كيف تُحمى الاتصالات الهامة من التجسس باستخدام فيزياء الكم؟

ما كان يستغرق شهوراً من العمل المتواصل من قِبل علماء عالميين مختصين، أصبح من الممكن أن ينجزه طلاب جامعيين في ثوان. يعود الفضل في ذلك لبرنامج جديد طُور في مختبر الحوسبة الكموميّة **IQC** التابع لجامعة واترلو **University of Waterloo** والذي مهّد الطريق نحو اتصال كمّي سريع وآمن.

يعمل الباحثون على تطوير أول برنامج متاح لتقييم درجة الأمان لأي بروتوكول مستخدم في عمليّة "نشر المفتاح الكمّي" **Quantum Key Distribution**، أو اختصارًا **QKD**.

يسمح **QKD** لطرفين ـأليس وبوب، على سبيل المثالـ بإنشاء مفتاح سري مشترك من خلال تبادل الفوتونات، حيث تتصرف الفوتونات وفقاً لقوانين ميكانيكا الكم. ينص القانون على أنّه ليس من الممكن قياس شيء كمي دون إدخال اضطراب عليه. لذا، فإذا اعترض متنصت ما، إيف مثلاً، وأجرى عملية قياس على الفوتونات، فإنّها سوف تسبّب اضطراباً بوسع أليس وبوب الكشف عنه. من ناحية أخرى، إذا لم يكن هنالك أي اضطراب، فسيتمكن أليس وبوب من ضمان أمان المفتاح المشترك بينهما.

من الناحية العملية، يؤدي الفقدان والتشويش في التنفيذ دائماً إلى بعض الاضطرابات، إلّا أنّ وجود كمية صغيرة من الاضطراب يعني أنّ كمية صغيرة من المعلومات حول المفتاح متاحة لإيف (المتنصّت). إنّ تمييز هذه الكمية من المعلومات يسمح لإليس وبوب بحذف هذه المعلومات من عند إيف، بتكلفة تساوي طول المفتاح النهائي الناتج عن ذلك. المشكلة النظرية الرئيسية في **QKD**، هي كيفية حساب الطول المسموح لهذا المفتاح السري النهائي، من أجل أي بروتوكول، وكذلك حساب الاضطراب الملاحظ تجريبياً.

لا تزال هناك حاجة إلى منهج رياضي لاجراء هذا الحساب الصعب. وقد اختار الباحثون تبني المنهج العددي، ولأسباب عملية، حولوا مسألة حساب معدّل المفتاح إلى "مسألة الحل الأمثل المزدوجة" **dual optimization problem**.

قال "باتريك كولز" **Patrick Coles**، وهو طالب دراسات ما بعد الدكتوراه في **IQC**: "أردنا تطوير برنامج معيّن من شأنه أن يكون سريعاً وسهل الاستخدام، بالاضافة إلى قابليته للعمل مع أي بروتوكول". ويتابع قائلاً: "لقد خفضت مسألة الحل الأمثل المزدوجة كثيرا من عدد المعاملات، إذ يقوم الحاسوب بعمل كل شيء".

نُشرت الورقة العلمية، وعنوانها "النهج العددي لنشر مفتاح الكم غير المنتظم"**Numerical approach for unstructured quantum key distribution**، في مجلة **Nature Communications**، وقد قدمت ثلاثة نتائج. أولاً، اختبر الباحثون البرنامج مع النتائج السابقة لبروتوكولات مدروسة ومعروفة، وكانت نتائجهم صحيحة بشكل مرض. وبعد ذلك، درسوا بروتوكولات لم تُدرس من قبل. وأخيراً، وضعوا إطار عمل لإعلام المستخدمين بكيفية إدخال البيانات باستخدام بروتوكول جديد في البرنامج.

وقد أشار "نوربرت لوتكنهاوس" **Norbert Lütkenhaus**،وهو بروفيسور في **IQC** وقسم الفيزياء والفلك في جامعة واترلو، إلى أن: "عمليّة تحري بروتوكولات **QKD** ركّزت إلى الآن على البروتوكولات التي تتبنى طرقاً معينة لأداء تحليل الأمن. والعمل الذي أنجزته مجموعتنا يسمح لنا بتحري بروتوكولات تتكيف مع القدرات التكنولوجية".

- التاريخ: 2016-08-26
- التصنيف: تكنولوجيا

#الاتصالات #الحوسبة الكمومية #فيزياء الكم

المصطلحات

- **الأمثلة (optimization)**: هي اختيار العنصر الأفضل، بالنسبة لمعيارٍ معين، من مجموعة من البدائل المحتملة.
- **الأيونات أو الشوارد (Ions)**: الأيون أو الشاردة هو عبارة عن ذرة تم تجريدها من الكترون أو أكثر، مما يُعطيها شحنة موجبة.وتسمى أيوناً موجباً، وقد تكون ذرة اكتسبت الكتروناً أو أكثر فتصبح ذات شحنة سالبة وتسمى أيوناً سالباً

المصادر

- science daily
- الصورة

المساهمون

- ترجمة
  - أمجد هواش
- مُراجعة
  - محمد اسماعيل باشا
- تحرير
  - أنس الهود
  - بنان محمود جوابره
- تصميم
  - علي كاظم
- نشر
  - سارة الراوي