



NIST y sus socios utilizan la mecánica cuántica para crear una fábrica de números aleatorios

[NIST](#) y sus socios de la [Universidad de Colorado en Boulder](#), en colaboración con ICFO y QuSide, construyeron el primer generador de números aleatorios que utiliza el entrelazamiento cuántico para producir números aleatorios verificables. Ofrecido como un servicio público gratuito, el Colorado University Randomness Beacon (CURBy) puede utilizarse en cualquier lugar donde una fuente pública e independiente de números aleatorios sea necesaria, como la selección de candidatos para un jurado o la asignación de recursos mediante una lotería pública.

June 12, 2025

La aleatoriedad es increíblemente útil. Las personas suelen recurrir a métodos como sacar pajitas, lanzar dados o tirar una moneda para tomar decisiones justas. Los números aleatorios permiten a los auditores hacer selecciones completamente imparciales. La aleatoriedad

también es clave para la seguridad: si una contraseña o código es una secuencia impredecible de números, es más difícil de descifrar. Muchos de nuestros sistemas criptográficos actuales utilizan generadores de números aleatorios para producir claves seguras.

Pero, ¿cómo saber si un número aleatorio es realmente aleatorio? Los algoritmos clásicos solo pueden crear números pseudoaleatorios, de modo que alguien con suficiente conocimiento del algoritmo o del sistema podría manipularlo o predecir el siguiente número. Un experto en prestidigitación podría manipular el lanzamiento de una moneda para garantizar un resultado de cara o cruz. Incluso los lanzamientos de moneda más cuidadosos pueden tener sesgos; con suficiente estudio, sus resultados podrían predecirse. ¿La verdadera aleatoriedad es algo que nada en el universo puede predecir con antelación? dijo Krister Shalm, físico [NIST](#). Incluso si un generador de números aleatorios utilizara procesos aparentemente aleatorios de la naturaleza, sería difícil verificar que esos números son verdaderamente aleatorios, agregó Shalm.

Einstein creía que la naturaleza no era aleatoria, pronunciando su frase célebre: ¿Dios o juega a los dados con el universo? Pero los científicos han demostrado que Einstein estaba equivocado. A diferencia de los dados o los algoritmos, la mecánica cuántica es inherentemente aleatoria. Realizando un experimento cuántico llamado test de Bell, Shalm y su equipo han transformado esta fuente de verdadera aleatoriedad cuántica en un servicio de generación de números aleatorios trazable y certificable. Sus resultados acabaron de publicarse [Nature](#).

¿Si Dios juega a los dados con el universo, entonces eso se puede convertir en el mejor generador de números aleatorios que el universo permite, dijo Shalm. ¿Que vamos realmente a sacar este experimento del laboratorio y convertirlo en un servicio público utilizable? Para lograrlo, los investigadores del NIST y sus compañeros de la Universidad de Colorado en Boulder crearon el Faro de Aleatoriedad de la Universidad de Colorado [CURBy](#) por sus siglas en inglés. CURBy produce números aleatorios de forma automática y los transmite diariamente a través de un sitio web para que cualquiera los use.

En el corazón de este servicio está la prueba de Bell operada por el NIST, que proporciona resultados verdaderamente aleatorios. Esta aleatoriedad actúa como una especie de materia prima que el resto del sistema de los investigadores refina hasta obtener los números aleatorios publicados por el f

El papel de ICFO y QuSide

Investigadores de ICFO (incluyendo cofundadores de QuSide) y personal de ingeniería de ICFO EW inventaron y construyeron los rápidos generadores cuánticos de números aleatorios que NIST utilizó para las pruebas de Bell.

El test de Bell mide pares de fotones *¿entrelazados?* cuyas propiedades están tan correlacionadas incluso cuando están separados por grandes distancias. Cuando

los investigadores miden una partícula individual, el resultado es aleatorio, pero las propiedades del par están más correlacionadas de lo que dicta la física clásica, permitiendo a los investigadores verificar la aleatoriedad. Einstein llamó a esta no-localidad cuántica "acción fantasmal a distancia".

¿Elegir que propiedades de las partículas entrelazadas medir debe hacerse muy rápidamente y con un alto grado de confianza en la aleatoriedad. Esa es la contribución de ICFO y QuSide. Gracias a ello, los resultados de las mediciones en el test de Bell también fueron aleatorios, pero a un nivel superior.

Este es el primer servicio de generación de números aleatorios que utiliza la no-localidad cuántica como fuente, siendo la fuente de números aleatorios más transparente hasta la fecha. Esto se debe a que el nivel de certificación y trazabilidad de los resultados es mucho mayor que nunca antes. De hecho, el gran avance del proyecto es que los usuarios pueden confiar en los números resultantes sin necesidad de confiar en las entidades que los generaron. Imagina que dos partidos políticos acuerdan verificar los resultados de una elección revisando una muestra aleatoria de votos. Ninguno de los dos confiaría en el otro para generar los números aleatorios, pero si pueden confiar en un faro de aleatoriedad.

Es un privilegio contribuir a esta generación de aleatoriedad pública sin precedentes usando fenómenos de física cuántica que fueron galardonados con el Nobel. Es un ejemplo claro de cómo las tecnologías cuánticas pueden contribuir a la seguridad en la era de internet. ¿Comento el profesor de ICREA y del ICFO Morgan Mitchell, quien participó en el estudio. El Dr. Carlos Abellán, CEO de QuSide, añadió: **Es realmente un honor contribuir a este experimento con nuestra tecnología de generación de números aleatorios cuánticos; en QuSide, seguimos impulsando el camino hacia la industrialización de estos nuevos dispositivos de generación de aleatoriedad con capacidades avanzadas de verificación.**

Un nuevo servicio público disponible

CURBy es uno de los primeros servicios públicos disponibles que opera con una venta cuántica demostrable. Eso es un gran hito para nosotros, explico Shalm. La calidad y el origen de estos bits aleatorios pueden certificarse directamente, algo que los generadores de números aleatorios convencionales no pueden hacer.

El NIST realizó una de las primeras pruebas experimentales completas de Bell en 2015 lo que estableció firmemente que [la mecánica cuántica es verdaderamente aleatoria](#). En 2018, el NIST fue pionero en métodos para usar estas pruebas de Bell para construir [las primeras fuentes del mundo de verdadera aleatoriedad](#).

Sin embargo, convertir estas correlaciones cuánticas en números aleatorios es un trabajo arduo. Las primeras demostraciones exitosas de la prueba de Bell del NIST requirieron meses de preparación para funcionar durante unas pocas horas, y tomaba mucho tiempo reunir suficientes datos para generar 512 bits de aleatoriedad verdadera. Shalm y su equipo pasaron los últimos años construyendo el experimento para que fuera robusto y funcionara de

manera automática, de modo que pueda proporcionar números aleatorios bajo demanda. En sus primeros 40 días de operación, el protocolo produjo números aleatorios en 7,434 de 7,454 intentos, una tasa de éxito del 99.7%.

¿Cómo generan y certifican aleatoriedad los investigadores?

El proceso comienza generando un par de fotones entrelazados dentro de un cristal no lineal especial. Los fotones viajan por fibra óptica a laboratorios separados en extremos opuestos del pasillo. Una vez que los fotones llegan a los laboratorios, se mide su polarización. Los resultados de estas mediciones son verdaderamente aleatorios. Este proceso se repite 250,000 veces por segundo.

El NIST transmite millones de estos 'lanzamientos de moneda' cuánticos a un programa informático en la Universidad de Colorado Boulder. Luego, ciertos pasos de procesamiento los convierten en una secuencia de bits aleatorios que nadie, ni siquiera Einstein, podría haber predicho. En cierto sentido, este sistema actúa como el mejor lanzamiento de moneda del universo.

NIST y sus colaboradores añadieron la capacidad de rastrear y verificar cada paso del proceso de generación de aleatoriedad. Desarrollaron el protocolo Twine, que marca cada conjunto de datos del faro con un hash. Los hashes se usan en la tecnología blockchain para marcar conjuntos de datos con una huella digital, lo que permite identificar y examinar cada bloque de datos.

El protocolo Twine permite a cualquier usuario verificar los datos detrás de cada número aleatorio, explicó Jasper Palfrey, asistente de investigación en el proyecto en la Universidad de Colorado Boulder. El protocolo puede expandirse para permitir que otros faros de números aleatorios se unan a la red de hashes, creando una red de aleatoriedad a la que todos contribuyen, pero que nadie controla.

Este entramado de cadenas de hashes actúa como una marca de tiempo, vinculando los datos del faro en una estructura trazable. También proporciona seguridad, permitiendo a los participantes del protocolo Twine detectar inmediatamente cualquier manipulación de datos.

¿El protocolo Twine nos permite entretrejer todos estos otros faros en un tapiz de confianza? agregó Palfrey

. Todo el proceso es de código abierto y está disponible para el público, lo que permite a cualquiera no solo verificar su funcionamiento, sino incluso construir su propio generador e números aleatorios sobre la base del faro

. Así, CURBy puede utilizarse en cualquier lugar donde se necesite una fuente pública e independiente de números aleatorios, como la selección de candidatos para jurado, selecciones aleatorias en auditorías o asignación de recursos mediante loterías públicas

Referencia:

Gautam A. Kavuri et al. Traceable random numbers from a non-local quantum advantage.

