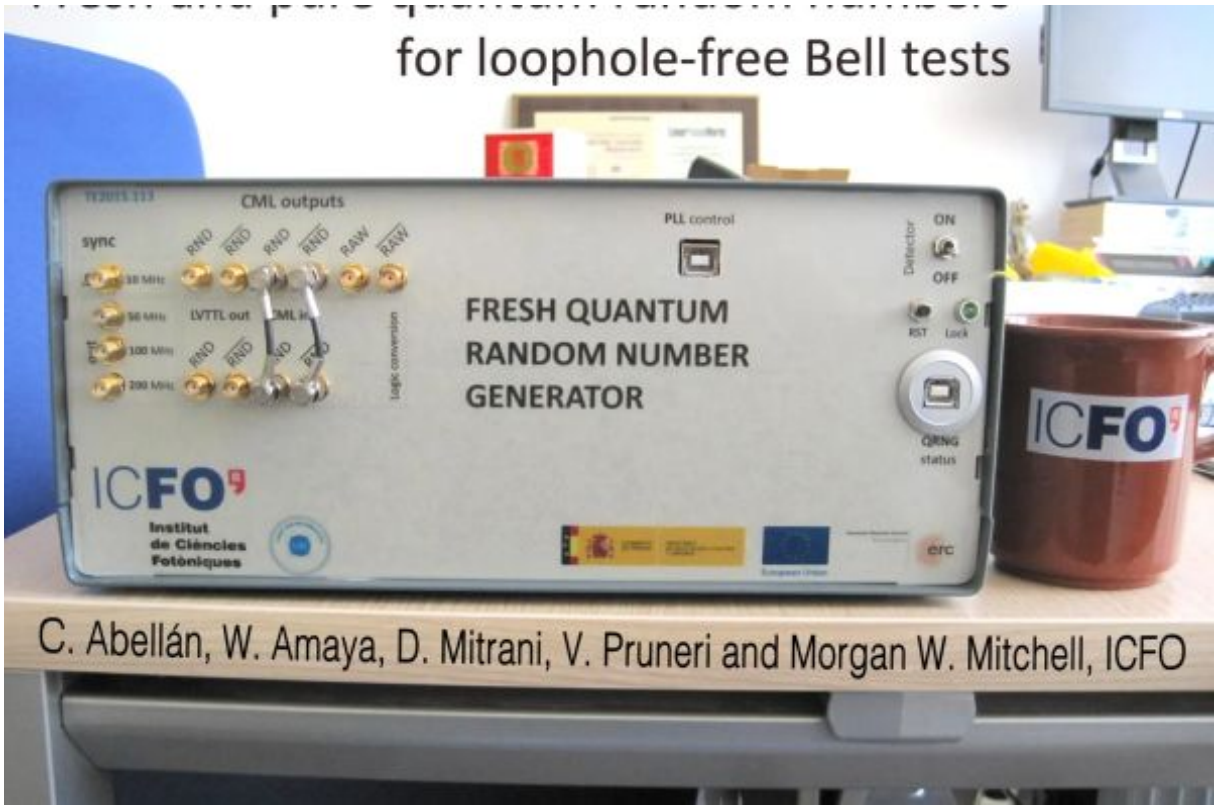


NIST i els seus socis utilitzen la mecanica quantica per crear una fabrica de nombres aleatoris

NIST i els seus socis de la Universitat de Colorado a Boulder, en col·laboracio amb ICFO i QuSide, han construit el prime generador de nombres aleatoris que utilitza l'entrellacamen quantic per produir nombres aleatoris verificables. Ofert com un servei public gratuit, el Colorado University Randomness Beacon (CURBy) es pot utilitzar a qualsevol lloc on una font publica i independent de nombres aleatoris sigui necessaria, com ara la seleccio de candidats per a un jurat o l'assignacio de recursos mitjancant un sorteig public.

June 12, 2025

L'aleatorietat es increiblement util. Sovint, les persones fan servir metodes com llencar daus o una moneda per prendre decisions justes. Els nombres aleatoris permeten als auditors fer seleccions completament imparcials. L'aleatorietat tambe es clau per a la seguretat: si una

contrasenya o codi es una seqüencia impredictible de nombres, es molt mes dificil d trencar. Molts dels sistemes criptografics actuals utilitzen generadors de nombres aleatori per produir claus segures

Pero com podem saber si un nombre es realment aleatori? Els algorismes classics nome poden crear nombres pseudoaleatoris, de manera que algu amb prou coneixement d l'algorisme o del sistema podria manipular-lo o predir el nombre següent. Un expert en tru s de mans podria manipular el llancament d'una moneda per garantir un resultat. Fins i tot e s llancaments mes acurats poden tenir biaix; amb prou estudi, els seus resultats podri n arribar a predir-s

. i¿½La veritable aleatorietat es allo que res en tot l'univers pot predir amb antelacioi¿? , diu Krister Shalm, fisic del NIST. Fins i tot si un generador fes servir processos naturals aparentment aleatoris, seria dificil verificar que realment ho son, afegeix Shalm.

Einstein creia que la natura no era aleatoria, pronunciant la seva famosa frase: i¿½Deu no ju a als daus amb l'univers.i¿½ Pero els cientifics han demostrat que s'equivocava. A difere cia dels daus o dels algorismes, la mecanica quantica es intrinsecament aleatoria. Am un experiment quantic anomenat test de Bell, Shalm i el seu equip han convertit aquesta ont d'autentica aleatorietat quantica en un servei de generacio de nombres aleatoris tracab e i certificable. Els seus resultats acaben de ser publicats a Nature.

i¿½Si Deu juga als daus amb l'univers, aleshores aixo es pot convertir en el millor generad r de nombres aleatoris que l'univers permeti¿½, diu Shalm. i¿½El que voliem era portar quest experiment fora del laboratori i convertir-lo en un servei public ut l.i¿½ Per fer-ho realitat, els investigadors del NIST i de la Universitat de Colorado a Bou der van crear el Far d'Aleatorietat de la Universitat de Colorado, o per les seves sigles en angles. CURBy produeix nombres aleatoris automaticament i els transmet diariament a traves d'un lloc web perque 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 materia primera que la resta del sistema i¿½refinai¿½ 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 rapids generadors de nombres aleatoris quantics que el NIST va fer servir per als tests de Bell.

El test de Bell mesura parelles de fotons i¿½entrellacatsi¿½ amb propietats correlacion des fins i tot quan estan separats per grans distancies. Quan els investigadors mesuren una particula individual, el resultat es aleatori, pero les propietats de la parella estan mes correlacionades del que dicta la fisica classica, cosa que permet verificar l'aleatorie at. Einstein va anomenar aquesta no-localitat quantica i¿½accio fantasmagorica a distanc ai¿½. Escollir quines propietats mesurar en les particules entrellacades s'ha de fer molt ra

idament i amb un alt grau de confianca en l'aleatorietat. Aquesta es la contribucio de l'ICFO i QuSide. Gracies a aixo, els resultats de les mesures al test de Bell tambe van ser aleatoris, p ro a un nivell s
perior. Aquest es el primer servei de generacio de nombres aleatoris que utilitza la no-l calitat quantica com a font, i es tambe la font mes transparent de nombres aleatoris fins ara. Aixo es deu al fet que els resultats son certificables i tracables com mai abans. De fet, el gr n avenc del projecte es que els usuaris poden confiar en els nombres resultants sense neces itat de confiar en les entitats que els generen. Imagina dues forces politiques que han d'audi ar unes eleccions revisant una mostra aleatoria de vots. Cap confiara en l'altra per gen rar els nombres, pero poden confiar en un far d'aleat
rietat.i¿½ **Es un privilegi contribuir a aquesta generacio publica sense precedents d'aleatorietat basada en fenomens de fisica quantica guardonats amb el Nobel. Es un exemple clar de com les tecnologies quantiques poden reforcar la seguretat en l'era d'internet**i¿½, comen a Morgan Mitchell, Professor ICREA i de l'ICFO. El Dr. Carlos Abellan, CEO de QuSide, afegei : i¿½ **Es un veritable honor contribuir a aquest experiment amb la nostra tecnologia de generacio de nombres aleatoris quantics. A QuSide, seguim avancant en la industrialitzacio d'aquests nous dispositius d'aleatorietat amb capacitats avancades de verificacio**i¿?

Un nou servei public disponible

i¿½CURBy es un dels primers serveis publics disponibles que opera amb un avantatge quant c demostrable. Es un gran assoliment per a nosaltres,i¿½ explica Shalm. i¿½La qualitat i l' rigen d'aquests bits aleatoris es poden certificar directament, cosa que els gene adors convencionals no poden f
r.i¿½ El NIST va fer una de les primeres proves experimentals completes de Bell l'a y 2015, establint 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 aixo, 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 comenca 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 i¿½tirades de monedai¿½ 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 ningu, 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 hashs 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 hashs,
creant una xarxa d'aleatorietat en la qual tothom contribueix pero ningu 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. i¿½El protocol Twine ens permet entreteixir tots aquests altres fars en un
tapis de confianca,i¿½ afegeix Palfre
. Tot el proces es de codi obert i esta disponible per al public, permetent que qualsev
l persona el revisi o fins i tot construeixi el seu propi generador basant-se en el fa
. Aixi, CURBy es pot utilitzar en qualsevol lloc on calgui una font publica i independent
e nombres aleatoris, com la seleccio de jurats, auditories aleatories o l'assignacio de recurs
s per sorteig publi

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