هل نقترب أكثر من الوصول إلى الحوسبة الكمومية؟

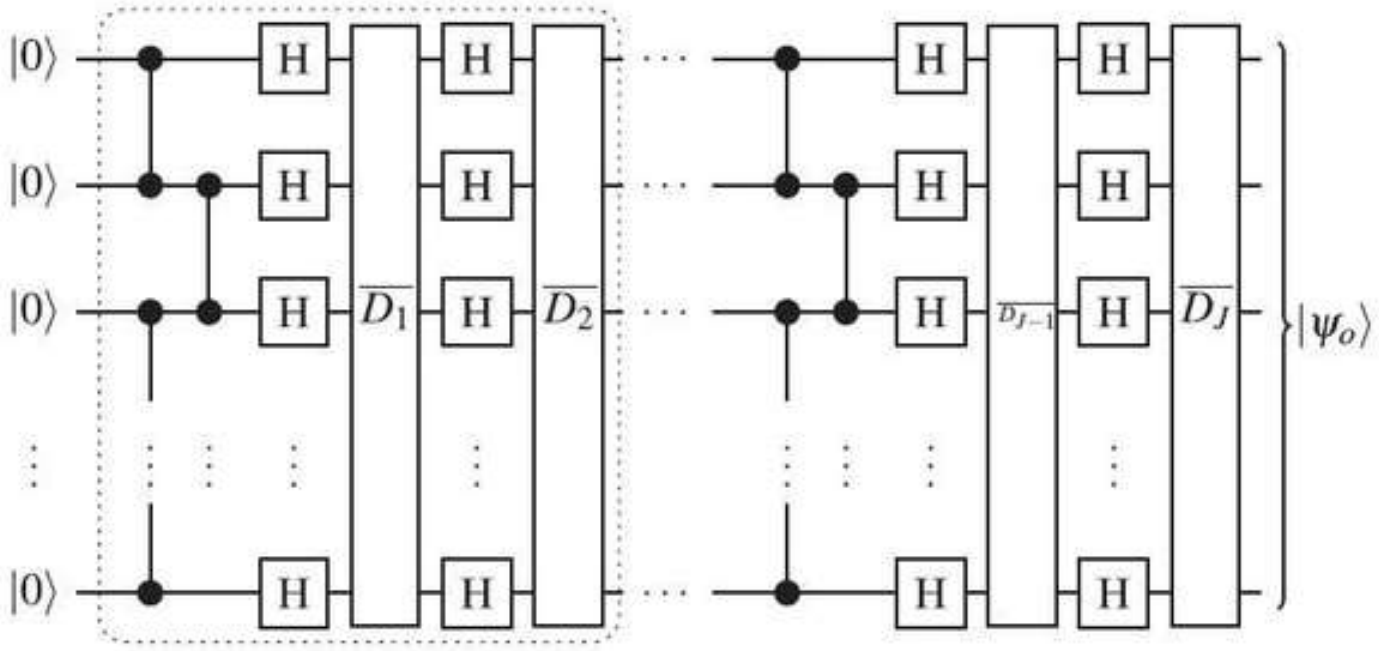


الحوسبة الكمومية العمياء تتجاوز قيد الفعالية

مبرهنة على أن الحدود وُضعت لتُحطم، تغلبت مجموعة من علماء الفيزياء على ما عُرف سابقاً بأنه حد عالمي أو طبيعي على فعالية مهمة التشفير الكمومية المعروفة بالحوسبة الكمومية العمياء (**blind quantum computing**)، وتُقدم الطريقة الجديدة تحسينات معتبرة وفعّالة، وفي بعض الأحيان تتطلب لتطبيقها مصادر اتصال أقل بشكلٍ أسي مقارنةً مع الطرق السابقة.

نشر الفيزيائيان كارلوس بيريز-ديلغادو **Carlos A. Pérez-Delgado** وجوزيف فيتزسيمونز **Joseph F. Fitzsimons** من جامعة

سنغافورة للتكنولوجيا والتصميم، ورقةً علمية تشرح كيفية تحسين طريقة الحوسبة الكمومية العمياء في العدد الحالي من مجلة **Physical Review Letters**، ويعمل فيتزسيمونز أيضاً مع مركز التقنيات الكمومية في الجامعة الوطنية في سنغافورة.



تُوضح المربعات ذات الخطوط المنقطة نمط التكرار للعمليات. Credit: Pérez-Delgado and Fitzsimons. ©2015 American Physical Society

وكما يبين اسمها، يُجري الحاسب عند تطبيق الحوسبة الكمومية العمياء، المهمة بشكلٍ أعمى، أي أن المدخلات وعملية الحوسبة والمخرجات تبقى جميعها مجهولة بالنسبة للحاسب، ويقول العلماء أن هذه القدرة: "تسمح للمستخدم بتوكيل الحساب إلى خادم غير موثوق، وفي الوقت نفسه الحفاظ على الحساب مخفي"، وباستمرار تطور هذه التكنولوجيا، فإنه من المتوقع أن تُقدم درجة أمان أكبر بكثير مقارنةً بالبروتوكولات الكلاسيكية بالنسبة لمجالٍ متنوع من التطبيقات.

على النقيض من كل مهام الحساب، تتطلب الحوسبة الكمومية العمياء عدداً أصغرياً من البتّات الكمومية (**qubits**)، والبوابات، ومصادر اتصال أخرى، من أجل إجراء عملية الحساب. وتقترح الأبحاث الحالية وجود قيد أصغري طبيعي على متطلبات الاتصالات تلك، ويعتمد ذلك القيد على ما يُعرف بنظرية اللابرمجة **no-programming theorem**.

ولأن هذا الحد الأدنى يقترح أن برتوكولات الحوسبة الكمومية العمياء ستتطلب دوماً كمية صُغرى محددة من المصادر، فإنه يُحد وبشكلٍ فعال من مردود إجراء تلك البروتوكولات.

نقلُ تصحيح الأخطاء

في الورقة العلمية الجديدة، برهن علماء الفيزياء على أن هذا القيد يصمد في سيناريوهات محددة فقط، ويُمكن التغلب عليه عبر استخدام تقنية تُعرف بـنقل البوابات المكرر (**iterated gate teleportation**).

تعتمد هذه التقنية على النقل القياسي للبوابات، الذي تنتقل فيه الحالات الكمومية (**quantum states**) بسرعة كبيرة من بوابة إلى أخرى عبر الاستفادة من التشابك الكمومي (**quantum entanglement**) بين البوابات، وفي النسخة التكرارية، تتم خطوات نقل بوابات إضافية بشكلٍ متكرر لتصحيح الأخطاء بالاعتماد على نتائج خطوات النقل السابقة.

يقول فيتزسيمونز لـ**Phys.org**: "إن الجزء الأهم في عملية نقل البوابات هو تقديمها طريقة لإجراء الحساب المرغوب به على نصف الحالة المتشابكة قبل أن تتم معرفة المُدخلات المرغوبة، مما يؤدي إلى إنتاج حالة مصدر خاصة".

ويتابع: "حالما تحصل على المدخلات، يُمكنك إجراء مجموعة خاصة من القياسات بين المدخلات وحالة المصدر، وبالنسبة لإحدى عمليات المخرجات المحتملة للقياسات، يكمن التأثير في تطبيق الحساب المُشفر على المدخلات المختارة. على أية حال، من المستحيل التحكم بمخرجات القياس الذي ستحصل عليه، وأي نتائج أخرى ينتج عنها خطأ غير مرغوب به ويحتاج إلى التصحيح. يستخدم برتوكول النقل التكراري الانتقالات لتصحيح الأخطاء الناجمة عن خطوات النقل السابقة بطريقة تقل معها الأخطاء في كل جولة لتختفي في النهاية".

برهن علماء الفيزياء على إمكانية قيام بضع خطوات نقل إضافية بتصحيح الأخطاء، التي سيجري تصحيحها في أحوالٍ أخرى باستخدام عدد أكبر من المصادر. بهذه الطريقة، تُخفض التقنية متطلبات الاتصال أسياً، ليصل ذلك التخفيض إلى أقل من القيمة الصغرى التي تفرضها نظرية اللابرمجة.

يقول فيتزسيمونز: "بالنسبة لي على الأقل، إنها نتيجة مفاجئة جداً لأنه تم في السابق الإثبات أن الحوسبة الحتمية، فإن البرامج المشفرة باستخدام الحالات الكمومية ليست أقصر من تلك التي تستخدم البتات الكلاسيكية".

ويُضيف: "لتوكيل حساب ما، من الطبيعي أن تفكر أنه من الضروري وصف البرنامج الذي سيجري تطبيقه، وبالتالي الاتصال اللازم سيكون من رتبة حجم البرنامج. على أية حال، تبيّن أن ذلك لا يُعبر عن الحالة، يستوعب بروتوكولنا هذا القيد عبر تشفير عدد كبير من البوابات في كل حالة كمومية، وبعد ذلك يتم إجراء تصحيح تكيفي لأية أخطاء ناجمة عن النقل. إذا أردت التفكير بالأمر بدلالة البرنامج، على البرنامج حينها أن يحتوي حالات كمومية لكل نتيجة قياس محتمله، مما ينتج عنه زيادة أسية، وهذا الأمر يُفسر لماذا لا يُوجد توتر بين نتيجتنا ونظرية اللابرمجة. ببساطة، يقرأ البرتوكول الخاص بنا قسماً صغيراً فقط من البرنامج الكامل على الرغم من أن هذا القسم لا يُمكن تحديده مسبقاً".

مستقبل الحوسبة الكمومية العمياء

يعتقد الفيزيائيون أن نهج نقل البوابات التكراري ربما يُمكن تطبيقه على مهام حساب غير الحوسبة الكمومية العمياء، مما يُقدم تحسينات فعالة في هذه المجالات أيضاً.

يقول فيتزسيمونز: "كي توسع من برتوكولات الحوسبة الكمومية العمياء، من المحتمل إضافة اختبارات تؤكد أنه تمّ إنجاز الحساب المرغوب به بشكلٍ صحيح، وهذا الأمر ليس بالشيء العملي جداً في هذه المرحلة؛ لأنه إذا ما أردنا أن يكون مفيداً حقاً، نحتاج في البداية إلى وجود حواسب كمومية كبيرة نسبياً. وحتى يومنا هذا، تم التحقق من صحة الحوسبة الكمومية العمياء والتي يُمكن اختبار صحتها عبر الإثباتات التجريبية باستخدام أنظمة رباعية البتات الكمومية (**our-qubit systems**)".

ويتابع: "لكن مع التطور المستمر للتكنولوجيا، نتوقع أن أهمية البرامج العاملة بشكلٍ آمن على خوادم كمومية بعيدة ستزداد أهميتها دوماً، تماماً كما ظهرت الحوسبة السحابية (**cloud computing**) في العالم التقليدي. تكمن أفضلية الحوسبة الكمومية العمياء والبرتوكولات

المُتحقق من صحتها في أنها تُقدم نوعاً من الأمان، وهو ببساطة غير متاح باستخدام البرتوكولات التقليدية".

في المستقبل، يُخطط الباحثون لتطوير برتوكولات الحوسبة الكمومية العمياء لاستخدامها في تطبيقات التشفير الجديدة، ويُعلق فيتزسيمونز قائلاً: "أصبح تعبير التشفير الكمومي (**quantum cryptography**) مرادفاً للتوزع الكمومي للمفاتيح (**quantum key distribution**). على الرغم من أن مجموعتي تعمل في العديد من مجالات البحث المتنوعة، إلا أنها تمتلك شيئاً مشتركاً بينها، هو إيجاد برتوكولات كمومية جديدة للاستخدام في مهام التشفير الكمومي ولا ترتبط بتوزع المفاتيح. تُثبت الحوسبة الوكيلة أنها مصدرٌ عظيم لمسائل التشفير الجديدة، ولذلك تتركز العديد من جهودنا في تلك المنطقة. قد يكون السؤال الأكثر أهمية بالنسبة لنا هو معرفة فيما إذا كان هناك برتوكولات حوسبة كمومية عمياء لا تتطلب أي اتصال كمومي أو تشابك بين الأجزاء. أنا ممتنٌ كثيراً لمؤسسة الأبحاث الوطنية التي تدعم بسخاء بحثنا في هذا المجال".

- التاريخ: 2015-08-05
- التصنيف: فيزياء

#التشابك الكمومي #الحوسبة الكمومية #نظرية اللابرمجة #الحوسبة الكمومية العمياء #الحوسبة السحابية

المصطلحات

- **التشابك الكمومي (quantum entanglement)**: التشابك الكمومي: ظاهرة كَمّية ترتبط فيها الجسيمات الكميّة ببعضها، رغم وجود مسافات كبيرة تفصل بينها. مما يقود إلى ارتباطات في الخواص الفيزيائية المقيسة لهذه الجسيمات الكمّية. المصدر: العلوم الأمريكية.
- **الحَوْسَبَة السحابيّة (Cloud computing)**: هي مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تُبَسِّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية. المصدر: ويكيبيديا
- **البت الكمومي (الكيوبت) (qubit)**: هو أصغر وحدة معلومات كمية، وهو الذي يقابل البت في الحواسيب العادية، ويستعمل في حقل الحوسبة الكمية.

المصادر

- phys.org
- الورقة العلمية
- الصورة

المساهمون

- ترجمة
  - همام بيطار
- مُراجعة
  - أسماء مساد
- تحرير

- آلاء محمد حيمور
- نور المصري

- تصميم
  - Tareq Halaby
- نشر
  - مي الشاهد