعبرة عن عدد التكرارات (العلاقة(12))، يمثل الشكل(27) الدارة الكمومية للبحث عن العنصر 0101 بطريقة التنبؤ الثنائي حيث طبقنا ثلاث تكرارات للوصول للنتيجة ونتاجت احتمالية الحالة الصحيحة 96.13% (الشكل(28)).



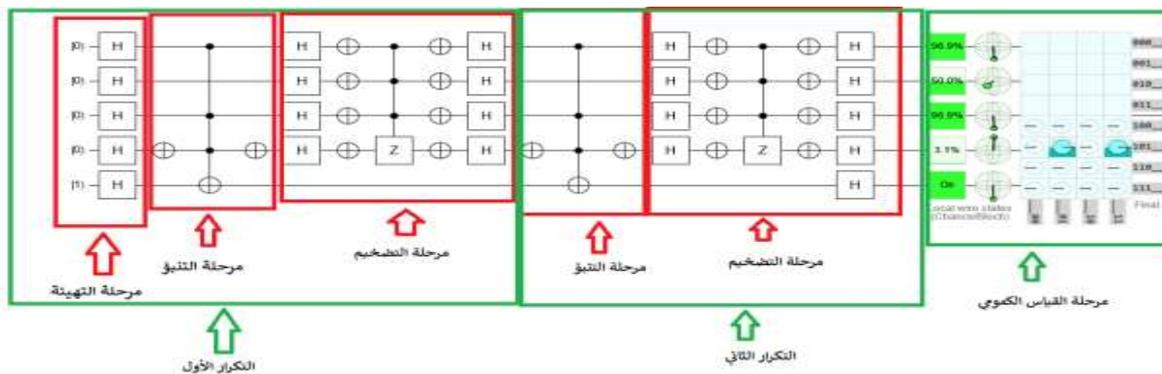
الشكل(27): تنفيذ خوارزمية كروفر للبحث عن العنصر 0101 بطريقة التنبؤ الثنائي.



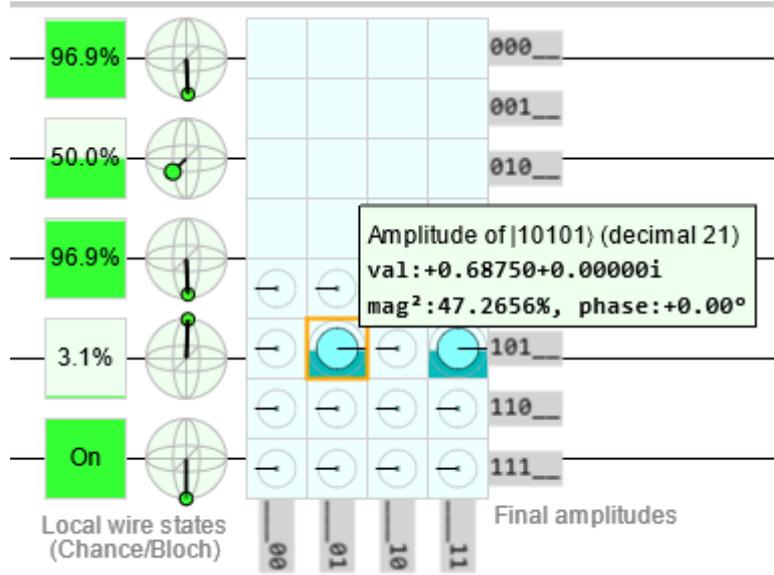
الشكل(28): مرحلة القياس الكمومي للدارة كروفر للبحث عن العنصر 0101 بطريقة التنبؤ الثنائي.

4-5-2 البحث عن حلين بطريقة التنبؤ الثنائي

عند البحث عن حلين فإننا نحتاج إلى تكرارين للوصول إلى الحل النهائي، يمثل الشكل(29) الدارة الكمومية للبحث عن العنصرين 1010,1110 بطريقة التنبؤ الثنائي حيث طبقنا تكرارين للوصول للنتيجة ومراحل الخوارزمية موضحة في الشكل وكانت احتمالية كل من الحالتين الصحيحتين الناتجتين 47.26% كما هو موضح في الشكل (30).



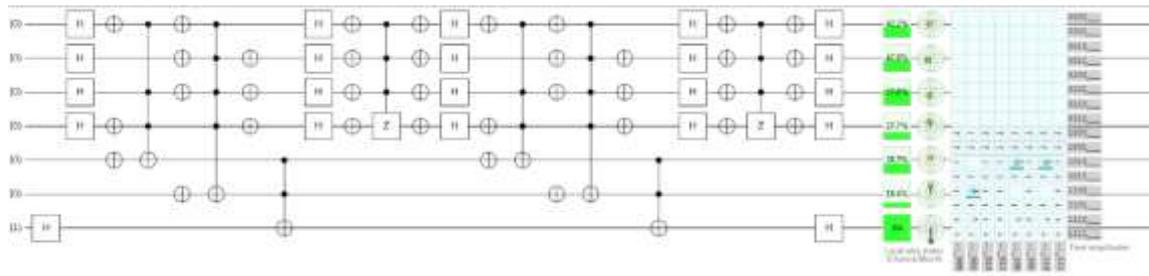
الشكل(29): تنفيذ خوارزمية كروفر للبحث عن العنصرين 1010,1110 بطريقة التنبؤ الثنائي.



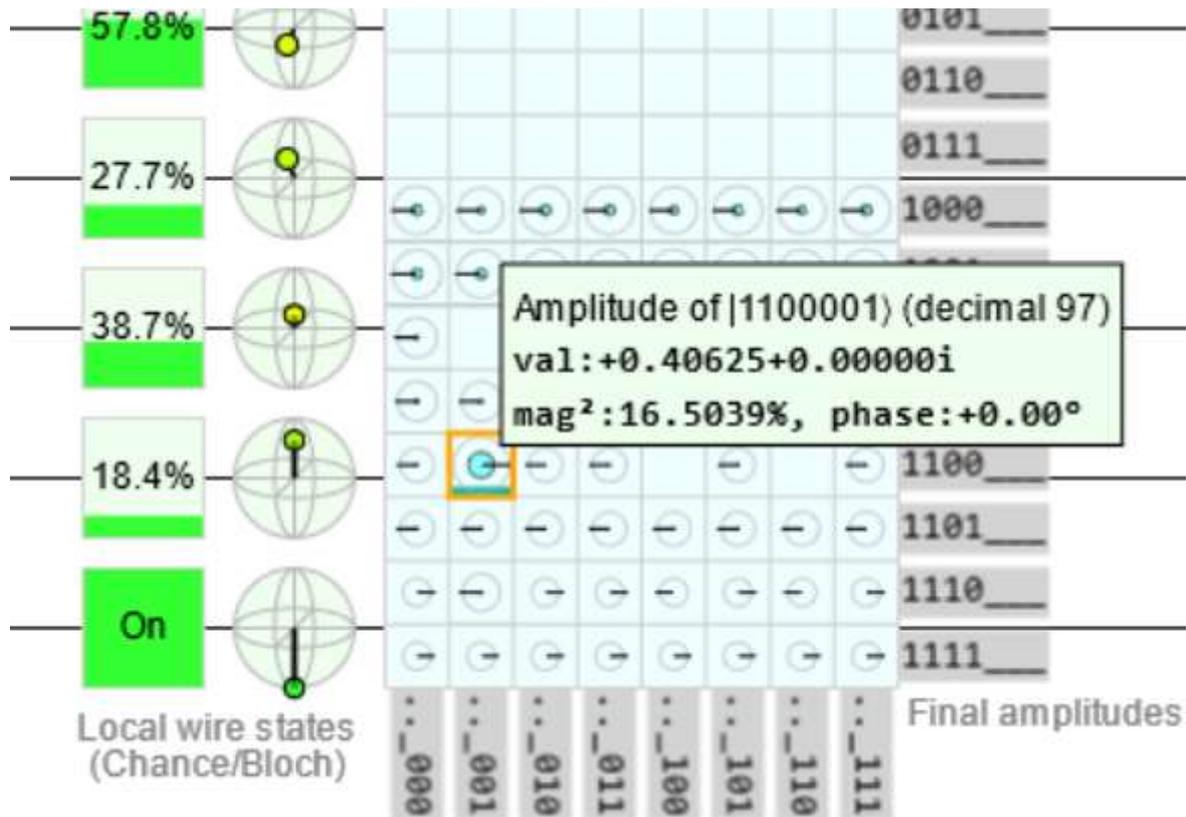
الشكل(30): مرحلة القياس الكمومي للدارة كروفر للبحث عن العنصر 0101 بطريقة التنبؤ الثنائي.

4-5-3 البحث عن ثلاثة حلول بطريقة التنبؤ الثنائي

عند البحث عن ثلاثة حلول فإننا نحتاج أيضاً إلى تكرارين للوصول إلى الحل النهائي، يمثل الشكل(31) الدارة الكمومية للبحث عن العناصر 0110,0010,1000 بطريقة التنبؤ الثنائي حيث تم استبدال كل مرحلة من مراحل الخوارزمية بالدارة الكمومية الموافقة(مرحلة التنبؤ بتغيير حسب الحلول التي نريد البحث عنها أما مرحلتي التنبؤ والتضخيم فلهما تصميم ثابت لا يتغير بتغيير الحل) وتم تطبيق تكرارين للوصول للنتيجة واحتمالية كل من الحلول الصحيحة 16.5%، واحتمالية كل من الحلول الخاطئة 0.39% حيث يوضح الشكل (32) مرحلة القياس الكمومي لهذه الدارة



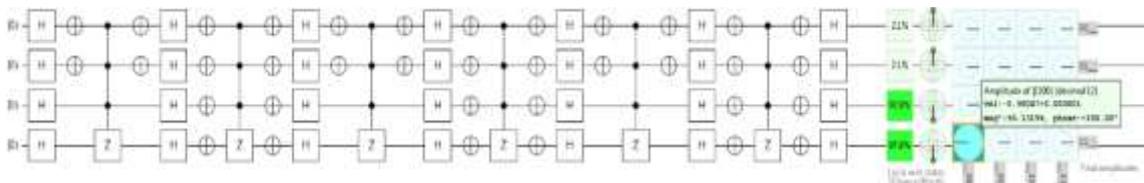
الشكل(31): تنفيذ خوارزمية كروفر للبحث عن العناصر 0010,0110,1000 بطريقة التنبؤ الثنائي.



الشكل(32): مرحلة القياس الكمومي للدارة كروفر للبحث عن العناصر 0010,0110,1000 بطريقة التنبؤ الثنائي.

4-5-4 البحث عن حل وحيد باستخدام طريقة التنبؤ بقلب الصفحة

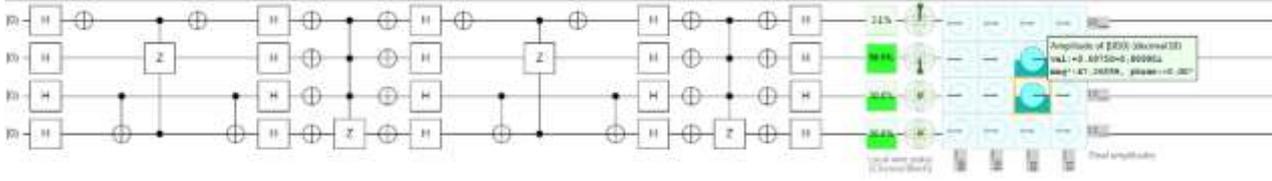
عند البحث عن حل وحيد فإننا نحتاج إلى ثلاث تكرارات للوصول إلى النتيجة، يمثل الشكل(33) الدارة الكمومية للبحث عن العنصر 0011 بطريقة التنبؤ بقلب الصفحة حيث طبقنا ثلاث تكرارات للوصول للنتيجة واحتمالية الحالة الصحيحة %96.13.



الشكل(33): تنفيذ خوارزمية كروفر للبحث عن العنصر 0011 بطريقة التنبؤ بقلب الصفحة.

4-5-5 البحث عن حلين بطريقة التنبؤ بقلب الصفحة

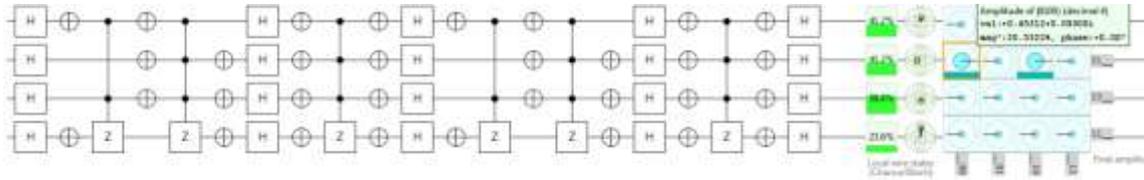
عند البحث عن حلين فإننا نحتاج إلى تكرارين للوصول إلى الحل النهائي، يمثل الشكل(34) الدارة الكمومية للبحث عن العنصرين 0101,0110 بطريقة التنبؤ بقلب الصفحة حيث طبقنا تكرارين للوصول للنتيجة واحتمالية كل من الحالتين الصحيحتين %47.26.



الشكل (34): تنفيذ خوارزمية كروفرف للبحث عن العنصرين 0101,0110 بطريقة التنبؤ بقلب الصفحة.

4-5-6 البحث عن ثلاثة حلول بطريقة التنبؤ بقلب الصفحة

عند البحث عن ثلاثة حلول فإننا نحتاج أيضاً إلى تكرارين للوصول إلى الحل النهائي، يمثل الشكل (35) الدارة الكمومية للبحث عن العناصر 1000,0110,0010 بطريقة التنبؤ بقلب الصفحة حيث طبقنا تكرارين للوصول للنتيجة واحتمالية كل من الحلول الصحيحة 20.53%، واحتمالية كل من الحلول الخاطئة 2.95%.



الشكل (35): تنفيذ خوارزمية كروفرف للبحث عن العناصر 1000,0110,0010 بطريقة التنبؤ الثاني.

5- الاستنتاجات والتوصيات:

تناولنا في سياق هذا البحث تشكيل توابع التنبؤ الكمومية انطلاقاً من جداول الحقيقة الكمومية وبناء دارات التنبؤ الكمومي الموافقة و توصلنا إلى أنه وبشكل مشابه للحوسبة التقليدية يمكن اختزال توابع التنبؤ الكمومي لتخفيض عدد البوابات الكمومية وعدد المداخل والمخارج المطلوبة.

وبالمقارنة مع الدراسة [7] تبدو الطريقة التي اعتمدها في استنتاج توابع التنبؤ الكمومية من جداول الحقيقة أكثر مرونة إذ يمكن أتمتة عملية تشكيل دارات التنبؤ وفق المنهجية والملاحظات المقترحة و لا حاجة لاستنتاج جميع الحالات المحتملة التي ستتضاعف مع ازدياد عدد الحلول أو حجم فضاء البحث. على سبيل المثال يمكن تلخيص الكود الوهمي (pseudocode) لدارة التنبؤ الكمومي بطريقة التنبؤ بقلب الصفحة للبحث عن حل وحيد بالخطوات التالية:

1. إضافة بوابة عكس على كل بت يفترض أن تكون قيمته في الحالة التي نبحث عنها 0
2. تطبيق بوابة controlled-controlled-Z ب n بت كمومي على خرج المرحلة السابقة حيث البت المتحكم به هو بت التنبؤ والبيانات المتحكم بها هي بقية البتات الممثلة لفضاء البحث.
3. إضافة بوابة عكس على كل بت تم تطبيق بوابة العكس عليه في المرحلة 1 من أجل إعادته إلى الحالة الابتدائية.

أيضاً بالمقارنة مع الدراسة [8] فإنها لم تتناول تمثيل التوابع الأساسية أو المختصرة باستخدام الوظائف الأساسية الممثلة باستخدام البوابات الكمومية، حيث اعتمدت الدراسة بشكل أساسي على تجزئة بوابة توفولي بأربع وخمس بيئات

إلى بوابات جزئية S,H,T,T⁺ ومن ثم اختصار البوابات الجزئية معاً. ومن المفيد مستقبلاً دمج نتائج الدراستين بحيث نحصل على اختزال مضاعف لدارات التنبؤ الكومومي.

بالمقارنة مع الدراسة [9] التي قدمت فكرة هامة وهي تمثيل قواعد البيانات غير البنيوية باستخدام متنبئات (oracles) بحيث يمكن لخوارزمية كروفر أن تبحث في قاعدة البيانات هذه بشكل مباشر. لكن الطريقة التي قدمتها لتمثيل قاعدة البيانات تضمنت تعقيداً كبيراً جعلت الخوارزمية أكثر تعقيداً من خوارزمية البحث التقليدي وبالتالي ألغت الميزة الأساسية لخوارزمية كروفر وقد أوصى كاتب المقالة بمحاولة حل مشكلة التعقيد بالاعتماد على تقنيات الذكاء الاصطناعي وغيرها من التقنيات.

بالنسبة لخوارزمتنا وحيث الدارة الكومومية لخوارزمية كروفر ذات تشكيل ثابت تماماً وما يتغير فقط هو مرحلة التنبؤ وعلى اعتبار أن كل عملية لاستنتاج مرحلة التنبؤ تستغرق وحدة زمنية أي يستغرق استنتاج مرحلة التنبؤ بطريقة قلب الصفحة ثلاث وحدات زمنية أي التعقيد $O(3\sqrt{N})$ وهو تعقيد أقل من تعقيد خوارزمية البحث التقليدي عندما حجم فضاء البحث أكبر من 81 (عدد البيئات 9) وأقل من خوارزمية البحث الثنائي عندما حجم فضاء البحث أكبر من 1296 (عدد البيئات 36). أي أن استخدامها فعال من أجل قواعد البيانات الضخمة.

من الملاحظ أن طريقة التنبؤ بقلب الصفحة تحتاج عدد بيئات أقل من البيئات في حالة التنبؤ الثنائي، حيث يمكن تمثيل التابع باستخدام عدد البيئات المطلوبة لتمثيل فضاء البحث فقط، وهذا مفيد جداً عند وجود قيود عتادية (عدد بيئات كومومية محدود للحاسب الكمي).

تتجلى أهمية إيجاد منهجية لاستنتاج توابع التنبؤ في إطفاء مرونة وسرعة على تنفيذ الخوارزميات الكومومية، فعلى سبيل المثال يتطلب تنفيذ خوارزمية كروفر إعادة تشكيل دارة التنبؤ الكومومي في كل مرة تتغير فيه القيمة أو القيم التي نبحث عنها ولكن وبالاستفادة من المنهجية المقترحة سواء للتنبؤ الثنائي أو التنبؤ بقلب الصفحة سيصبح من الممكن أتمتة عملية تشكيل دارات التنبؤ مما يجعل تنفيذ مثل هذه الخوارزميات الكومومية على الحواسيب الكومومية المنتجة حالياً أقرب إلى التطبيق والواقع

إن طريقة استنتاج مرحلة التنبؤ الكومومي سواء الثنائي أو قلب الصفحة من دون عملية اختزال بسيطة ويمكن تحويلها إلى خوارزمية وتمثيلها برمجياً بسهولة ولكنها تتطلب عدداً كبيراً من البوابات بالمقارنة مع الطريقة المختزلة التي يبدو تمثيلها برمجياً أكثر تشعباً وتعقيداً

فيما يتعلق بنتائج تنفيذ خوارزمية كروفر نلاحظ ما يلي:

- تتخفف عدد التكرارات التي تحتاجها الخوارزمية مع ازدياد عدد الحلول التي نبحث عنها، وتتنقص احتمالية كل من الحلول الصحيحة أيضاً حيث يجري توزيع الاحتمالية الكلية على هذه الحلول، وإن انخفاض الاحتمالية يشكل ثغرة بالنسبة للخوارزمية إذ يجعل عملية القياس الكومومي أصعب وتتطلب عدداً أكبر من العينات، وبالتالي فإن خوارزمية كروفر مثالية بالنسبة للتطبيقات التي تتطلب البحث عن قيمة واحدة أو عدد محدود من القيم كما في تطبيقات كسر خوارزميات التشفير.

تتضمن التوصيات بالنسبة للدراسات المستقبلية ما يلي:

- العمل على بناء خوارزمتين وتمثيلهما برمجياً من أجل استخلاص دارات التنبؤ الكومومي بنوعيه بشكل مؤتمت وذلك اعتماداً على المنهجية والملاحظات المستنتجة في سياق هذا البحث.

-6 المراجع

- [1] CHUANG,I,L;NIELSEN,M,A.2010,*Quantum Computation and Quantum Information*.10th Anniversary Edition,Cambridge University Press,U.K,710.
- [2] Cacciapuoti,A;Caleffi,M;METER,R;HANZO,L.2020,When Entanglement meets Classical Communication:Quantum Teleportation for Quantum Internet.IEEE Transaction on Communication.
- [3] GROVER,L.1996,A fast quantum mechanical for database search.Proceedings of the twenty-eighty annual ACM symposium on Theory of Computing.U.S.A,212-219.
- [4] COLLINS;D;KIM,K,A;HOLTOM,W,C.1998,Deutsch-Joza algorithm as a test of quantum computation,Physical Review,Vol.58,No.3.
- [5] BEHERA,B;PANIGRAHI,P.2018,Solving Linear Systems of Equations by Gaussian Elimination Method Using Grover's Search Algorithm:An IBM Experience. <https://arxiv.org/pdf/quant-ph/9807012>.
- [6] JU,Y;TSAI,I;KUO,S.2007,Quantum Circuit Design and Analysis for Database Search Application,IEEE TRANSACTION ON CIRCUITS AND SYSTEMS,Vol.54,No.11,2552-2563.
- [7] VATHSAN,R.2015,Introduction to Quantum Physics and information processing.CRC Press,France.268.
- [8] MUTIARA,A;REFIANTI,R.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.
- [9] SEIDEL,R;BECKER,C.2023,Automatic generation of Grover quantum oracles for arbitrary data structures.Quantum Science and technology,Vol.8,No.2, 025003.
- [10] <https://algassert.com/quirk>.
- [11] FIGGAT,C;MASLOV,D;LANDSMAN,K.A;LINKE,N.M;DEBNATH,S;MONROE,C.2017,Complete 3-Qubit Grover search on a programmable quantum computer,Nature Communication,USA,Vol.8,No.1,1-9.
- [12] POLAK,W,H;RIEFFEL,E,G.2011,Quantum Mechanics,springer International publishing,Germany.349.
- [13] BAE,J-H;ALSING,P;AHN,D;MILLER,W.2020,Quantum circuit optimization using quantum karnaugh map.scientific reports,Vol.10,No.1,1-8.
- [14]] ZETTILLI,N,Quantum Mechanics"Cocepts and Application".Second Edition,A John Wiley and Sons Publication,U.S.A.690.+
- [15] خوارزمية كمومية لحل مشاكل البحث في فضاءات البحث غير , غانم،يانا،:البستاني، حسن[15] البنيوية ، مجلة جامعة تشرين للبحوث والدراسات العلمية.المجلد.41، العدد5.