

Image not found

NIST i els seus socis utilitzen la mecànica quàntica per crear una fàbrica de nombres aleatoris

NIST i els seus socis de la Universitat de Colorado a Boulder, en col·laboració amb ICFO i QuSide, han construït el primer generador de nombres aleatoris que utilitza l'entrellacament quàntic per produir nombres aleatoris verificables.

Ofert com un servei públic gratuït, el Colorado University Randomness Beacon (CURBy) es pot utilitzar a qualsevol lloc on una font pública i independent de nombres aleatoris sigui necessària, com ara la selecció de candidats per a un jurat o l'assignació de recursos mitjançant un sorteig públic.

June 12, 2025

L'aleatorietat és increïblement útil. Sovint, les persones fan servir mètodes com llençar daus o una moneda per prendre decisions justes. Els nombres aleatoris permeten als auditors fer seleccions completament imparcials. L'aleatorietat també és clau per a la seguretat: si una contrasenya o codi és una seqüència impredecible de nombres, és molt més difícil de trencar. Molts dels sistemes criptogràfics actuals utilitzen generadors de nombres aleatoris per produir claus segures.

Pero com podem saber si un nombre és realment aleatori? Els algorismes clàssics només poden crear nombres pseudoaleatoris, de manera que algú amb prou coneixement de l'algorisme o del sistema podria manipular-lo o predir el nombre següent. Un expert en truques de mans podria manipular el llançament d'una moneda per garantir un resultat. Fins i tot els llançaments més acurats poden tenir biaix; amb prou estudi, els seus resultats podrien arribar a predir-se.

«La veritable aleatorietat és allò que res en tot l'univers pot predir amb antelació?»

, diu Krister Shalm, físic **NIST**. Fins i tot si un generador fes servir processos naturals aparentment aleatoris, seria difícil verificar que realment ho són, afegeix Shalm.

Einstein creia que la natura no era aleatòria, pronunciant la seva famosa frase: «Deu no jura als daus amb l'univers.» Però els científics han demostrat que s'equivocava. A diferència dels daus o dels algorismes, la mecànica quàntica és intrínsecament aleatòria. Amb un experiment quàntic anomenat test de Bell, Shalm i el seu equip han convertit aquesta font d'autèntica aleatorietat quàntica en un servei de generació de nombres aleatoris traca-

e i certificable. Els seus resultats acaben de ser publicats [a Nature](#).

¿Si Deu juga als daus amb l'univers, aleshores això es pot convertir en el millor generador de nombres aleatoris que l'univers permeti, diu Shalm. ¿El que volíem era portar aquest experiment fora del laboratori i convertir-lo en un servei públic utilitzant la física quàntica? Per fer-ho realitat, els investigadors del NIST i de la Universitat de Colorado Boulder van crear el Far d'Aleatorietat de la Universitat de Colorado [CURBy](#) per les seves sigles en anglès. CURBy produeix nombres aleatoris automàticament i els transmet diàriament a través d'un lloc web perquè qualsevol els pugui fer servir.

Al cor del servei hi ha el test de Bell operat pel NIST, que proporciona resultats veritablement aleatoris. Aquesta aleatorietat actua com a matèria primera que la resta del sistema refina i processa per produir els nombres publicats pel

El paper de l'ICFO i QuSide

Investigadors de l'ICFO (inclosos cofundadors de QuSide) i l'equip d'enginyeria d'ICFO EW van inventar i construir els ràpids generadors de nombres aleatoris quàntics que el NIST va fer servir per als tests de Bell.

El test de Bell mesura parelles de fotons *entrellacats* amb propietats correlacionades fins i tot quan estan separats per grans distàncies. Quan els investigadors mesuren una partícula individual, el resultat és aleatori, però les propietats de la parella estan més correlacionades del que dicta la física clàssica, cosa que permet verificar l'aleatorietat. Einstein va anomenar aquesta no-localitat quàntica *acció fantasmagòrica a distància*. Escollir quines propietats mesurar en les partícules entrellacades s'ha de fer molt ràpidament i amb un alt grau de confiança en l'aleatorietat. Aquesta és la contribució de l'ICFO i QuSide. Gràcies a això, els resultats de les mesures al test de Bell també van ser aleatoris, però a un nivell superior.

Aquest és el primer servei de generació de nombres aleatoris que utilitza la no-localitat quàntica com a font, i és també la font més transparent de nombres aleatoris fins ara. Això es deu al fet que els resultats són certificables i tracables com mai abans. De fet, el gran avanç del projecte és que els usuaris poden confiar en els nombres resultants sense necessitat de confiar en les entitats que els generen. Imagina dues forces polítiques que han d'auditar unes eleccions revisant una mostra aleatòria de vots. Cap confiaria en l'altra per generar els nombres, però poden confiar en un far d'aleatorietat.

Es un privilegi contribuir a aquesta generació pública sense precedents d'aleatorietat basada en fenòmens de física quàntica guardonats amb el Nobel. És un exemple clar de com les tecnologies quàntiques poden reforçar la seguretat en l'era d'internet. Morgan Mitchell, Professor ICREA i de l'ICFO. El Dr. Carlos Abellán, CEO de QuSide, afegí: **Es un veritable honor contribuir a aquest experiment amb la nostra tecnologia de generació de nombres aleatoris quàntics. A QuSide, seguim avançant en la industrialització d'aquests nous dispositius d'aleatorietat amb capacitats avançades de verificació.**

Un nou servei public disponible

i½CURBy es un dels primers serveis publics disponibles que opera amb un avantatge quant c demostrable. Es un gran assoliment per a nosaltres,i½ explica Shalm. i½La qualitat i l' rigen d'aquests bits aleatoris es poden certificar directament, cosa que els gene adors convencionals no poden f

r.i½ El NIST va fer una de les primeres proves experimentals completes de Bell l'a y 2015, establir que [la mecanica quantica es veritablement aleatoria](#). El 2018, el NIST va ser pioner en metodes per utilitzar aquests tests de Bell per construir les [primeres fonts d'aleatorietat autentica](#) al mon.

No obstant això, convertir aquestes correlacions quantiques en nombres aleatoris es una feina complexa. Les primeres demostracions del test de Bell per part del NIST van requerir mesos de preparacio per funcionar unes poques hores, i va caldre molt de temps per recollir prou dades per generar 512 bits d'aleatorietat. Shalm i el seu equip han passat anys millorant l'experiment perque sigui robust i funcioni automaticament per poder proporcionar nombres aleatoris sota demanda. Durant els primers 40 dies d'operacio, el protocol va generar nombres aleatoris en 7.434 dels 7.454 intents, una taxa d'exit del 99,7 %.

Com generen i certifiquen l'aleatorietat els investigadors?

El proces comença amb la generacio d'una parella de fotons entrellacats dins d'un cristall no lineal especial. Els fotons viatgen per fibra optica cap a laboratoris separats als extrems del passadis. Quan hi arriben, es mesura la seva polaritzacio. Els resultats d'aquestes mesures son veritablement aleatoris. Aquest proces es repeteix 250.000 cops per segon.

El NIST transmet milions d'aquestes i½tirades de monedai½ quantiques a un prog ama informatic a la Universitat de Colorado Boulder. Seguidament, passos especial de processament les converteixen en una seqüencia de bits aleatoris que ningú, ni tan sols Einstein, podria haver predit. En certa manera, aquest sistema actua com la millor tira a de moneda de l'uni

ers. El NIST i els seus col·laboradors han afegit la capacitat de rastrejar i verificar cada p s del proces. Han desenvolupat el protocol [Twine](#), que marca cada conjunt de dades del far amb un hash. Els hashes s'utilitzen en tecnologia blockchain per marcar dades amb una empremta digital, cosa que permet identificar i examinar cada bloc.

El protocol Twine permet que qualsevol usuari verifiqui les dades darrere de cada nombre aleatori, explica Jasper Palfree, assistent d'investigacio del projecte a la Universitat de Colorado Boulder. El protocol pot ampliar-se perque altres fars s'uneixin a la xarxa de hashes, creant una xarxa d'aleatorietat en la qual tothom contribueix pero ningú controla.

Aquest enllac de cadenes de hashes actua com una marca de temps, unint les dades del far en una estructura tracable. Tambe proporciona seguretat, permetent detectar manipulacions immediatament. i½El protocol Twine ens permet entreteixir tots aquests altres fars en un

tapis de confiança, i $\frac{1}{2}$ afegix Palfre

- . Tot el procés és de codi obert i està disponible per al públic, permetent que qualsevol persona el revisi o fins i tot construeixi el seu propi generador basant-se en el fet
- . Així, CURBy es pot utilitzar en qualsevol lloc on calgui una font pública i independent de nombres aleatoris, com la selecció de jurats, auditories aleatòries o l'assignació de recursos per sorteig públic

Referència:

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](https://doi.org/10.1038/s41586-025-09054-3)