Proponen un nuevo método para generar auténticos números aleatorios

Un equipo internacional en el que ha participado el investigador Antonio Acín del Instituto de Ciencias Fotónicas (ICFO) ha logrado generar números autenticamente aleatorios con un nuevo método, según publica hoy la revista *Nature*. El trabajo, además de las implicaciones conceptuales que conlleva, tiene aplicaciones prácticas en campos como la criptografía o las simulaciones numéricas en sistemas físicos y biológicos.

SINC 15/4/2010 17:53 CEST

Los números aleatorios se han generado "certificados" por el Teorema de Bell, lo que quiere decir que es posible obtener una secuencia numérica auténticamente aleatoria sin ningún género de duda usando la característica cuántica más intrínseca, denominada la violación de las

desigualdades de Bell. Foto: David Darkmatter.

“Contrariamente a todos los métodos existentes hasta ahora, tanto clásicos como cuánticos, la aleatoriedad de los números generados con el nuevo método está garantizada de manera inequívoca por las leyes cuánticas y es independiente de los dispositivos que se utilizan en la generación”, resume a SINC Antonio Acín, científico del Instituto de Ciencias Fotónicas (ICFO) en Castelldefels (Barcelona).

Acín y otros investigadores de Europa y EE UU publican hoy en *Nature* los resultados de su estudio, en el que demuestran por primera vez que se pueden producir números aleatorios sin necesidad de un conocimiento preciso de los dispositivos.

“Las implicaciones pueden ser muchas”, destaca Acín. “Por un lado, y es fundamental, proponemos las herramientas para cuantificar el azar producido por la física cuántica; pero nuestra propuesta tiene también implicaciones prácticas, ya que los números aleatorios encuentran utilidad en muy diversas aplicaciones, desde la criptografía a la simulación de sistemas físicos y biológicos”, apunta el experto.

Certificado por el Teorema de Bell

Los números aleatorios se han generado "certificados" por el Teorema de Bell, lo que quiere decir que es posible obtener una secuencia numérica auténticamente aleatoria sin ningún género de duda usando la característica cuántica más intrínseca, denominada la violación de las desigualdades de Bell.

En la naturaleza, la aleatoriedad intrínseca sólo se puede encontrar en los procesos cuánticos. En el mundo clásico, todo proceso es determinista, y lo que normalmente se percibe como aleatoriedad es tan solo consecuencia de una falta de conocimiento o de control. A pesar de ello verificar el comportamiento aleatorio de un proceso físico, incluso si es cuántico, supone un problema notablemente difícil.

Las pruebas de aleatoriedad en informática padecen un defecto fundamental: se basan en sistemas clásicos finitos, los ordenadores, y por

tanto son incapaces de producir una frase como "esta secuencia no forma parte de ninguna de las infinitamente diversas secuencias deterministas".

Pero ahora los investigadores explican cómo detectar y cuantificar la aleatoriedad cuántica intrínseca de un dispositivo usando “las correlaciones no locales presentes en los estados cuánticos entrelazados”.

Estos resultados se pueden emplear para diseñar un nuevo tipo de generador de números aleatorios sin análogo clásico. Este dispositivo crearía números aleatorios que serían certificados por el Teorema de Bell, privados e independientes del dispositivo, en el sentido de que sus rasgos aleatorios no dependerían del funcionamiento interno de los dispositivos empleados para generarlos. Ninguna de estas propuestas fundamentales se encontraban en otras existentes hasta ahora para la generación de aletoriedad, ni clásicas ni cuánticas.

Los autores ilustran este enfoque teórico mediante un experimento de prueba de Bell con dos átomos en dos trampas separadas. Mediante su protocolo, han certificado por primera vez que es posible producir aleatoriedad en un experimento sin disponer de un modelo detallado de los dispositivos. Los científicos han conseguido concretamente 42 números autenticamente aleatorios de esta forma.

Referencia bibliográfica:

S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning y C. Monroe. “Random numbers certified by Bell’s theorem”. *Nature* 464, 15 de abril de 2010.

TAGS | NÚMEROS ALEATORIOS |