ICFO

Image not found

NIST y sus socios utilizan la mecanica cuantica para crear una fabrica de numeros aleatorios

NIST y sus socios de la Universidad de Colorado en Boulder, en colaboracion con ICFO y QuSide, construyeron el primer generador de numeros aleatorios que utiliza el entrelazamiento cuantico para producir numeros aleatorios verificables. Ofrecido como un servicio publico gratuito, el Colorado University Randomness Beacon (CURBy) puede utilizarse en cualquier lugar donde una fuente publica e independiente de numeros aleatorios sea necesaria, como la seleccion de candidatos para un jurado o la asignacion de recursos mediante una loteria publica.

June 12, 2025

La aleatoriedad es increiblemente util. Las personas suelen recurrir a metodos como sacar pajitas, lanzar dados o tirar una moneda para tomar decisiones justas. Los numeros aleatorios permiten a los auditores hacer selecciones completamente imparciales. La aleatoriedad tambien es clave para la seguridad: si una contrasena o codigo es una secuencia impredecible de numeros, es mas dificil de descifrar. Muchos de nuestros sistemas criptograficos actuales utilizan generadores de numeros aleatorios para producir claves seguras.

Pero, ¿como saber si un numero aleatorio es realmente aleatorio? Los algoritmos clasico solo pueden crear numeros pseudoaleatorios, de modo que alguien con suficient conocimiento del algoritmo o del sistema podria manipularlo o predecir el siguiente numero Un experto en prestidigitacion podria manipular el lanzamiento de una moneda par garantizar un resultado de cara o cruz. Incluso los lanzamientos de moneda mas cuidadoso pueden tener sesgos; con suficiente estudio, sus resultados podrian predecirse

i¿½La verdadera aleatoriedad es algo que nada en el universo puede predecir on antelacioni¿½, dijo Krister Shalm, fisico del NIST. Incluso si un generador de numeros aleatorios utilizara procesos aparentemente aleatorios de la naturaleza, seria dificil verificar que esos numeros son verdaderamente aleatorios, agrego Shalm.

Einstein creia que la naturaleza no era aleatoria, pronunciando su frase celebre: i¿½Dios o juega a los dados con el universo.i¿½ Pero los cientificos han demostrado que Einstein es aba equivocado. A diferencia de los dados o los algoritmos, la mecanica cuantic

es inherentemente aleatoria. Realizando un experimento cuantico llamado test de Bell, Sha
m y su equipo han transformado esta fuente de verdadera aleatoriedad cuantica en un serv
cio de generacion de numeros aleatorios trazable y certificable. Sus resultados acaba
de publicarse en Nature.

i¿½Si Dios juega a los dados con el universo, entonces eso se puede convertir en el mej
r generador de numeros aleatorios que el universo permite,i¿½ dijo Shalm. i¿½Que
iamos realmente sacar este experimento del laboratorio y convertirlo en un servicio publico ut
l.i¿½ Para lograrlo, los investigadores del NIST y sus companeros de la Universidad de Col
rado en Boulder crearon el Faro de Aleatoriedad de la Universidad de Colorado, o CURBy por sus
siglas en ingles. CURBy produce numeros aleatorios de forma automatica y los transmite
diariamente a traves de un sitio web para que cualquiera los use.

En el corazon de este servicio esta la prueba de Bell operada por el NIST, que proporciona
resultados verdaderamente aleatorios. Esta aleatoriedad actua como una especie de materia
prima que el resto del sistema de los investigadores i¿½refinai¿½ hasta obtener los num
ros aleatorios publicados por el f

El papel de ICFO y QuSide

Investigadores de ICFO (incluyendo cofundadores de QuSide) y personal de ingenieria de
ICFO EW inventaron y construyeron los rapidos generadores cuanticos de numeros aleatorios
que NIST utilizo para las pruebas de Bell.

El test de Bell mide pares de fotones i¿½entrelazadosi¿½ cuyas propiedades e
tan correlacionadas incluso cuando estan separados por grandes distancias. Cuando
los investigadores miden una particula individual, el resultado es aleatorio, pero las propied
des del par estan mas correlacionadas de lo que dicta la fisica clasica, permitiendo a
los investigadores verificar la aleatoriedad. Einstein llamo a esta no localidad cuantica i¿½
ccion fantasmal a distanc
a.i¿½ Elegir que propiedades de las particulas entrelazadas medir debe hacerse muy rap
damente y con un alto grado de confianza en la aleatoriedad. Esa es la contribucion de ICFO y
QuSide. Gracias a ello, los resultados de las mediciones en el test de Bell tambien fueron ale
torios, pero a un nivel s
perior. Este es el primer servicio de generacion de numeros aleatorios que utiliza la no l
calidad cuantica como fuente, siendo la fuente de numeros aleatorios mas transparente
asta la fecha. Esto se debe a que el nivel de certificacion y trazabilidad de los resultados
s mucho mayor que nunca antes. De hecho, el gran avance del proyecto es que los usuario
pueden confiar en los numeros resultantes sin necesidad de confiar en las entidades
que los generaron. Imagina que dos partidos politicos acuerdan verificar los resultado
de una eleccion revisando una muestra aleatoria de votos. Ninguno de los dos confiara en
el otro para generar los numeros aleatorios, pero si pueden confiar en un faro de aleat
riedad.

Es un privilegio contribuir a esta generacion de aleatoriedad publica sin precedentes

usando fenomenos de fisica cuantica que fueron galardonados con el Nobel. Es un ejemplo claro de como las tecnologias cuanticas pueden contribuir a la seguridad en la era de interneti¿½, comento el profesor de ICREA y del ICFO Morgan Mitchell, quien participo en l estudio. El Dr. Carlos Abellan, CEO de QuSide, anadio: i¿½**Es realmente un honor contribuir a este experimento con nuestra tecnologia de generacion de numeros aleatorios cuanticos; en QuSide, seguimos impulsando el camino hacia la industrializacion de estos nuevos dispositivos de generacion de aleatoriedad con capacidades avanzadas de verificacion**i¿?

Un nuevo servicio publico disponible

i¿½CURBy es uno de los primeros servicios publicos disponibles que opera con una venta a cuantica demostrable. Eso es un gran hito para nosotros,i¿½ explico Shalm. i¿½La calida y el origen de estos bits aleatorios pueden certificarse directamente, algo que los gener dores de numeros aleatorios convencionales no pueden hac r.i¿½ El NIST realizo una de las primeras pruebas experimentales completas de Bell en 2015 lo que establecio firmemente que la mecanica cuantica es verdaderamente aleatoria. En 2018, el NIST fue pionero en metodos para usar estas pruebas de Bell para construir las primeras fuentes del mundo de verdadera aleatoriedad.

Sin embargo, convertir estas correlaciones cuanticas en numeros aleatorios es un trabajo arduo. Las primeras demostraciones exitosas de la prueba de Bell del NIST requirieron meses de preparacion 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 ultimos anos construyendo el experimento para que fuera robusto y funcionara de manera automatica, de modo que pueda proporcionar numeros aleatorios bajo demanda. En sus primeros 40 dias de operacion, el protocolo produjo numeros aleatorios en 7,434 de 7,454 intentos, una tasa de exito del 99.7%.

¿Como 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 optica a laboratorios separados en extremos opuestos del pasillo. Una vez que los fotones llegan a los laboratorios, se mide su polarizacion. 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' cuanticos a un programa informatico en la Universidad de Colorado Boulder. Luego, ciertos pasos de procesamiento los convierten en una secuencia de bits aleatorios que nadie, ni siquiera Einstein, podria haber predicho. En cierto sentido, este sistema actua como el mejor lanzamiento de moneda del universo.

NIST y sus colaboradores anadieron la capacidad de rastrear y verificar cada paso del proceso de generacion de aleatoriedad. Desarrollaron el protocolo Twine, que marca cada

conjunto de datos del faro con un hash. Los hashes se usan en la tecnologia 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 detras de cada numero aleatorio, explico Jasper Palfree, asistente de investigacion en el proyecto en la Universidad de Colorado Boulder. El protocolo puede expandirse para permitir que otros faros de numeros 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 actua como una marca de tiempo, vinculando los datos del faro en una estructura trazable. Tambien proporciona seguridad, permitiendo a los participantes del protocolo Twine detectar inmediatamente cualquier manipulacion de datos.

i¿½El protocolo Twine nos permite entretejer todos estos otros faros en un tapiz de confianzai¿½, agrego Palfre

. Todo el proceso es de codigo abierto y esta disponible para el publico, lo que permite a cualquiera no solo verificar su funcionamiento, sino incluso construir su propio generador e numeros aleatorios sobre la base del far

. Asi, CURBy puede utilizarse en cualquier lugar donde se necesite una fuente publica e independiente de numeros aleatorios, como la seleccion de candidatos para jurado , selecciones aleatorias en auditorias o asignacion de recursos mediante loterias publica

Referencia:

Gautam A. Kavuri et al. Traceable random numbers from a non-local quantum advantage. Nature. Published online June 11, 2025. DOI: 10.1038/s41586-025-09054-3