الفيزيائي نيكولاس بوليدو يقف أمام نموذج أولي لجهاز كمبيوتر كمي في برونزويك بألمانيا.

الحوسبة الكمية: الفرص والمخاطر

يمكن لأجهزة الكمبيوتر الكمية فك التشفير الذي يدعم الاستقرار المالي

خوسيه ديودورو، ومايكل غوريانيوف، وماجد ملائكة، وتحسين سعدي صديق

كان الجنود في اليونان القديمة يبعثون رسائل سرية عن طريق لف شريط من الجلد الرقيق حول عصا والكتابة عليه. ولا يمكن فك شفرة رسائلهم إلا عن طريق شخص معه عصا لها نفس السُّمْك. إنه أحد أقدم الأمثلة على التشفير. أما أسرار اليوم، مثل الاتصالات عبر الإنترنت والصيرفة الرقمية والتجارة الإلكترونية، فتتم حمايتها من أعين المتطفلين عن طريق خوارزميات حاسوبية قوية. ومع ذلك فإن هذه الرموز التشفيرية التي لا يمكن اختراقها حتى الآن يمكن أن تصبح جزءا من التاريخ عما قريب.

ويمكن لأجهزة الكمبيوتر الكمية أن تصل إلى مستوى من التحسين من شأنه فك العديد من مفاتيح التشفير الحالية في وقت أقل مما يحتاجه إنشاؤها باستخدام أجهزة الكمبيوتر الرقمية التقليدية. وينبغي للمؤسسات المالية أن تعمل دون تأخير على حماية نظم الأمن السيبراني الخاصة بها من التقادم في المستقبل، وإلا سيتعرض الاستقرار المالي للخطر.

ثورة كمية

الحوسبة الكمية هي استخدام الظواهر الكمية مثل التراكب والتشابك لإجراء العمليات الحسابية. والوحدة الأساسية لجهاز الكمبيوتر الكمي هي البت الكمي (أو اختصارا الكيوبت) التي تستمد إمكاناتها عادة من خلال الخصائص الكمية للجسيمات دون الذرية، مثل دوران الإلكترونات أو استقطاب الفوتون. وفي حين أن كل بت ثنائي مستخدم في أجهزة الكمبيوتر الرقمية اليوم يمثل قيمة الصفر أو الواحد

تفوق أجهزة الكمبيوتر الكمية نظيراتها الرقمية التي تتبع قوانين الفيزياء التقليدية من حيث قدرتها الهائلة على معالجة البيانات.

الصحيح، فإن الكيوبتات تمثل كلا من الصفر والواحد الصحيح (أو مزيجا من الاثنين) في نفس الوقت. وهذه الظاهرة تسمى التراكب. أما التشابك الكمي فهو ارتباط خاص بين أزواج أو مجموعات من العناصر الكمية. ويؤثر تغير حالة أحد العناصر على العناصر المتشابكة الأخرى على الفور – بغض النظر عن المسافة بينها.

وتؤدي زيادة عدد الكيوبتات إلى زيادة أسية في سرعة معالجة العملية الحسابية. وهناك حاجة إلى اثنين من البتات الثنائية التقليدية لمضاهاة قوة كيوبت واحد؛ وإلى أربعة بتات لمضاهاة اثنين من الكيوبتات؛ وإلى ثمانية بتات لمضاهاة ثلاثة كيوبتات؛ وهكذا. وهناك حاجة إلى حوالي ١٨ كوادريليون بت من الذاكرة التقليدية لتصميم نموذج لجهاز كمبيوتر كمي يستخدم ٥٤ كيوبت فقط. ويحتاج جهاز كمبيوتر كمي يستخدم ١٠٠ كيوبت عددا من البتات يفوق عدد الذرات الموجودة على سطح الكرة الأرضية. ويحتاج جهاز كمبيوتر يستخدم ٢٨٠ كيوبت عددا من البتات يفوق عدد الذرات الموجودة في الكون المعروف.

وتفوق أجهزة الكمبيوتر الكمية نظيراتها الرقمية التي تتبع قوانين الفيزياء التقليدية من حيث قدرتها الهائلة على معالجة البيانات. فقد شبه ويليام فيليبس، الفيزيائي الحائز على جائزة نوبل، القفزة من تكنولوجيا اليوم إلى تكنولوجيا الكم بالقفزة من العدَّاد اليدوي إلى جهاز الكمبيوتر الرقمي نفسه. وحتى وقت قريب، كانت هذه الميزة التي تسمى الميزة الكمية أو «التفوق الكمي» مجرد نظرية. لكن في عام ٢٠١٩، استخدمت شركة غوغل جهاز كمبيوتر كميا لأداء مهمة حسابية محددة في ٢٠٠ ثانية فقط. وقالت الشركة إن المهمة نفسها كانت ستستغرق في ذلك الوقت ١٠ آلاف سنة باستخدام أقوى جهاز كمبيوتر رقمي فائق السرعة.

الفرص المتاحة

إن المهام الحسابية المعقدة تشبه إيجاد المَخْرَج من متاهة. فالكمبيوتر التقليدي سيحاول الهروب باتباع كل المسارات بصورة متسلسلة إلى أن يصل إلى المَخْرَج. وفي المقابل، يسمح التراكب للكمبيوتر الكمي بتجربة جميع المسارات في آن واحد. ويؤدي ذلك إلى خفض كبير في الزمن اللازم لإيجاد حل.

ومن خلال حل المسائل بدقة وسرعة أكبر مقارنة بأجهزة الكمبيوتر الرقمية، فإن أجهزة الكمبيوتر الكمية يمكنها تعجيل الاكتشافات والابتكارات العلمية، وإحداث ثورة في نماذج وعمليات محاكاة الأسواق المالية، والمساعدة على تعلُّم الآلة واستخدام الذكاء الاصطناعي. كذلك يمكن استخدام أجهزة الكمبيوتر الكمية في وضع نموذج للجسيمات دون الذرية، والتفاعلات الجزيئية، والتفاعلات الكيميائية. ويمكن أن يُحدث ذلك ثورة في الهندسة الكيميائية وعلوم المواد، ويسمح بتصميم مواد جديدة، مثل بطاريات الحالة الصلبة. ويمكن لأجهزة الكمبيوتر الكمية أيضا أن تساعدنا في فهم تغير المناخ.

ويمكن لأجهزة الكمبيوتر الكمية أن تحُدث تحولا في النظام المالي أيضا، حيث يمكنها إجراء عمليات محاكاة مونت كارلو– التي تُستخدم في التنبؤ بسلوك الأسواق من خلال نماذج محاكاة الأسعار والمخاطر – بصورة أكثر دقة في الوقت الحقيقي تقريبا. ولن تكون هناك حاجة إلى تبسيط هذه النماذج بوضع افتراضات غير واقعية. ويمكن لأجهزة الكمبيوتر الكمية أيضا حل المشكلات المتعلقة بتعظيم الفائدة – مثل تخصيص رأس المال، أو تحديد استثمارات الحافظة، أو إدارة النقود في شبكات ماكينات الصراف الآلي – في جزء من الوقت الذي تحتاجه أجهزة الكمبيوتر الرقمية. ويمكن لأجهزة الكمبيوتر الكمية أيضا تعجيل تدريب خوارزميات تَعلُّم الآلة. ويزداد الوقت الذي تحتاجه أجهزة الكمبيوتر الرقمية للقيام بذلك زيادة أسية مع كل بُعد تتم إضافته. ولا يكون الحال كذلك مع أجهزة الكمبيوتر الكمية.

والمخاطر

ومع ذلك، هناك مخاطر. فقوة المعالجة الحاسوبية التي تتميز بها هذه الآلات الكمية القوية يمكن أن تهدد أساليب التشفير الحديثة، وهو ما يكون له انعكاسات واسعة النطاق على الاستقرار المالي والخصوصية. ويستند التشفير في الوقت الحالي إلى ثلاثة أنواع رئيسية من الخوارزميات: المفاتيح المتماثلة، والمفاتيح غير المتماثلة (المعروفة أيضا باسم المفاتيح العامة)، ووظائف التجزئة. فاستنادا إلى خوارزمية المفاتيح المتماثلة، يتم استخدام نفس المفتاح لتشفير الرسالة وفك تشفيرها. أما خوارزمية التشفير غير المتماثل فتستخدم زوجا مترابطا من المفاتيح (أحدهما خاص والآخر عام). ولا يمكن فك تشفير رسالة مشفرة بمفتاح واحد إلا عن طريق الزوج الخاص بهذا المفتاح. وتُستخدم هذه الخوارزميات على نطاق واسع في التحقق الرقمي من الهوية، والتوقيعات الرقمية، وأمن البيانات. وتعمل وظائف التجزئة على تحويل المُدخل الرقمي إلى مجموعة فريدة من البايتات ذات الحجم الثابت. ويتم استخدامها لتخزين كلمات السر بشكل آمن ودعم الهويات الرقمية.

وقد نجحت هذه الخوارزميات التشفيرية غالبا في حماية البيانات. فحتى أجهزة الكمبيوتر الرقمية فائقة السرعة وتقنيات تحليل الشفرات الأكثر تقدما اليوم لا يمكنها فك تشفير هذه البيانات بالسرعة الكافية. ومع ذلك، ستكون أجهزة الكمبيوتر الكمية قادرة على حل المشكلات الرياضية بسرعة أكبر بكثير من أجهزة الكمبيوتر الرقمية فائقة السرعة. وسيؤدي ذلك إلى

الصورة: GETTY IMAGES / PICTURE ALLIANCE / JULIAN STRATENSCHULTE

يجب على المؤسسات المالية اتخاذ خطوات فورية للاستعداد لعملية تحول التشفير.

جعل التشفير غير المتماثل غير قابل للتطبيق وسيُضعف مفاتيح التشفير ووظائف التجزئة الأخرى. ومن الناحية النظرية، يمكن لجهاز كمبيوتر كمي يعمل بكامل طاقته فك مفتاح تشفير غير متماثل في غضون دقائق. وتكون مفاتيح التشفير العامة معرضة للخطر بوجه خاص لأن معظمها يستند إلى مسألة التحليل إلى العوامل: حيث يصعب على أجهزة الكمبيوتر الرقمية إيجاد عددين أوليين من حاصل ضربهما. وفي المقابل، يمكن لأجهزة الكمبيوتر الكمية أن تفعل ذلك بسهولة.

وتُستخدم مفاتيح التشفير غير المتماثلة على نطاق واسع لتأمين الاتصالات عبر الإنترنت. وقد تؤدي الهجمات الناجحة ضد هذه الخوارزميات إلى تعريض الروابط التي يستخدمها النظام المالي للخطر، بما في ذلك على سبيل المثال الصيرفة عبر الهاتف المحمول، والتجارة الإلكترونية، ومعاملات الدفع، والسحب النقدي من ماكينات الصراف الآلي، واتصالات الشبكة الخاصة الافتراضية. أما التطبيقات المعرضة للخطر التي تعتمد على التشفير باستخدام المفاتيح العامة أيضا فتشمل الأصول الرقمية الشهيرة، مثل البيتكوين والإثيريوم، بالإضافة إلى تطبيقات شبكة الإنترنت المحمية بكلمة السر. وأشهر هذه البروتوكولات، وهو «HTTPS»، يستخدمه ٩٧ من أفضل ١٠٠ موقع إلكتروني في العالم.

وربما يكون الوقت قد فات بالفعل بالنسبة لبعض التطبيقات. فأي معلومات يُفترض أنها آمنة اليوم يمكن رصدها وتخزينها لفك تشفيرها لاحقا بمجرد إنشاء أجهزة كمبيوتر كمية تتسم بقدر كاف من القوة. والواقع أن أي رسالة شخصية أو مالية مشفرة يتم إرسالها وتخزينها اليوم يمكن فك تشفيرها بأثر رجعي باستخدام جهاز كمبيوتر كمي قوي. غير أن معظم المؤسسات المالية والأجهزة التنظيمية لم تنتبه بعد لهذه المخاطر الجديدة.

سباق مع الآلة

بدأ بالفعل السباق لتطوير معايير وخوارزميات جديدة للتشفير مضادة لهجمات أجهزة الكمبيوتر الكمية. ففي الولايات المتحدة، يُجري المعهد الوطني للمعايير والتكنولوجيا مسابقة لتطوير خوارزميات التشفير المضادة لهجمات أجهزة الكمبيوتر الكمية. ويأمل المعهد أن يعلن عن فائز بحلول عام ٢٠٢٤. ويقوم المعهد الأوروبي لمعايير الاتصالات بدور قيادي أيضا. وتساهم هذه الجهود في أنشطة الجهات الأخرى المعنية بوضع المعايير. ولكن بسبب المخاطر ذات الأثر الرجعي، فإن المؤسسات المالية لديها فرصة محدودة لتنفيذ المعايير الجديدة.

ويجب على المؤسسات المالية اتخاذ خطوات فورية للاستعداد لعملية تحول التشفير. وينبغي أن تبدأ بتقييم المخاطر ذات الأثر الرجعي والمخاطر المستقبلية الناشئة عن أجهزة الكمبيوتر الكمية، بما في ذلك مخاطر المعلومات التي ربما تكون قد تم رصدها بالفعل ويمكن استغلالها بعد سنوات. وينبغي للمؤسسات المالية بعد ذلك وضع خطط لتحويل التشفير الحالي إلى خوارزميات التشفير المضادة لهجمات أجهزة الكمبيوتر الكمية. ويتضمن ذلك إجراء حصر لعمليات التشفير باستخدام المفاتيح العامة التي تستخدمها هذه المؤسسات بالإضافة إلى تلك التي يستخدمها أي موردين آخرين. وسيتطلب الأمر تحويل الخوارزميات الضعيفة إلى خوارزميات تشفير مضادة لهجمات أجهزة الكمبيوتر الكمية. وينبغي أن تعمل المؤسسات المالية أيضا على زيادة مرونة التشفير بحيث يمكن الارتقاء بالخوارزميات بسلاسة. وتوضح تجارب عمليات استبدال الخوارزميات، رغم أنها أبسط بكثير من الانتقال إلى معايير التشفير المضادة لهجمات أجهزة الكمبيوتر الكمية، أنها يمكن أن تكون مربكة للغاية. كذلك فإن إجراء عمليات الاستبدال هذه غالبا ما يستغرق سنوات أو عقودا.

وهناك دور مهم يقوم به صندوق النقد الدولي في زيادة وعي بلدانه الأعضاء بالمخاطر التي يتعرض لها الاستقرار المالي من أجهزة الكمبيوتر الكمية وفي تعزيز معايير وممارسات التشفير المضادة لهجمات أجهزة الكمبيوتر الكمية. وينبغي للصندوق أن يشجع البلدان الأعضاء على التعاون الوثيق في مجال تطوير معايير التشفير المضادة لهجمات أجهزة الكمبيوتر الكمية لضمان إمكانية التشغيل البيني واعتماد خطط تحويل التشفير في قطاعاتها المالية.

وتتسم أجهزة الكمبيوتر الكمية اليوم بالحساسية الشديدة. فأي اضطراب بيئي، مثل الحرارة أو الضوء أو الاهتزاز، يؤدي إلى تحول الكيوبتات من حالتها الكمية إلى بتات منتظمة. وينتج عن ذلك أخطاء حسابية. ومع ذلك فإن الآلات التي تحسب بأخطاء أقل وقادرة على فك الرموز ليست بعيدة. وينبغي للمؤسسات المالية إدراك المخاطر وتأمين نظمها قبل فوات الأوان. وفي نهاية المطاف، يزخر التاريخ بالقصص التي تحذر من رموز كان من المفترض أنها غير قابلة للاختراق ولكن تم اختراقها عن طريق التكنولوجيا الجديدة. FD

خوسيه ديودورو هو مالك منصة جمع البيانات، **وماجد ملايكا** هو خبير أول في التحول الرقمي ومخاطر الأمن السيبراني في إدارة تكنولوجيا المعلومات بصندوق النقد الدولي. **ومايكل غوربانيوف** هو اقتصادي أول في إدارة الاستراتيجية والسياسات والمراجعة بصندوق النقد الدولي، **وتحسين سعدي صديق** هو نائب رئيس قسم في إدارة آسيا والمحيط الهادئ بصندوق النقد الدولي.

يستند هذا المقال إلى ورقة العمل رقم ٢١/٧١ الصادرة عن الصندوق بعنوان *"Quantum Computing and the Financial System: Spooky Action at a Distance?"*.