

Un cami eficient cap a claus quantiques segures

Les entropies de Renyi, centrals en les proves de seguretat modernes de distribucio quantica de claus, han estat tradicionalment dificils d'optimitzar des del punt de vista computacional. Investigadors de l'ICFO ara han presentat, en un article de PRX Quantum, un metode per calcular-les de manera eficient i fiable, cosa que dona lloc a proves de seguretat mes estables.

September 14, 2026

Era 1984 quan Bennett i Brassard van dissenyar el primer protocol de distribucio quantica de claus (QKD, per les seves sigles en angles), el BB84, marcant l'inici el camp de la criptografia quantica. Mes de quaranta anys despres, investigadors i investigadores d'arreu del mon han dut a terme nombrosos experiments, han ampliat els marcs teorics i han desenvolupat una gran varietat de nous protocols QKD. La idea fonamental, pero, es mante intacta: l'Alicia i en Bob, dos usuaris honestos que volen comunicar-se de forma segura, intercanvien i mesuren estats quantics per obtenir una clau secreta, confiant unicament en les lleis de la fisica

quantica per protegir-se de l'Eva, l'espia mes intel·ligent i maliciosa de totes
Per avaluar si un protocol QKD es segur, cal acotar la quantitat d'informacio que l'Eva po arribar a obtenir dels estats quantics intercanviats. Aixo s'ha calculat tradicionalmen mitjancant l'anomenada entropia de von Neumann, pero la majoria de les proves d seguretat modernes ara utilitzen una**entropia** mes general anomenada de **Renyi**, una familia d'entropies que te en compte com son d'optimes les mesures escollides. Introduint un pas addicional d'optimitzacio sobre aquest conjunt, els investigadors poden aproximar-se encara mes a la clau que l'Alicia i en Bob obtenen realment.
Aquesta optimitzacio, pero, es computacionalment dificil de resoldre. Els enfocaments actualment disponibles es basen en algorismes ad hoc que son lents, numericament inestables o aplicables nomes a casos particulars. Almenys, aquesta era la situacio fins que la **Mariana Navarro,** investigadora de l'ICFO que esta duent a terme un doctorat industrial a Luxquanta, una spin-off de l'ICFO que ofereix solucions de criptografia quantica per a empreses i xarxes de telecomunicacions, va trobar una manera de superar aquestes dificultats computacionals. Sota la supervisio del **Dr. Carlos Pascual Garcia**, antic investigador de l'ICFO i ara Cap de Teoria Quantica a Luxquanta, juntament amb l'Andre Gonzalez Lorente, en Pablo Parellada i el Dr. Mateus Araujo de la Universitat de Valladolid, utilitzant metodes numerics ja consolidats (concretament, l'optimitzacio conica), l'equip h desenvolupat**un metode practic i fiable per calcular entropies de Renyi.**
Publicat recentment a PRX Quantum, el seu metode basat en optimitzacio conica permet abordar de manera eficient diversos protocols QKD, des de l'historic BB84 fins a un protocol mes exigent de variables continues amb modulacio discreta, el qual requereix sistemes quantics mes grans i restriccions experimentals mes complexes.
i¿½Al principi, ens va sorprendre la velocitat de la nostra estrategiai¿½, recorda la Mar ana Navarro, primera autora de l'article. En la prova numerica per al BB84 amb qbits, per exemple, el metode conic va resoldre l'optimitzacio en una fraccio de segon, mentre que implementacions comparables trigaven desenes de segons. i¿½A mes, **el nostre metode no nomes es mes rapid, sino tambe mes sistematic i numericament precis que els enfocaments anteriors**i¿½, afegei
. El següent pas natural seria calcular taxes de clau segura per a protocols mes complex s, com el BB84 amb estats esquer (decoy-state) i el QKD independent del dispositiu de mesura. Ara be, segons en Carlos Pascual Garcia, un dels investigadors senior de l'estudi, aquest no es l'unic benefici. L'optimitzacio conica tambe te el potencial de permetre comparacions mes justes entre dissenys de protocols alternatius, estudiar amb precisio les perdues del canal o l'eficiencia dels detectors en un experiment, i oferir informacio practica sobre a quina distancia poden estar l'Alicia i en Bob tot mantenint la seguretat.
i¿½Fa quaranta anys, ni tan sols Bennett i Brassard haurien pogut imaginar com seria avui a criptografia quanticai¿½, reflexiona l'investigador. i¿½El futur es incert, i nomes el temp dira l'impacte que tindra el nostre estudi. Pero m'alegro de poder dir que ja estem pers

guint aquests objectius mes ambiciosos, i els resultats preliminars son molt prometedo

Referencia:
Navarro, M., et. al., Finite-size quantum key distribution rates from Renyi entropies using conic optimization, PRX Quantum **7**, 033051 (2026).
DOI: https://doi.org/10.1103/bf9s-m4jb

Agraiments:
MN and CPG were supported by the Government of Spain (Severo Ochoa CEX2019-000910-S, FUNQIP and NextGeneration EU PRTR-C17.I1) and European Union (QSNP, 101114043). MN acknowledges funding from the European Union's Horizon Europe research and innovation programme under the MSCA Grant Agreement No. 101081441. CPG has received funding from the European Union's Digital Europe Programme under the project QUARTER (101091588) and Horizon 2020 Research and Innovation Programme under the project QSNP (101114043), and from the European Innovation Council's Horizon Europe EIC Accelerator Programme under the project MIQRO (101161539). The research of AGL, PVP, and MA was supported by the Q-CAYLE project, funded by the European Union-Next Generation UE/MICIU/Plan de Recuperacion, Transformacion y Resiliencia/Junta de Castilla y Leon (PRTRC17.11), and also by the Department of Education of the Junta de Castilla y Leon and FEDER Funds (Reference: CLU-2023-1-05). PVP has also been funded under the UVa 2024 predoctoral contract, co-financed by Banco Santander. MA was also supported by the Spanish Agencia Estatal de Investigacion, Grant Nos.~RYC2023-044074-I and PID2024-161725OA-I00.