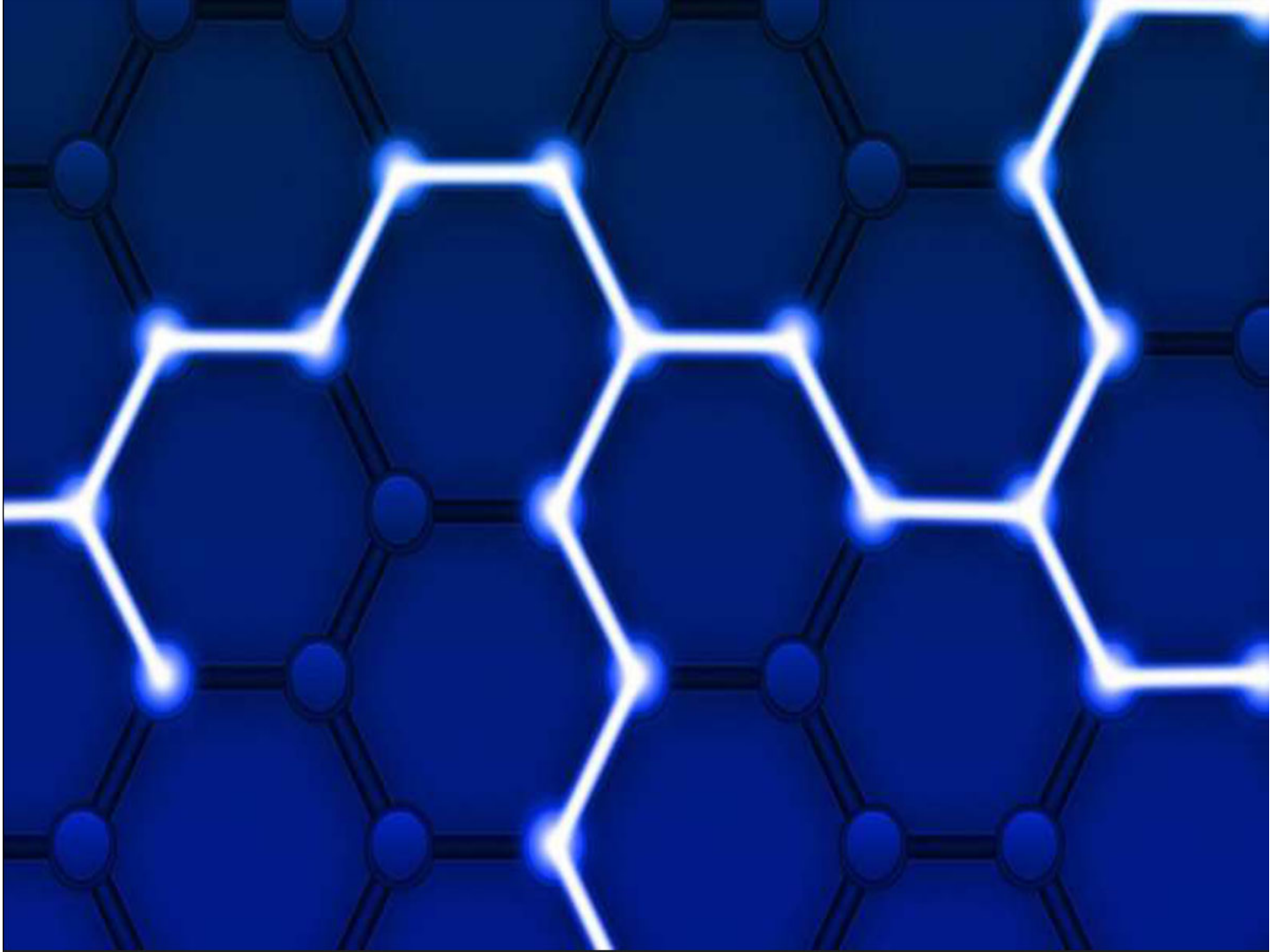


نظرية العشوائية قد تحمل المفتاح لأمن المعلومات على الإنترنت



نظرية العشوائية قد تحمل المفتاح لأمن المعلومات على الإنترنت



www.nasainarabic.net

[@NasalnArabic](https://twitter.com/NasalnArabic) [f NasalnArabic](https://www.facebook.com/NasalnArabic) [NasalnArabic](https://www.youtube.com/channel/UCNasalnArabic) [NasalnArabic](https://www.instagram.com/NasalnArabic) [NasalnArabic](https://www.linkedin.com/company/NasalnArabic)



حقوق الصورة: Pixabay/CC0 Public Domain.

هل هناك رمز غير قابل للفك؟

كان هذا السؤال محورياً في علم التشفير منذ آلاف السنين، ويقع في صميم الجهود المبذولة لتأمين المعلومات الخاصة على الإنترنت؛ حدد باحثون في جامعة **Cornell Tech** في ورقة بحثية جديدة مشكلةً تحمل مفتاح ما إذا كان يمكن كسر كل التشفير على الإنترنت، بالإضافة إلى ارتباط مفاجئ بمفهوم رياضي يهدف إلى تعريف العشوائية وقياسها.

أي طول أقصر برنامج يمكنه إخراج سلسلة من الأرقام في فترة زمنية معينة.

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

على الرغم من أن اكتشافهم نظرياً، لكن له تداعيات محتملة 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 التوقعات الرقمية. مع ذلك، إذا لم تكن هناك خوارزمية فعالة لحل هذه المشكلة، يمكنك الحصول على دالة أحادية الاتجاه، وبالتالي يمكنك الحصول على تشفير آمن وتوقعات 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 الكتلون أو أكثر، مما يُعطيها شحنة موجبة. وتسمى أيوناً موجباً، وقد تكون ذرة اكتسبت الكتلوناً أو أكثر فتصبح ذات شحنة سالبة وتسمى أيوناً سالباً

المصادر

• techxplore.com

المساهمون

• ترجمة

◦ لوتيسيا هيثم يوسف

• مراجعة

◦ Azmi Salem

• تحرير

◦ رأفت فياض

• تصميم

◦ Azmi Salem

• نشر

