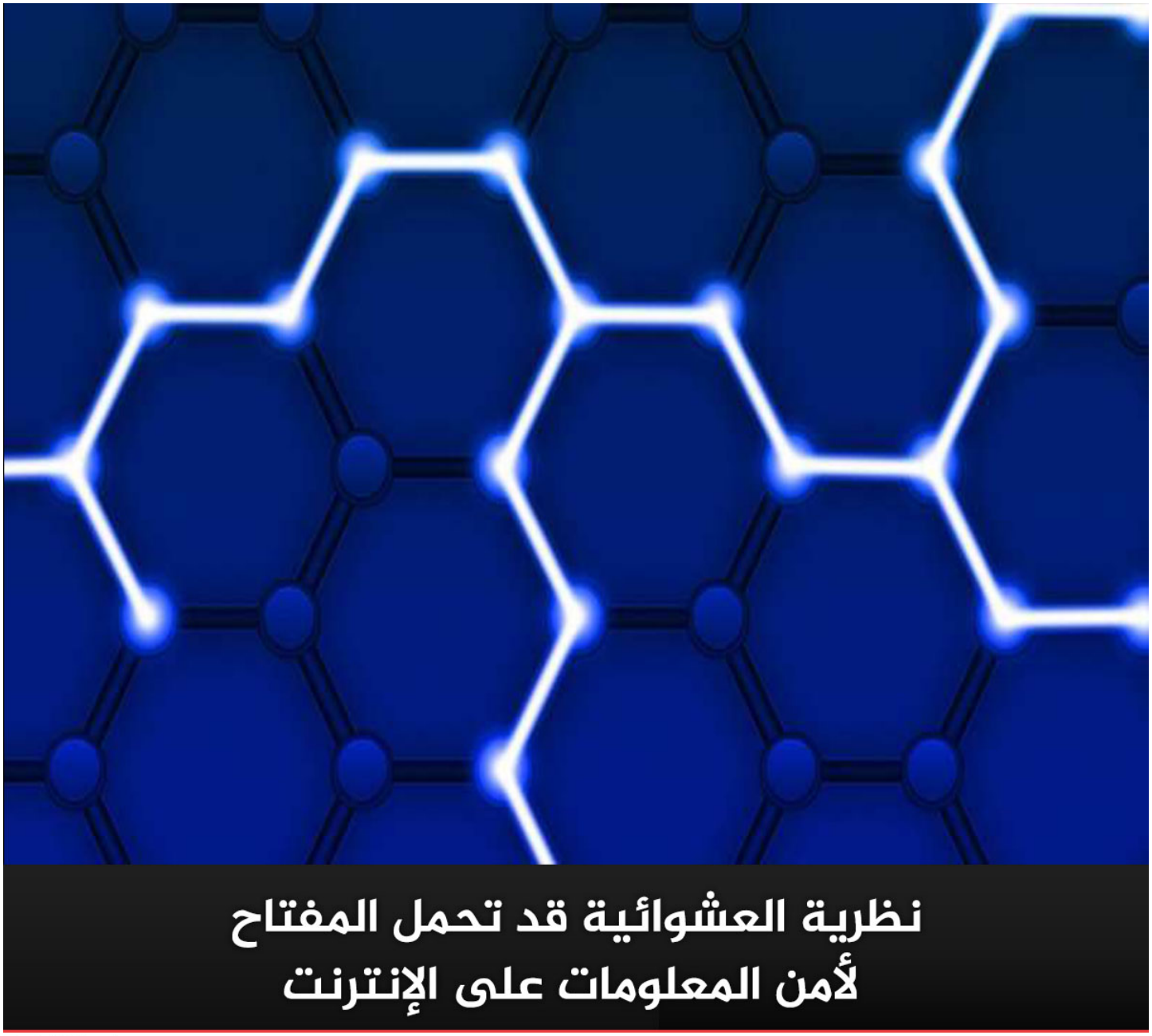
نظرية العشوائية قد تحمل المفتاح لأمن المعلومات على الإنترنت



حقوق الصورة: Pixabay/CC0 Public Domain.

هل هناك رمز غير قابل للفك؟

كان هذا السؤال محوريًا في علم التشفير منذ آلاف السنين، ويقع في صميم الجهود المبذولة لتأمين المعلومات الخاصة على الإنترنت؛ حدد باحثون في جامعة **Cornell Tech** في ورقةٍ بحثية جديدة مشكلةً تحمل مفتاح ما إذا كان يمكن كسر كل التشفير على الانترنت، بالإضافة إلى ارتباطٍ مفاجئٍ بمفهومٍ رياضيٍّ يهدف إلى تعريف العشوائية وقياسها.

قال رافائيل باس **Rafael Pass**، أستاذ علوم الحاسوب في جامعة كورنيل: "لا تُظهر نتيجتنا أن في التشفير مشكلةً طبيعيةً فحسب، بل تظهر أيضًا ارتباطًا عميقًا بين مجالين منفصلين تمامًا للرياضيات وعلوم الحاسوب، وهما علم التشفير ونظرية المعلومات الخوارزمية".

رافائيل باس هو مؤلف مشارك لكتاب "**On-Way Functions Kolmogorov Complexity**"، والذي سيُقدَّم في ندوة **IEEE** حول أسس علوم الحاسوب، التي ستُعقد في الفترة من 16 إلى 19 نوفمبر/تشرين الثاني في دورهام، شمال كارولينا.

وقد قال: "النتيجة هي أن هناك مشكلة حسابيةً طبيعيةً قد قُدِّمت في الستينيات في الاتحاد السوفيتي تميز جدوى التشفير الأساسي، أي تشفير المفتاح الخاص والتوقيعات الرقمية والمصادقة، على سبيل المثال".

اعتُبِر التشفير دورةً منذ آلاف السنين: اخترع شخصٌ ما رمزًا، وكانت الشيفرة فعالةً حتى كسرها شخصٌ ما في النهاية، وأصبح الرمز غير فعالٍ. في سبعينيات القرن الماضي، سعى الباحثون للحصول على نظريةٍ أفضل للتشفير، وقدموا مفهوم الدالة أحادية الاتجاه، وهي مهمةٌ أو مشكلةٌ سهلةٌ في اتجاهٍ واحدٍ ومستحيلةٌ في الاتجاه الآخر.

على سبيل المثال، من السهل إشعال عود ثقاب، لكن من المستحيل إعادة عود ثقابٍ مشتعلٍ إلى حالته غير المشتعلة دون إعادة ترتيب ذراته، وهي مهمةٌ صعبةٌ للغاية.

قال باس: "كانت الفكرة، إذا كانت لدينا دالةٌ أحاديةُ الاتجاه، فقد يكون ذلك نقطةَ انطلاقٍ جيدةً جدًا لفهم التشفير. تشفير الرسالة سهلٌ للغاية، وإذا كان لديك المفتاح، فيمكنك أيضًا فك تشفيرها، ولكن يجب على أي شخص لا يعرف المفتاح أن يفعل نفس الشيء مثل استعادة عود ثقابٍ مضاءٍ".

ولكن لم يتمكن الباحثون من إثبات وجود دالة أحادية الاتجاه؛ يعتمد المرشح الأكثر شهرة، والذي يُعد أيضًا أساس مخططات التشفير الأكثر استخدامًا على الإنترنت، على تحليل الأعداد الصحيحة. من السهل ضرب عددين أوليين عشوائيين ــ على سبيل المثال، 23 و47– ولكن من الصعب جدًا العثور على هذين العاملين إذا أعطيت ناتجهما فقط والذي هو 1081.

يُعتقد بعدم وجود خوارزمية فعالة للأعداد الكبيرة، على الرغم من عدم عثور الباحثين على الخوارزميات الصحيحة بعد، وفق قول باس.

وأضاف: "السؤال المركزي الذي نتناوله هو: هل هي موجودة؟ هل هناك بعض المشاكل الطبيعية التي تميز وجود دوالٍّ أحادية الاتجاه؟ إذا كان الأمر كذلك، فهذه هي أصل كل المشكلات، وإذا كان لديك طريقة لحل هذه المشكلة، يمكنك كسر جميع الوظائف ذات الاتجاه الواحد المزعومة، وإذا كنت لا تعرف كيفية حل هذه المشكلة، فيمكنك في الواقع الحصول على تشفير آمن".

في غضون ذلك، حدد علماء الرياضيات في الستينيات ما يُعرف باسم تعقيد كولموغوروف **Kolmogorov**، الذي يشير إلى قياس كمية العشوائية أو نمط سلسلة من الأرقام؛ يُعرَّف تعقيد كولموغوروف لسلسلةٍ من الأرقام على أنه طول أقصر برنامج حاسوب يمكنه إنشاء السلسلة؛ بالنسبة لبعض السلاسل، مثل 121212121212121212121212121212، يوجد برنامج قصير يُنشِئُه، لكن بالنسبة لسلاسل الأرقام الأكثر تعقيدًا والعشوائية، مثل 375390173328403934529543290، قد لا يوجد برنامج أقصر من طول السلسلة نفسها.

لطالما كانت هذه المشكلة محط اهتمام علماء الرياضيات والحاسوب، بمن فيهم جوريس هارتمانيس **Juris Hartmanis**، الأستاذ الفخري لعلوم وهندسة الحاسوب. نظرًا لأن برنامج الحاسوب الذي يحاول إنشاء الرقم قد يستغرق ملايين أو حتى مليارات السنين، فقد طور الباحثون في الاتحاد السوفيتي خلال الستينيات، وكذلك هارتمانيس وآخرون في الثمانينيات، تعقيد كولموغوروف المحددة زمنيًا،

أي طول أقصر برنامج يمكنه إخراج سلسلة من الأرقام في فترةٍ زمنيةٍ معينةٍ.

في الورقة البحثية، أظهر باس وطالب الدكتوراه ياني ليو**Yaniy Lou** ، أنه إذا كانت حوسبة تعقيد كولموغوروف المقيدة بالزمن صعبة، فعندئذ توجد دوالٌّ أحادية الاتجاه.

على الرغم من أن اكتشافهم نظريًا، لكنّ له تداعياتٌ محتملةٌ في التشفير، بما في ذلك أمن الإنترنت.

قال باس: "إذا كان بإمكانك التوصل إلى خوارزمية لحل مشكلة تعقيد كولموغوروف المقيدة بالزمن، يمكنك كسر جميع أنظمة التشفير، وجميع التوقيعات الرقمية. مع ذلك، إذا لم تكن هناك خوارزميةٌ فعالةٌ لحل هذه المشكلة، يمكنك الحصول على دالة أحادية الاتجاه، وبالتالي يمكنك الحصول على تشفير آمن وتوقيعات رقمية وما إلى ذلك".

- التاريخ: 2020-09-01
- التصنيف: علوم أخرى

#علوم الحاسوب #التشفير الرقمي

المصطلحات

- **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

- techxplore.com

المساهمون

- ترجمة
  - لوتيسيا هيثم يوسف
- مُراجعة
  - Azmi J. Salem
- تحرير
  - رأفت فياض
- تصميم
  - Azmi J. Salem
- نشر

- احمد صلاح