توليد الأرقام العشوائية كمومياً

توليد الأرقام العشوائية كمومياً

مولد أرقام عشوائية كمومي يجمع أفضل ما في النهجين

إن العلم نهج غالباً ما يسعى إلى النظام والأنماط الموجودة في العالم المحيط بنا، لكن للعشوائية (**Randomness**) استخداماتها أيضاً، فالأعداد العشوائية أداة مهمة جداً في مجالات مثل التشفير (**Cryptography**)، والنمذجة الحاسوبية (**Computer Simulations**)، والتحليل الإحصائي(**Statistical Analysis**)، ولعل توليد سلسلة محارف طويلة من أرقام عشوائية أمرٌ صعب ، وهو ضروري لتحقيق أداء أفضل والوصول إلى أمانٍ أكبر في تلك التطبيقات.

تتضمن إحدى طرق توليد الأرقام العشوائية الاستفادة من العشوائية المتأصلة في أنظمة كمومية (**Quantum System**) معروفة بالضجيج الكمومي (**Quantum Noise**)، وتتضمن إجراءات التوليد الكمومي للأرقام العشوائية (**QRNG**) مصادر فوتونية مفردة، ولأنّ إصدار الفوتونات المفردة يجري عند أزمنة عشوائية، فمن المستحيل القيام بتحديد مثالي لعدد الفوتونات الصادرة عند زمنٍ محدد، ما يؤدي إلى وجود ارتياب في القياس وعشوائية أيضاً.

تنتمي الطرق المستخدمة حالياً في مجال **QRNG** إلى نوعين: طرق تعتمد على الجهاز (**Device-Dependent**)، وطرق لا تعتمد على الجهاز (**Device-Independent**)، حيث تتطلب الطرق التي تعتمد على الجهاز، والمستخدمة في كل التطبيقات التجارية لـ **QRNGs**، وجود معرفة تفصيلية بآلية عمل الأجهزة المستخدمة في البروتوكول (**Protocol**)، وتُولد هذه الطريقة الأرقام العشوائية عند معدلات مرتفعة جداً (4 مليون بت عشوائي في الثانية الواحدة) وعند مستوى أمان أقوى بكثير من ذلك الموجود في مولدات الأرقام التقليدية شبه العشوائية (**Classical Pseudo-Random Number Generators**)، لكنها تعتمد على افتراضات من الصعب التحقق منها.

ومن ناحية أخرى، لا تتطلب الطرق التي لا تعتمد على الجهاز وجود نفس المعرفة بالأجهزة وهي تُقدم أماناً أقوى كذلك، إلا أن التطبيق العملي لها يتطلب وجود إعدادات متطورة ومعقدة جداً، ولا يُمكن إنجاز ذلك إلا عند معدلات منخفضة جداً لتوليد الأرقام العشوائية.

وفي ورقة علمية جديدة نُشرت في مجلة "**Physical Review Letters**"، قام علماء فيزياء من جامعة جنيف بتطوير بروتوكول يُقدم نهجاً وسيطاً للوصول إلى QRNG، وهو يتطلب وجود افتراضات عامة قليلة حول الأجهزة، لكنه ليس بحاجة إلى نموذج تفصيلي خاص بعملها، ويقع كلٌ من معدل أداء هذا النهج (23 بت عشوائي في الثانية الواحدة) ومستوى أمانه بين المستويات الخاصة بالطرق التي تعتمد على الجهاز وتلك المستقلة عنه؛ لكنّ هذا النهج يشترك مع الأولى بإمكانية تطبيقه بوجود التكنولوجيا القياسية الحالية.

يقول نيكولا برونر (**Nicolas Brunner**)، المؤلف المشارك في الدراسة من جامعة جنيف لـ **Phys.org**: "قد تكون الأهمية الأساسية لعملنا هي القدرة على التحقق من حصول عملية التوليد العشوائي للأرقام ضمن سيناريو تعاني فيه الأجهزة من عيوب تقنية، لكنها ليست ضارة بالنسبة للمستخدم". ويُضيف قائلاً: "إنه سيناريو يقع في مكانٍ ما بين الطرق المعتمدة على الأجهزة، التي يُفترض فيها أن الأجهزة موصوفة بشكلٍ جيد، وبين تلك المستقلة عن الأجهزة التي يُمكن فيها للعد من حيث المبدأ إدارة الجهاز".

يكمن التحسين الأساسي في البروتوكول الجديد في كونه ذاتي الاختبار (**Self-testing**)، أي أن باستطاعته تقديم تقدير بالزمن الحقيقي لعشوائية بيانات الفوتونات التجريبية بالاعتماد على قياس الانتروبي (**Entropy**) الخاص بها، كما يُمكن للنهج الجديد التمييز بين هذه العشوائية الحقيقية وتلك الناجمة عن مصادر عشوائية أخرى مثل العيوب التقنية (**Technical Imperfections**).

عندما تتم معرفة مقدار العشوائية الحقيقية، يُمكن بعدها معالجة البيانات الخام بشكلٍ مناسب لتوليد محارف من الأرقام العشوائية، ومن أجل إثبات القدرة الذاتية للاختبار، فقد أطفأ الباحثون وببساطة مكيف الهواء في الغرفة، وبسبب الحساسية الشديدة لأنظمة كمومية كتلك المعتمدة على مصادر فوتونات مفردة لبيئاتها، فإن التغير الحاصل في درجة الحرارة يؤثر على تحاذي التجهيز البصري عشوائية الفوتونات الصادرة، ومن ثم يستطيع النظام التعرف مباشرةً على أي تغير في عشوائية التوليد بحيث يُمكن تطبيق المزيد من المعالجة، وضمان استمرار الحصول على جيل من الأرقام العشوائية عالية النوعية.

وبشكل عام، فإن البروتوكول الجديد يقدم طريقة **QRNG** مبسطة على الرغم من عدم تحقيقها لمعدلات مرتفعة كتلك الموجودة في التطبيقات التجارية لـ **QRNGs**، إلا أنها تؤدي إلى الحصول على مستوى أمني أقوى ودون الحاجة إلى التوصيف التفصيلي للأجهزة، وقد يكون هذا الجمع بين المميزات مفيداً جداً للتطبيقات المستقبلية.

يقول برونر: "إن العشوائية مصدر مهم جداً للعديد من التطبيقات". ويتابع قائلاً: "ومع ذلك، فإنّ موثوقية العشوائية لا تزال تُمثل تحدياً مهماً؛ أي بمعنى آخر القدرة على تحديد مدى عشوائية مخرجات بعض الأجهزة بالاعتماد على افتراضات بسيطة يُمكن التحقق منها".

ويختم برونر قائلاً: "إن هدفنا هو تطوير مخططات أفضل، يُمكن استخدامها عملياً بشكلٍ أسهل وتُحقق معدلات أكثر ارتفاعاً بكثير، ومع ذلك، فالهدف الرئيسي لا يزال يكمن في إيجاد سيناريو يُقدم الحل الأمثل عند المفاضلة بين الأمان وسهولة التطبيق".

- التاريخ: 2015-05-18
- التصنيف: فيزياء

#physics #quantum #photon

المصطلحات

- **الإنتروبي (entropy)**: هو كمية الطاقة غير المتاحة للقيام بعمل في نظام فيزيائي، وقد أطلق عليه كلاوزيوس مصطلح الإنتروبي ملهماً بكلمة tropi التي تعني التحول، واختيرت لتكون أقرب ما يُمكن من كلمة الطاقة (energy)، ويقول أشهر قوانين الطبيعة المعروف بالقانون الثاني في الترموديناميك "لا يُمكن لانتروبي نظام فيزيائي مغلق أن يتناقص أبداً".
- **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
- **قسم استكشاف الكون (EUD)**: قسم استكشاف الكون، ويقع في مركز غودارد_ناسا لرحلات الفضاء. يقوم العلماء، والمهندسون والتقنيون الذين يعملون هناك بدراسة الفيزياء الفلكية الخاصة بالأجسام التي تُصدر أشعة كونية، وأشعة اكس و إشعاع غاما.

المصدر: ناسا

المصادر

- phys.org
- الورقة العلمية
- الصورة

المساهمون

- ترجمة
  - همام بيطار
- تحرير
  - آلاء محمد حيمور
- تصميم
  - عمار الكنعان

- صوت
  - إيناس قضماني
- مكساج
  - أنس الهود
- نشر
  - ريم المير أبو عجيب
  - أنس الهود